

Command Line Interface Reference for the ProSafe 7200 Series Layer-2 Switches, Software Version 6.0

NETGEAR®

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10235-01
February 2007

Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc..

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

February 2007

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

EN 55 022 Declaration of Conformance

This is to certify that the ProSafe 7200 Series Layer-2 Managed Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe 7200 Series Layer-2 Managed Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe 7200 Series Layer-2 Managed Switch gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Product and Publication Details

| | |
|-----------------------------------|--|
| Model Number: | FSM72xx/GSM72xx |
| Publication Date: | February 2007 |
| Product Family: | managed switch |
| Product Name: | ProSafe 7200 Series Layer-2 Managed Switch |
| Home or Business Product: | Business |
| Language: | English |
| Publication Part Number: | 202-10235-01 |
| Publication Version Number | 1.0 |

Contents

Command Line Interface Reference for the ProSafe 7200 Series Layer-2 Switches, Software Version 6.0

Chapter 1

About This Manual

| | | |
|-----|---------------------------------|-----|
| 1.1 | Audience | 1-1 |
| 1.2 | Scope | 1-1 |
| 1.3 | Typographical Conventions | 1-2 |
| 1.4 | Special Message Formats | 1-2 |
| 1.5 | How to Use This Manual | 1-3 |
| 1.6 | How to Print this Manual | 1-3 |
| 1.7 | Revision History | 1-4 |

Chapter 2

Overview

| | | |
|-------|--|------|
| 2.1 | Scope | 2-1 |
| 2.2 | Product Concept | 2-1 |
| 2.3 | Using the Command-Line Interface | 2-2 |
| 2.3.1 | Command Syntax | 2-2 |
| 2.3.2 | Command Conventions | 2-3 |
| 2.3.3 | Unit-Slot-Port Naming Convention | 2-5 |
| 2.3.4 | Using the “No” Form of a Command | 2-6 |
| 2.3.5 | Command Modes | 2-6 |
| 2.3.6 | Entering CLI Commands | 2-9 |
| 2.3.7 | Using CLI Help | 2-10 |
| 2.3.8 | Accessing the CLI | 2-11 |

Chapter 3

Administrative Access Commands

| | | |
|-------|----------------------------------|-----|
| 3.1 | Network Interface Commands | 3-1 |
| 3.1.1 | enable | 3-1 |

| | | |
|-------|--|------|
| 3.1.2 | network parms (parameter) | 3-2 |
| 3.1.3 | network mgmt_vlan | 3-2 |
| 3.1.4 | network protocol | 3-2 |
| 3.1.5 | show network | 3-3 |
| 3.2 | Configuring the Switch Management CPU (ezconfig) | 3-5 |
| 3.3 | Console Port Access Commands | 3-7 |
| 3.3.1 | configuration | 3-7 |
| 3.3.2 | lineconfig | 3-7 |
| 3.3.3 | serial baudrate | 3-8 |
| 3.3.4 | serial timeout | 3-8 |
| 3.3.5 | show serial | 3-9 |
| 3.4 | Telnet Commands | 3-10 |
| 3.4.1 | telnet | 3-10 |
| 3.4.2 | transport input telnet | 3-10 |
| 3.4.3 | transport output telnet | 3-11 |
| 3.4.4 | session-limit | 3-11 |
| 3.4.5 | session-timeout | 3-12 |
| 3.4.6 | telnetcon maxsessions | 3-12 |
| 3.4.7 | telnetcon timeout | 3-13 |
| 3.4.8 | show telnet | 3-13 |
| 3.4.9 | show telnetcon | 3-14 |
| 3.5 | Secure Shell (SSH) Command | 3-15 |
| 3.5.1 | ip ssh | 3-15 |
| 3.5.2 | ip ssh protocol | 3-15 |
| 3.5.3 | sshcon maxsessions | 3-16 |
| 3.5.4 | sshcon timeout | 3-16 |
| 3.5.5 | show ip ssh | 3-17 |
| 3.6 | Hypertext Transfer Protocol (HTTP) Commands | 3-17 |
| 3.6.1 | ip http secure-port | 3-17 |
| 3.6.2 | ip http secure-protocol | 3-18 |
| 3.6.3 | ip http secure-server | 3-18 |
| 3.6.4 | ip http server | 3-18 |
| 3.6.5 | network javamode | 3-19 |
| 3.6.6 | show ip http | 3-19 |
| 3.7 | User Account Commands | 3-20 |

| | | |
|-------|-----------------------------------|------|
| 3.7.1 | users name | 3-20 |
| 3.7.2 | users passwd | 3-21 |
| 3.7.3 | users snmpv3 accessmode | 3-21 |
| 3.7.4 | users snmpv3 authentication | 3-22 |
| 3.7.5 | users snmpv3 encryption | 3-22 |
| 3.7.6 | show login session | 3-23 |
| 3.7.7 | show users | 3-23 |
| 3.7.8 | disconnect | 3-24 |

Chapter 4

Port and System Setup Commands

| | | |
|--------|--|------|
| 4.1 | Port Configuration Commands | 4-1 |
| 4.1.1 | interface | 4-1 |
| 4.1.2 | interface range | 4-2 |
| 4.1.3 | interface vlan | 4-2 |
| 4.1.4 | interface lag | 4-2 |
| 4.1.5 | cablestatus | 4-2 |
| 4.1.6 | auto-negotiate | 4-3 |
| 4.1.7 | auto-negotiate all | 4-3 |
| 4.1.8 | mtu | 4-4 |
| 4.1.9 | shutdown | 4-4 |
| 4.1.10 | shutdown all | 4-5 |
| 4.1.11 | speed | 4-5 |
| 4.1.12 | speed all | 4-6 |
| 4.1.13 | monitor session | 4-6 |
| 4.1.14 | no monitor | 4-7 |
| 4.1.15 | show monitor session | 4-7 |
| 4.1.16 | show port | 4-7 |
| 4.1.17 | show port protocol | 4-8 |
| 4.1.18 | show port status | 4-9 |
| 4.2 | Pre-login Banner and System Prompt Commands | 4-9 |
| 4.2.1 | copy | 4-9 |
| 4.2.2 | set prompt | 4-9 |
| 4.3 | Simple Network Time Protocol (SNTP) Commands | 4-11 |
| 4.3.1 | sntp broadcast client poll-interval | 4-11 |
| 4.3.2 | sntp client mode | 4-11 |

| | | |
|--------|--|------|
| 4.3.3 | sntp client port | 4-12 |
| 4.3.4 | sntp unicast client poll-interval | 4-12 |
| 4.3.5 | sntp unicast client poll-timeout | 4-12 |
| 4.3.6 | sntp unicast client poll-retry | 4-13 |
| 4.3.7 | sntp multicast client poll-interval | 4-13 |
| 4.3.8 | sntp server | 4-14 |
| 4.3.9 | show sntp | 4-14 |
| 4.3.10 | show sntp client | 4-14 |
| 4.3.11 | show sntp server | 4-15 |
| 4.3.12 | clock timezone | 4-16 |
| 4.4 | MAC Address and MAC Database Commands | 4-16 |
| 4.4.1 | network mac-address | 4-17 |
| 4.4.2 | network mac-type | 4-17 |
| 4.4.3 | macfilter | 4-18 |
| 4.4.4 | macfilter adddest | 4-18 |
| 4.4.5 | macfilter adddest all | 4-19 |
| 4.4.6 | macfilter addsrc | 4-19 |
| 4.4.7 | macfilter addsrc all | 4-20 |
| 4.4.8 | bridge aging-time | 4-21 |
| 4.4.9 | show forwardingdb agetime | 4-22 |
| 4.4.10 | show mac-address-table multicast | 4-22 |
| 4.4.11 | show mac-address-table static | 4-23 |
| 4.4.12 | show mac-address-table staticfiltering | 4-24 |
| 4.4.13 | show mac-address-table stats | 4-24 |
| 4.5 | DNS Client Commands | 4-25 |
| 4.5.1 | ip domain-lookup | 4-26 |
| 4.5.2 | ip domain-name | 4-26 |
| 4.5.3 | ip name-server | 4-26 |
| 4.5.4 | ip host | 4-27 |
| 4.5.5 | clear host | 4-27 |
| 4.5.6 | show hosts | 4-27 |

Chapter 5

Spanning Tree Protocol Commands

| | | |
|-------|----------------------------------|-----|
| 5.1 | STP Configuration Commands | 5-1 |
| 5.1.1 | spanning-tree | 5-1 |

| | | |
|--------|--|------|
| 5.1.2 | spanning-tree bpdumigrationcheck | 5-2 |
| 5.1.3 | spanning-tree configuration name | 5-2 |
| 5.1.4 | spanning-tree configuration revision | 5-3 |
| 5.1.5 | spanning-tree edgeport | 5-3 |
| 5.1.6 | spanning-tree edgeport all | 5-3 |
| 5.1.7 | spanning-tree forceversion | 5-4 |
| 5.1.8 | spanning-tree forward-time | 5-4 |
| 5.1.9 | spanning-tree hello-time | 5-5 |
| 5.1.10 | spanning-tree max-age | 5-5 |
| 5.1.11 | spanning-tree max-hops | 5-6 |
| 5.1.12 | spanning-tree mst | 5-6 |
| 5.1.13 | spanning-tree mst instance | 5-7 |
| 5.1.14 | spanning-tree mst priority | 5-8 |
| 5.1.15 | spanning-tree mst vlan | 5-9 |
| 5.1.16 | spanning-tree port mode | 5-9 |
| 5.1.17 | spanning-tree port mode all | 5-9 |
| 5.1.18 | spanning-tree bpduforwarding | 5-10 |
| 5.2 | STP Show Commands | 5-10 |
| 5.2.1 | show spanning-tree | 5-10 |
| 5.2.2 | show spanning-tree summary | 5-12 |
| 5.2.3 | show spanning-tree interface | 5-13 |
| 5.2.4 | show spanning-tree mst port detailed | 5-14 |
| 5.2.5 | show spanning-tree mst port summary | 5-16 |
| 5.2.6 | show spanning-tree mst summary | 5-16 |
| 5.2.7 | show spanning-tree vlan | 5-17 |

Chapter 6

VLAN Commands

| | | |
|-------|-----------------------------------|-----|
| 6.1 | VLAN Configuration Commands | 6-1 |
| 6.1.1 | vlan database | 6-1 |
| 6.1.2 | network mgmt_vlan | 6-2 |
| 6.1.3 | vlan | 6-2 |
| 6.1.4 | vlan acceptframe | 6-2 |
| 6.1.5 | vlan ingressfilter | 6-3 |
| 6.1.6 | vlan makestatic | 6-3 |
| 6.1.7 | vlan name | 6-4 |

| | | |
|--------|---|------|
| 6.1.8 | vlan participation | 6-4 |
| 6.1.9 | vlan participation all | 6-5 |
| 6.1.10 | vlan port acceptframe all | 6-5 |
| 6.1.11 | vlan port pvid all | 6-6 |
| 6.1.12 | vlan port tagging all | 6-6 |
| 6.1.13 | vlan port ingressfilter all | 6-7 |
| 6.1.14 | Global Config | 6-7 |
| 6.1.15 | vlan protocol group | 6-7 |
| 6.1.16 | vlan protocol group add protocol | 6-7 |
| 6.1.17 | vlan protocol group remove | 6-8 |
| 6.1.18 | protocol group | 6-8 |
| 6.1.19 | protocol vlan group | 6-9 |
| 6.1.20 | protocol vlan group all | 6-9 |
| 6.1.21 | vlan pvid | 6-10 |
| 6.1.22 | vlan tagging | 6-10 |
| 6.2 | VLAN Show Commands | 6-11 |
| 6.2.1 | show vlan | 6-11 |
| 6.2.2 | show vlan <vlan_id> | 6-11 |
| 6.2.3 | show vlan port | 6-13 |
| 6.3 | Provisioning (IEEE 802.1p) Commands | 6-14 |
| 6.3.1 | vlan port priority all | 6-14 |
| 6.3.2 | vlan priority | 6-14 |

Chapter 7

DHCP Commands

| | | |
|--------|--|-----|
| 7.1 | DHCP Server Commands (DHCP Config Pool Mode) | 7-2 |
| 7.1.1 | ip dhcp pool | 7-2 |
| 7.1.2 | client-identifier | 7-2 |
| 7.1.3 | client-name | 7-3 |
| 7.1.4 | default-router | 7-3 |
| 7.1.5 | dns-server | 7-4 |
| 7.1.6 | hardware-address | 7-4 |
| 7.1.7 | host | 7-4 |
| 7.1.8 | lease | 7-5 |
| 7.1.9 | network | 7-6 |
| 7.1.10 | bootfile | 7-6 |

| | | |
|--------|---|------|
| 7.1.11 | domain-name | 7-6 |
| 7.1.12 | netbios-name-server | 7-7 |
| 7.1.13 | netbios-node-type | 7-7 |
| 7.1.14 | next-server | 7-8 |
| 7.1.15 | option | 7-8 |
| 7.2 | DHCP Server Commands (Global Config Mode) | 7-9 |
| 7.2.1 | ip dhcp excluded-address | 7-9 |
| 7.2.2 | ip dhcp ping packets | 7-10 |
| 7.2.3 | service dhcp | 7-10 |
| 7.2.4 | ip dhcp bootp automatic | 7-11 |
| 7.2.5 | ip dhcp conflict logging | 7-11 |
| 7.3 | DHCP Server Clear and Show Commands | 7-12 |
| 7.3.1 | clear ip dhcp binding | 7-12 |
| 7.3.2 | clear ip dhcp server statistics | 7-12 |
| 7.3.3 | clear ip dhcp conflict | 7-12 |
| 7.3.4 | show ip dhcp binding | 7-12 |
| 7.3.5 | show ip dhcp global configuration | 7-13 |
| 7.3.6 | show ip dhcp pool configuration | 7-13 |
| 7.3.7 | show ip dhcp server statistics | 7-14 |
| 7.3.8 | show ip dhcp conflict | 7-15 |
| 7.4 | DHCP and BOOTP Relay Commands | 7-15 |
| 7.4.1 | ip dhcp relay information option | 7-15 |
| 7.4.2 | bootpdhcprelay | 7-16 |
| 7.4.3 | bootpdhcprelay maxhopcount | 7-16 |
| 7.4.4 | bootpdhcprelay minwaittime | 7-17 |
| 7.4.5 | bootpdhcprelay serverip | 7-17 |
| 7.4.6 | show bootpdhcprelay | 7-18 |

Chapter 8

GARP, GVRP, and GMRP Commands

| | | |
|-------|-------------------------------|-----|
| 8.1 | GARP Commands | 8-2 |
| 8.1.1 | set garp timer join | 8-2 |
| 8.1.2 | set garp timer leave | 8-3 |
| 8.1.3 | set garp timer leaveall | 8-4 |
| 8.1.4 | show garp | 8-4 |
| 8.2 | GVRP Commands | 8-5 |

| | | |
|-------|-----------------------------------|------|
| 8.2.1 | set gvrp adminmode | 8-5 |
| 8.2.2 | set gvrp interfacemode | 8-5 |
| 8.2.3 | show gvrp configuration | 8-6 |
| 8.3 | GMRP Commands | 8-7 |
| 8.3.1 | set gmrp adminmode | 8-7 |
| 8.3.2 | set gmrp interfacemode | 8-8 |
| 8.3.3 | show gmrp configuration | 8-8 |
| 8.3.4 | show mac-address-table gmrp | 8-10 |

Chapter 9

Port-Based Traffic Control Commands

| | | |
|--------|--------------------------------------|-----|
| 9.1 | Port Security Commands | 9-1 |
| 9.1.1 | port-security | 9-2 |
| 9.1.2 | port-security max-dynamic | 9-2 |
| 9.1.3 | port-security max-static | 9-3 |
| 9.1.4 | port-security mac-address | 9-3 |
| 9.1.5 | port-security mac-address move | 9-3 |
| 9.1.6 | show port-security | 9-4 |
| 9.1.7 | show port-security | 9-4 |
| 9.1.8 | show port-security dynamic | 9-4 |
| 9.1.9 | show port-security static | 9-4 |
| 9.1.10 | show port-security violation | 9-5 |
| 9.2 | Storm Control Commands | 9-5 |
| 9.2.1 | storm-control broadcast | 9-5 |
| 9.2.2 | storm-control multicast all | 9-6 |
| 9.2.3 | storm-control unicast all | 9-6 |
| 9.2.4 | storm-control broadcast | 9-7 |
| 9.2.5 | storm-control multicast | 9-7 |
| 9.2.6 | storm-control unicast | 9-8 |
| 9.2.7 | storm-control flowcontrol | 9-8 |
| 9.2.8 | show storm-control | 9-9 |

Chapter 10

SNMP Commands

| | | |
|--------|-----------------------------------|------|
| 10.1 | SNMP Configuration Commands | 10-1 |
| 10.1.1 | snmp-server | 10-1 |
| 10.1.2 | snmp-server community | 10-2 |

| | | |
|---------|------------------------------------|-------|
| 10.1.3 | snmp-server community ipaddr | 10-2 |
| 10.1.4 | snmp-server community ipmask | 10-3 |
| 10.1.5 | snmp-server community mode | 10-3 |
| 10.1.6 | snmp-server community ro | 10-4 |
| 10.1.7 | snmp-server community rw | 10-4 |
| 10.1.8 | snmp-server traps violation | 10-4 |
| 10.1.9 | snmp-server traps | 10-5 |
| 10.1.10 | snmp-server traps bcstorm | 10-5 |
| 10.1.11 | snmp-server traps linkmode | 10-6 |
| 10.1.12 | snmp-server traps multiusers | 10-6 |
| 10.1.13 | snmp-server traps stpmode | 10-6 |
| 10.1.14 | snmptrap | 10-7 |
| 10.1.15 | snmptrap snmpversion | 10-8 |
| 10.1.16 | snmptrap ipaddr | 10-8 |
| 10.1.17 | snmptrap mode | 10-8 |
| 10.1.18 | snmp trap link-status | 10-9 |
| 10.1.19 | snmp trap link-status all | 10-9 |
| 10.2 | SNMP Show Commands | 10-10 |
| 10.2.1 | show snmpcommunity | 10-10 |
| 10.2.2 | show snmptrap | 10-11 |
| 10.2.3 | show trapflags | 10-11 |

Chapter 11

Port-Based Access and Authentication Commands

| | | |
|---------|--|------|
| 11.1 | Port-Based Network Access Control Commands | 11-1 |
| 11.1.1 | authentication login | 11-1 |
| 11.1.2 | clear dot1x statistics | 11-3 |
| 11.1.3 | clear radius statistics | 11-3 |
| 11.1.4 | dot1x defaultlogin | 11-3 |
| 11.1.5 | dot1x initialize | 11-3 |
| 11.1.6 | dot1x login | 11-3 |
| 11.1.7 | dot1x max-req | 11-4 |
| 11.1.8 | dot1x port-control | 11-4 |
| 11.1.9 | dot1x port-control all | 11-5 |
| 11.1.10 | dot1x re-authenticate | 11-5 |
| 11.1.11 | dot1x re-authentication | 11-6 |

| | | |
|---------|---------------------------------|-------|
| 11.1.12 | dot1x system-auth-control | 11-6 |
| 11.1.13 | dot1x timeout | 11-6 |
| 11.1.14 | dot1x user | 11-7 |
| 11.1.15 | users defaultlogin | 11-8 |
| 11.1.16 | users login | 11-8 |
| 11.1.17 | show authentication | 11-8 |
| 11.1.18 | show authentication users | 11-9 |
| 11.1.19 | show dot1x | 11-9 |
| 11.1.20 | show dot1x users | 11-13 |
| 11.1.21 | show users authentication | 11-13 |
| 11.2 | RADIUS Commands | 11-13 |
| 11.2.1 | radius accounting mode | 11-13 |
| 11.2.2 | radius server host | 11-14 |
| 11.2.3 | radius server key | 11-15 |
| 11.2.4 | radius server msgauth | 11-15 |
| 11.2.5 | radius server primary | 11-16 |
| 11.2.6 | radius server retransmit | 11-16 |
| 11.2.7 | radius server timeout | 11-16 |
| 11.2.8 | show radius | 11-17 |
| 11.2.9 | show radius accounting | 11-18 |
| 11.2.10 | show radius statistics | 11-19 |

Chapter 12

Port-Channel/LAG (802.3ad) Commands

| | | |
|---------|---|------|
| 12.1 | Port-Channel Configuration Commands | 12-1 |
| 12.1.1 | addport | 12-2 |
| 12.1.2 | deleteport (Interface Config) | 12-2 |
| 12.1.3 | deleteport (Global Config) | 12-2 |
| 12.1.4 | port-channel | 12-3 |
| 12.1.5 | clear port-channel | 12-3 |
| 12.1.6 | port-channel staticcapability | 12-3 |
| 12.1.7 | port lacpmode | 12-4 |
| 12.1.8 | port lacpmode all | 12-4 |
| 12.1.9 | port-channel adminmode | 12-4 |
| 12.1.10 | port-channel name | 12-5 |
| 12.1.11 | port-channel linktrap | 12-5 |

| | | |
|--------|----------------------------------|------|
| 12.2 | Port-Channel Show Commands | 12-6 |
| 12.2.1 | show port-channel | 12-6 |
| 12.2.2 | show port-channel | 12-6 |

Chapter 13

IGMP Snooping Commands

| | | |
|--------|--|-------|
| 13.1 | IGMP Snooping Configuration Commands | 13-1 |
| 13.1.1 | ip igmpsnooping | 13-1 |
| 13.1.2 | ip igmpsnooping interfacemode | 13-2 |
| 13.1.3 | ip igmpsnooping groupmembership-interval | 13-3 |
| 13.1.4 | ip igmpsnooping maxresponse | 13-4 |
| 13.1.5 | ip igmpsnooping mcruntime | 13-4 |
| 13.1.6 | ip igmp mrouter | 13-5 |
| 13.1.7 | ip igmp mrouter interface | 13-5 |
| 13.1.8 | ip igmpsnooping unknown-multicast | 13-6 |
| 13.2 | IGMP Snooping Show Commands | 13-6 |
| 13.2.1 | show ip igmp | 13-6 |
| 13.2.2 | show ip igmp mrouter interface | 13-8 |
| 13.2.3 | show ip igmp mrouter vlan | 13-8 |
| 13.2.4 | show mac-address-table igmpsnooping | 13-8 |
| 13.3 | IGMP Querier Commands | 13-9 |
| 13.3.1 | ip igmpsnooping querier | 13-10 |
| 13.3.2 | ip igmpsnooping querier ip-address | 13-10 |
| 13.3.3 | ip igmpsnooping querier query-interval | 13-11 |
| 13.3.4 | show ip igmpsnooping querier | 13-11 |

Chapter 14

Quality of Service (QoS) Commands

| | | |
|--------|--|------|
| 14.1 | Class of Service (CoS) Commands (GSM7248 only) | 14-2 |
| 14.1.1 | classofservice dot1p-mapping | 14-2 |
| 14.1.2 | classofservice ip-precedence-mapping | 14-2 |
| 14.1.3 | classofservice ip-dscp-mapping | 14-3 |
| 14.1.4 | classofservice trust | 14-3 |
| 14.1.5 | cos-queue min-bandwidth | 14-4 |
| 14.1.6 | cos-queue strict | 14-4 |
| 14.1.7 | traffic-shape | 14-5 |
| 14.1.8 | show classofservice dot1p-mapping | 14-5 |

| | | |
|---------|---|-------|
| 14.1.9 | show classofservice ip-precedence-mapping | 14-5 |
| 14.1.10 | show classofservice ip-dscp-mapping | 14-6 |
| 14.1.11 | show classofservice trust | 14-6 |
| 14.1.12 | show interfaces cos-queue | 14-7 |
| 14.2 | Differentiated Services (DiffServ) Commands | 14-8 |
| 14.2.1 | diffserv | 14-9 |
| 14.3 | DiffServ Class Commands (GSM7248 only) | 14-9 |
| 14.3.1 | class-map | 14-10 |
| 14.3.2 | class-map rename | 14-11 |
| 14.3.3 | match ethertype | 14-11 |
| 14.3.4 | match any | 14-11 |
| 14.3.5 | match class-map | 14-11 |
| 14.3.6 | match cos | 14-12 |
| 14.3.7 | match destination-address mac | 14-13 |
| 14.3.8 | match dstip | 14-13 |
| 14.3.9 | match dstl4port | 14-13 |
| 14.3.10 | match ip dscp | 14-14 |
| 14.3.11 | match ip precedence | 14-14 |
| 14.3.12 | match ip tos | 14-15 |
| 14.3.13 | match protocol | 14-16 |
| 14.3.14 | match source-address mac | 14-16 |
| 14.3.15 | match srcip | 14-16 |
| 14.3.16 | match srcl4port | 14-17 |
| 14.3.17 | match vlan | 14-17 |
| 14.4 | DiffServ Policy Commands (GSM7248 only) | 14-17 |
| 14.4.1 | policy-map | 14-18 |
| 14.4.2 | assign-queue | 14-19 |
| 14.4.3 | drop | 14-19 |
| 14.4.4 | conform-color | 14-20 |
| 14.4.5 | class | 14-20 |
| 14.4.6 | mark cos | 14-21 |
| 14.4.7 | mark ip-dscp | 14-21 |
| 14.4.8 | mark ip-precedence | 14-22 |
| 14.4.9 | police-simple | 14-22 |
| 14.4.10 | policy-map rename | 14-23 |

| | | |
|--------|---|-------|
| 14.5 | DiffServ Service Commands (GSM7248 only) | 14-23 |
| 14.5.1 | service-policy | 14-24 |
| 14.6 | DiffServ Show Commands | 14-25 |
| 14.6.1 | show class-map (GSM7248 only) | 14-25 |
| 14.6.2 | show diffserv | 14-26 |
| 14.6.3 | show policy-map (GSM7248 only) | 14-27 |
| 14.6.4 | show diffserv service (GSM7248 only) | 14-29 |
| 14.6.5 | show diffserv service brief (GSM7248 only) | 14-29 |
| 14.6.6 | show policy-map interface (GSM7248 only) | 14-30 |
| 14.6.7 | show service-policy (GSM7248 only) | 14-31 |
| 14.7 | MAC Access Control List (ACL) Commands (GSM7248 only) | 14-31 |
| 14.7.1 | mac access-list extended | 14-31 |
| 14.7.2 | mac access-list extended rename | 14-32 |
| 14.7.3 | {deny permit} | 14-32 |
| 14.7.4 | mac access-group | 14-34 |
| 14.7.5 | show mac access-lists | 14-34 |
| 14.8 | IP Access Control List (ACL) Commands (GSM7248 only) | 14-35 |
| 14.8.1 | access-list | 14-36 |
| 14.8.2 | ip access-group | 14-37 |
| 14.8.3 | show ip access-lists | 14-38 |
| 14.8.4 | show access-lists | 14-38 |

Chapter 15

System Maintenance Commands

| | | |
|---------|--|-------|
| 15.1 | System Information and Statistics Commands | 15-1 |
| 15.1.1 | show arp switch | 15-2 |
| 15.1.2 | show eventlog | 15-2 |
| 15.1.3 | show hardware | 15-2 |
| 15.1.4 | show interface | 15-3 |
| 15.1.5 | show interface ethernet | 15-5 |
| 15.1.6 | show logging | 15-14 |
| 15.1.7 | show mac-addr-table | 15-14 |
| 15.1.8 | clear mac-addr-table | 15-15 |
| 15.1.9 | show running-config | 15-16 |
| 15.1.10 | terminal length | 15-16 |
| 15.1.11 | show sysinfo | 15-16 |

| | | |
|---------|--|-------|
| 15.2 | System Utility Commands | 15-17 |
| 15.2.1 | traceroute | 15-17 |
| 15.2.2 | clear config | 15-18 |
| 15.2.3 | clear counters | 15-18 |
| 15.2.4 | clear igmpsnooping | 15-18 |
| 15.2.5 | clear pass | 15-18 |
| 15.2.6 | enable passwd | 15-18 |
| 15.2.7 | clear port-channel | 15-19 |
| 15.2.8 | clear traplog | 15-19 |
| 15.2.9 | clear vlan | 15-19 |
| 15.2.10 | copy | 15-19 |
| 15.2.11 | logout | 15-21 |
| 15.2.12 | ping | 15-21 |
| 15.2.13 | reload | 15-21 |
| 15.3 | Logging Commands | 15-22 |
| 15.3.1 | logging buffered | 15-22 |
| 15.3.2 | logging buffered wrap | 15-22 |
| 15.3.3 | logging console | 15-23 |
| 15.3.4 | logging host | 15-23 |
| 15.3.5 | logging host remove | 15-23 |
| 15.3.6 | logging port | 15-24 |
| 15.3.7 | logging syslog | 15-24 |
| 15.3.8 | show logging | 15-24 |
| 15.3.9 | show logging buffered | 15-26 |
| 15.3.10 | clear logging buffered | 15-26 |
| 15.3.11 | show logging hosts | 15-26 |
| 15.3.12 | show logging traplogs | 15-27 |
| 15.4 | CLI Command Logging Command | 15-27 |
| 15.4.1 | logging cli-command | 15-27 |
| 15.5 | Configuration Scripting Commands | 15-28 |
| 15.5.1 | script apply | 15-29 |
| 15.5.2 | script delete | 15-29 |
| 15.5.3 | script list | 15-29 |
| 15.5.4 | show script | 15-29 |
| 15.5.5 | script validate | 15-29 |

| | | |
|--------|--|-------|
| 15.6 | Packet Capture | 15-30 |
| 15.6.1 | capture transmit packet | 15-30 |
| 15.6.2 | capture receive packet | 15-30 |
| 15.6.3 | capture all packets | 15-31 |
| 15.6.4 | capture wrap | 15-31 |
| 15.6.5 | show capture packets | 15-31 |
| 15.7 | Dumping System Information | 15-32 |
| 15.8 | Setting the Output Length of show running-config | 15-32 |
| 15.8.1 | terminal length | 15-32 |
| 15.8.2 | terminal no length | 15-32 |

Appendix A

Command Changes from Release 3 to Release 5

Chapter 1

About This Manual

This chapter introduces the Command Line Interface Reference for the ProSafe 7200 Series Layer-2 Switches, Software Version 6.0. It describes the command-line interface (CLI) commands used to view and configure the 7200 Series Managed Switch software. You can access the CLI by using a direct connection to the serial port or by using telnet or SSH over a remote network connection.

1.1 Audience

This document is for system administrators who configure and operate systems using 7200 Series Managed Switch software. Software engineers who integrate 7200 Series Managed Switch software into their hardware platform can also benefit from a description of the configuration options.

This document assumes that the reader has an understanding of the 7200 Series Managed Switch software base and has read the appropriate specification for the relevant networking device platform. It also assumes that the reader has a basic knowledge of Ethernet and networking concepts.

1.2 Scope

This manual is written for the 7200 Series Managed Switch according to these specifications:

Table 1-1. Manual Specifications

| | |
|-------------------------|--|
| Product | ProSafe 7200 Series Layer-2 Managed Switch |
| Manual Part Number | 202-10235-01 |
| Manual Publication Date | February 2007 |



Note: Product updates are available on the NETGEAR Web site at <http://kbserver.netgear.com/products/>.

1.3 Typographical Conventions

This guide uses the following typographical conventions:

Table 1-2. Typographical conventions

| | |
|----------------|-------------------------------|
| <i>italics</i> | Emphasis. |
| bold | User input. |
| Small Caps | DOS file and directory names. |

1.4 Special Message Formats

This guide uses the following formats to highlight special messages:



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



Tip: A time-saving or resource-saving procedural step.








Warning: This is a warning of possible damage to the equipment or software malfunction.



Danger: Ignoring this type of warning could result in personal injury or death.

1.5 How to Use This Manual

The HTML version of this manual includes the following:

- Buttons  and  for browsing forwards or backwards through the manual one page at a time.
- A  button that displays the table of contents and possibly an  button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A  button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

1.6 How to Print this Manual

To print this manual, choose one of the following options.

- **Printing a Page in the HTML View.**

Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter.**

Use the *PDF of This Chapter* link at the top left of any page.

- Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

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

- Click the print icon in the window toolbar.



Tip: If your printer supports printing of two or more pages on a single sheet of paper, you can save paper and printer ink by clicking the printer Properties button and increasing the number of pages per sheet.

- **Printing the Full Manual.**

Use the *Complete PDF Manual* link at the top left of any page.

- Click the *Complete PDF Manual* link at the top left of any page in the manual.
The PDF version of the complete manual opens in a browser window.
- Click the print icon in the window toolbar.



Tip: If your printer supports printing of two or more pages on a single sheet of paper, you can save paper and printer ink by clicking the printer Properties button and increasing the number of pages per sheet.

1.7 Revision History

Table 1-3 lists the revision history of this manual.

Table 1-3. Revision History of This Manual

| Document Part Number | Revision | Change Description |
|----------------------|----------|---|
| 202-10235-01 | 1.0 | Document for version 6.0 software release |

Chapter 2

Overview

The 7200 Series Managed Switch software has two purposes:

- Assist attached hardware in switching frames, based on Layer 2, 3, or 4 information contained in the frames.
- Provide a complete device management portfolio to the network administrator.

2.1 Scope

7200 Series Managed Switch software encompasses both hardware and software support. It software is partitioned to run in the following processors:

- **CPU**—This code runs the networking device management portfolio and controls the overall networking device hardware. It also assists in frame forwarding, as needed and specified. This code is designed to run on multiple platforms with minimal changes from platform to platform.
- **Networking Device Processor**—This code does the majority of the packet switching, usually at wire speed. This code is platform dependent, and substantial changes might exist across products.

2.2 Product Concept

Fast Ethernet and Gigabit Ethernet switching continues to evolve from high-end backbone applications to desktop switching applications. The price of the technology continues to decline, while performance and feature sets continue to improve. Devices that are capable of switching Layers 2, 3, and 4 are increasingly in demand. 7200 Series Managed Switch software provides a flexible solution to these ever-increasing needs.

The exact functionality provided by each networking device on which the 7200 Series Managed Switch software base runs varies depending upon the platform and requirements of NETGEAR.

7200 Series Managed Switch software includes a set of comprehensive management functions for managing both the switch and the network. You can manage the 7200 Series Managed Switch software by using one of the following three methods:

- Web-based
- VT100 interface
- Simple Network Management Protocol (SNMP)

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

2.3 Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

This section describes the CLI syntax, conventions, and modes. It contains the following topics:

- [Section 2.3.1 “Command Syntax” on page 2-2](#)
- [Section 2.3.2 “Command Conventions” on page 2-3](#)
- [Section 2.3.3 “Unit-Slot-Port Naming Convention” on page 2-5](#)
- [Section 2.3.4 “Using the “No” Form of a Command” on page 2-6](#)
- [Section 2.3.5 “Command Modes” on page 2-6](#)
- [Section 2.3.6 “Entering CLI Commands” on page 2-9](#)
- [Section 2.3.7 “Using CLI Help” on page 2-10](#)
- [Section 2.3.8 “Accessing the CLI” on page 2-11](#)

2.3.1 Command Syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as **show network** or **clear vlan**, do not require parameters. Other commands, such as **network parms**, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the **network parms** command syntax:

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

- **network parms** is the command name.
- *<ipaddr>* and *<netmask>* are parameters and represent required values that you must enter after you type the command keywords.
- [*gateway*] is an optional parameter, so you are not required to enter a value in place of the parameter.

The CLI Command Reference lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The **show** commands also contain a description of the information that the command displays.

2.3.2 Command Conventions

In this document, the command name is in **bold** font. Parameters are in *italic* font. You must replace the parameter name with an appropriate value, which might be a name or number. Parameters are order dependent.

The parameters for a command might include mandatory values, optional values, or keyword choices. Table 2-1 describes the conventions this document uses to distinguish between value types.

Table 2-1. Parameter Conventions

| Symbol | Example | Description |
|--------------------|----------------------|---|
| <> angle brackets | <i><value></i> | Indicates that you must enter a value in place of the brackets and text inside them. |
| [] square brackets | <i>[value]</i> | Indicates an optional parameter that you can enter in place of the brackets and text inside them. |

Table 2-1. Parameter Conventions

| Symbol | Example | Description |
|-------------------------------------|----------------------------|--|
| { } curly braces | <i>{choice1 choice2}</i> | Indicates that you must select a parameter from the list of choices. |
| Vertical bars | <i>choice1 choice2</i> | Separates the mutually exclusive choices. |
| [{ }] Braces within square brackets | <i>[{choice1} choice2]</i> | Indicate a choice within an optional element. |

2.3.2.1 Common Parameter Values

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“ ”) are not valid user-defined strings. Table 2-2 describes common parameter values and value formatting.

Table 2-2. Parameter Descriptions

| Parameter | Description |
|------------------------|--|
| ipaddr | <p>This parameter is a valid IP address. You can enter the IP address in the following formats:</p> <ul style="list-style-type: none"> a (32 bits) a.b (8.24 bits) a.b.c (8.8.16 bits) a.b.c.d (8.8.8.8) <p>In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where <i>n</i> is any valid hexadecimal, octal or decimal number):</p> <ul style="list-style-type: none"> 0xn (CLI assumes hexadecimal format) 0n (CLI assumes octal format with leading zeros) n (CLI assumes decimal format) |
| macaddr | The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40. |
| areaid | Enter area IDs 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 format as IP addresses but are distinct from IP addresses. You can use the IP network number of the sub-netted network for the area ID. |
| routerid | Enter the value of <i><routerid></i> in dotted-decimal notation, such as 0.0.0.1. A router ID of 0.0.0.0 is invalid. |
| Interface or slot/port | Valid slot and port number separated by forward slashes. For example, 0/1 represents slot number 0 and port number 1. |

Table 2-2. Parameter Descriptions

| Parameter | Description |
|-------------------|--|
| Logical Interface | Logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical slot/port to configure the port-channel. |
| Character strings | Use double quotation marks to identify character strings, for example, "System Name with Spaces". An empty string ("") is not valid. |

2.3.3 Unit-Slot-Port Naming Convention

7200 Series Managed Switch software references physical entities such as cards and ports by using a Unit-Slot-Port (USP) naming convention. The software also uses this convention to identify certain logical entities, such as port-channel interfaces.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Table 2-3. Type of Slots

| Slot Type | Description |
|-----------------------|---|
| Physical slot numbers | Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots. |
| Logical slot numbers | Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces. |
| CPU slot numbers | The CPU slots immediately follow the logical slots. |

The port identifies the specific physical port or logical interface being managed on a given slot.

Table 2-4. Type of Ports

| Port Type | Description |
|--------------------|--|
| Physical Ports | The physical ports for each slot are numbered sequentially starting from zero. |
| Logical Interfaces | Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions. VLAN routing interfaces are only used for routing functions. |
| CPU ports | CPU ports are handled by the driver as one or more physical entities located on physical slots. |

2.3.4 Using the “No” Form of a Command

The **no** keyword is a specific form of an existing command and does not represent a new or distinct command. 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** 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.

Only the configuration commands are available in the **no** form.

2.3.5 Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific 7200 Series Managed Switch software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. Table 2-5 describes the command modes and the prompts visible in that mode.

Table 2-5. CLI Command Modes

| Command Mode | Prompt | Mode Description |
|-----------------|------------------|---|
| User EXEC | Switch> | Contains a limited set of commands to view basic system information. |
| Privileged EXEC | Switch# | Allows you to issue any EXEC command, enter the VLAN mode, or enter the Global Configuration mode. |
| Global Config | Switch (Config)# | Groups general setup commands and permits you to make modifications to the running configuration. |
| VLAN Config | Switch (Vlan)# | Groups all the VLAN commands. |

Table 2-5. CLI Command Modes (continued)

| Command Mode | Prompt | Mode Description |
|--------------------------|--------------------------------------|--|
| Interface Config | Switch (Interface <unit/slot/port>)# | Allows you to enable or modify the operation of an interface and provides access to the router interface configuration commands. Use this mode to set up a physical port for a specific logical connection operation. |
| Line Config | Switch (line)# | Allows you to configure various telnet settings and the console interface. |
| Policy Map Config | Switch (Config policy-map)# | Allows you to access the QoS Policy-Map configuration mode to configure the QoS Policy-Map. |
| Policy Class Config | Switch (Config policy-class-map)# | Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria. |
| Class Map Config | Switch (Config class-map)# | Allows you to access the QoS Class-Map configuration mode to configure QoS class maps. |
| Router OSPF Config | Switch (Config router)# | Allows you to access the router OSPF configuration commands. |
| Router RIP Config | Switch (Config router)# | Allows you to access the router RIP configuration commands. |
| MAC Access-list Config | Switch (Config mac-access-list)# | Allows you to create a MAC Access-List and to enter the mode containing Mac Access-List configuration commands. |
| DHCP Pool Config | Switch (Config dhcp-pool)# | Allows you to access the DHCP Pool configuration. |
| Stack Global Config Mode | Switch (Config stack)# | Allows you to access the Stack Global Config Mode. |

Table 2-6 explains how to enter or exit each command mode.

Table 2-6. CLI Mode Access and Exit

| Command Mode | Access Method | Exit or Access Previous Mode |
|--------------------------|--|--|
| User EXEC | This is the first level of access. | To exit, enter <code>logout</code> . |
| Privileged EXEC | From the User EXEC mode, enter <code>enable</code> . | To exit to the User EXEC mode, enter <code>exit</code> or press <code>Ctrl-Z</code> . |
| Global Config | From the Privileged EXEC mode, enter <code>configure</code> . | To exit to the Privileged EXEC mode, enter <code>exit</code> , or press <code>Ctrl-Z</code> . |
| VLAN Config | From the Privileged EXEC mode, enter <code>vlan database</code> . | To exit to the Privileged EXEC mode, enter <code>exit</code> , or press <code>Ctrl-Z</code> . |
| Interface Config | From the Global Config mode, enter <code>interface <slot/port></code> . | To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| Line Config | From the Global Config mode, enter <code>lineconfig</code> . | To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| Policy-Map Config | From the Global Config mode, enter <code>policy-map</code> . | To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| Policy-Class-Map Config | From the Policy Map mode enter <code>class</code> . | To exit to the Policy Map mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| Class-Map Config | From the Global Config mode, enter <code>class-map</code> . | To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| Router OSPF Config | From the Global Config mode, enter <code>router ospf</code> . | To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| Router RIP Config | From the Global Config mode, enter <code>router rip</code> . | To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| MAC Access-list Config | From the Global Config mode enter <code>mac access-list extended <name></code> . | To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| DHCP Pool Config | From the Global Config mode, enter <code>ip dhcp pool <name></code> . | To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |
| Stack Global Config Mode | From the Global Config mode, enter the <code>stack</code> command. | To exit to the Global Config mode, enter the <code>exit</code> command. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> . |

2.3.6 Entering CLI Commands

The 7200 Series Managed Switch supports several features to help you enter commands.

2.3.6.1 Command Completion and Abbreviation

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the SPACEBAR or TAB key to complete the word.

Command abbreviation allows you to execute a command when you type enough letters of a command to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

2.3.6.2 CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 2-7 describes the most common CLI error messages.

Table 2-7. CLI Error Messages

| Message Text | Description |
|---|--|
| % Invalid input detected at '^' marker. | Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized. |
| Command not found / Incomplete command. Use ? to list commands. | Indicates that you did not enter the required keywords or values. |
| Ambiguous command | Indicates that you did not enter enough letters to uniquely identify the command. |

2.3.6.3 CLI Line-Editing Conventions

Table 2-8 describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering **help** from the User or Privileged EXEC modes.

Table 2-8. CLI Editing Conventions

| Key Sequence | Description |
|------------------|---------------------------|
| DEL or Backspace | Delete previous character |
| Ctrl-A | Go to beginning of line |
| Ctrl-E | Go to end of line |
| Ctrl-F | Go forward one character |

Table 2-8. CLI Editing Conventions

| Key Sequence | Description |
|--------------|--|
| Ctrl-B | Go backward one character |
| Ctrl-D | Delete current character |
| Ctrl-U, X | Delete to beginning of line |
| Ctrl-K | Delete to end of line |
| Ctrl-W | Delete previous word |
| Ctrl-T | Transpose previous character |
| Ctrl-P | Go to previous line in history buffer |
| Ctrl-R | Rewrites or pastes the line |
| Ctrl-N | Go to next line in history buffer |
| Ctrl-Y | Prints last deleted character |
| Ctrl-Q | Enables serial flow |
| Ctrl-S | Disables serial flow |
| Ctrl-Z | Return to root command prompt |
| Tab, <SPACE> | Command-line completion |
| Exit | Go to next lower command prompt |
| ? | List available commands, keywords, or parameters |

2.3.7 Using CLI Help

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
(switch) >?
```

| | |
|--------|---|
| enable | Enter into user privilege mode. |
| help | Display help for various special keys. |
| logout | Exit this session. Any unsaved changes are lost. |
| ping | Send ICMP echo packets to a specified IP address. |
| show | Display switch options and settings. |

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
(switch) #network ?
```

| | |
|-----------|---|
| javamode | Enable/Disable. |
| parms | Configure Network Parameters of the router. |
| protocol | Select DHCP, BootP, or None as the network config protocol. |
| mgmt_vlan | Configure the Management VLAN ID of the switch. |

If the help output shows a parameter in angle brackets, you must replace the parameter with a value.

```
(switch) #network parms ?
```

```
<ipaddr>                Enter the IP Address.
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>                    Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(switch) #show m?
```

```
mac-addr-table           mac-address-table           monitor
```

2.3.8 Accessing the CLI

You can access the CLI by using a direct console connection or by using a telnet or SSH connection from a remote management host.

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address and subnet mask. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP or DHCP server on your network. For more information, see [Section 3.1 “Network Interface Commands” on page 3-1](#).

Chapter 3

Administrative Access Commands

This section describes the management access and basic port configuration commands available in the 7200 Series Managed Switch CLI.

This section contains the following topics:

- [Section 3.1 “Network Interface Commands” on page 3-1](#)
- [Section 3.3 “Console Port Access Commands” on page 3-7](#)
- [Section 3.4 “Telnet Commands” on page 3-10](#)
- [Section 3.5 “Secure Shell \(SSH\) Command” on page 3-15](#)
- [Section 3.6 “Hypertext Transfer Protocol \(HTTP\) Commands” on page 3-17](#)
- [Section 3.7 “User Account Commands” on page 3-20](#)

The commands in this section are divided into two 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.

To manage the device by using SNMP, see [“SNMP Commands” in Chapter 10](#).

3.1 Network Interface Commands

This section describes the commands you use to configure a logical interface for management access.

3.1.1 enable

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

| | |
|---------------|---------------------|
| Format | <code>enable</code> |
| Mode | User EXEC |

3.1.2 network parms (parameter)

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

| | |
|---------------|--|
| Format | <code>network (parms parameter) <ipaddr> <netmask> [<i><gateway></i>]</code> |
| Mode | Privileged EXEC |

3.1.3 network mgmt_vlan

This command configures the Management VLAN ID.

| | |
|----------------|---|
| Default | 1 |
| Format | <code>network mgmt_vlan <1-4069></code> |
| Mode | Privileged EXEC |

3.1.3.1 no network mgmt_vlan

This command sets the Management VLAN ID to the default.

| | |
|---------------|-----------------------------------|
| Format | <code>no network mgmt_vlan</code> |
| Mode | Privileged EXEC |

3.1.4 network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you modify this value, the change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

| | |
|----------------|---|
| Default | none |
| Format | <code>network protocol {none bootp dhcp}</code> |
| Mode | Privileged EXEC |

3.1.5 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 |
| Modes | Privileged EXEC User EXEC |
| IP Address | The IP address of the interface. The factory default value is 0.0.0.0 |
| Subnet Mask | The IP subnet mask for this interface. The factory default value is 0.0.0.0 |
| Default Gateway | The default gateway for this IP interface. The factory default value is 0.0.0.0 |
| Burned In MAC Address | The burned in MAC address used for in-band connectivity. |
| Locally Administered MAC Address | If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol. |
| MAC Address Type | Specifies which MAC address should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address. |

**Network
Configuration
Protocol Current**

Indicates which network protocol is being used. The options are bootp | dhcp | none.

Java Mode

Specifies if the switch should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is disabled.

Web Mode

Specifies if the switch should allow access to the Web Interface.

3.2 Configuring the Switch Management CPU (ezconfig)

| | |
|---------------|-----------------|
| Format | ezconfig |
| Mode | Privileged EXEC |

To manage the switch via the web GUI or telnet, an IP address needs to be assigned to the switch management CPU. Whereas there are CLI commands that can be used to do this, **ezconfig** simplifies the task. The tool is applicable to all NETGEAR 7000-series managed switches, and allows you to configure the following parameters:

1. The administrator's user password and administrator-enable password
2. Management CPU IP address and network mask
3. System name and location information

The tool is interactive and uses questions to guide you through the steps required to perform its task. At the end of the session, it will ask you if you want to save the changed information. To see exactly what has been changed by ezconfig at the end of the session, use the **show running-config** command.

To perform any switch configuration other than the items listed above, use other CLI commands or the Web GUI.

The following is an example of an **ezconfig** session.

```
NETGEAR EZ Configuration Utility
-----
Hello and Welcome!

This utility will walk you thru assigning the IP address for the switch
management CPU. It will allow you to save the changes at the end. After
the session, simply use the newly assigned IP address to access the Web
GUI using any public domain Web browser.

Admin password not defined. Do you want to change the password?
(Y/N/Q)  y
Enter new password:*****
Confirm new password:*****
Password Changed!

The 'enable' password required for switch configuration via the command
line interface is currently not configured. Do you wish to change it (Y/
N/Q)?  y

Enter new password:*****
Confirm new password:*****
Password Changed!

Assigning an IP address to your switch management

Current IP Address Configuration
-----
IP address: 0.0.0.0
Subnet mask: 0.0.0.0
Gateway address: 0.0.0.0

Would you like to assign an IP address now (Y/N/Q)?  y

IP Address: 10.10.10.1
Subnet mask: 255.255.255.0
Gateway address: 10.10.10.10

Do you want to assign switch name and location information (Y/N/Q)?  y

System Name: testunit1
System Location: testlab
System Contact: Bud Lightyear
```

```
There are changes detected, do you wish to save the changes permanently
(Y/N)?  y

The configuration changes have been saved succesfully.  Please enter
'show running-config' to see the final configuration.

Thanks for using EzConfig!
```

3.3 Console Port Access Commands

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

3.3.1 configuration

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

| | |
|---------------|----------------------------|
| Format | <code>configuration</code> |
| Mode | Privileged EXEC |

3.3.2 lineconfig

This command gives you access to the Line Config mode, which allows you to configure various telnet settings and the console port.

| | |
|---------------|-------------------------|
| Format | <code>lineconfig</code> |
| Mode | Global Config |

3.3.3 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 |

3.3.3.1 no serial baudrate

This command sets the communication rate of the terminal interface.

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

3.3.4 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 |

3.3.4.1 no serial timeout

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

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

3.3.5 show serial

This command displays serial communication settings for the switch.

| | |
|--|---|
| Format | <code>show serial</code> |
| Modes | Privileged EXEC 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 (bps) | 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 (bits) | 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. |

3.4 Telnet Commands

This section describes the commands you use to configure and view telnet settings. You can use telnet to manage the device from a remote management host.

3.4.1 telnet

This command establishes a new outbound telnet connection to a remote host. The *host* value must be a valid IP address. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If *[debug]* is used, the current telnet options enabled is displayed. The optional *line* parameter sets the outbound telnet operational mode as 'linemode', where by default, the operational mode is 'character mode'. The *noecho* option disables local echo.

| | |
|---------------|---|
| Format | <code>telnet <host> <port> [debug] [line] [noecho]</code> |
| Modes | Privileged EXEC User EXEC |

3.4.2 transport input 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 the session.

| | |
|----------------|-------------------------------------|
| Default | enabled |
| Format | <code>transport input telnet</code> |
| Mode | Line Config |

3.4.2.1 no transport input telnet

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

| | |
|---------------|--|
| Format | <code>no transport input telnet</code> |
| Mode | Line Config |

3.4.3 transport output telnet

This command regulates new outbound telnet connections. If enabled, new outbound telnet sessions can be established until it reaches the maximum number of simultaneous outbound telnet sessions allowed. If disabled, no new outbound telnet session can be established. An established session remains active until the session is ended or an abnormal network error ends it.

| | |
|----------------|--------------------------------------|
| Default | enabled |
| Format | <code>transport output telnet</code> |
| Mode | Line Config |

3.4.3.1 no transport output telnet

This command disables new outbound telnet connections. If disabled, no new outbound telnet connection can be established.

| | |
|---------------|---|
| Format | <code>no transport output telnet</code> |
| Mode | Line Config |

3.4.4 session-limit

This command specifies the maximum number of simultaneous outbound telnet sessions. A value of 0 indicates that no outbound telnet session can be established.

| | |
|----------------|--|
| Default | 5 |
| Format | <code>session-limit <0-5></code> |
| Mode | Line Config |

3.4.4.1 no session-limit

This command sets the maximum number of simultaneous outbound telnet sessions to the default value.

| | |
|---------------|-------------------------------|
| Format | <code>no session-limit</code> |
| Mode | Line Config |

3.4.5 session-timeout

This command sets the telnet session timeout value. The timeout value unit of time is minutes. A value of 0 indicates that a session remains active indefinitely.

| | |
|----------------|--|
| Default | 0 |
| Format | <code>session-timeout <0-160></code> |
| Mode | Line Config |

3.4.5.1 no session-timeout

This command sets the telnet session timeout value to the default. The timeout value unit of time is minutes.

| | |
|---------------|---------------------------------|
| Format | <code>no session-timeout</code> |
| Mode | Line Config |

3.4.6 telnetcon maxsessions

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

| | |
|----------------|--|
| Default | 5 |
| Format | <code>telnetcon maxsessions <0-5></code> |
| Mode | Privileged EXEC |


3.4.6.1 no telnetcon maxsessions

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

| | |
|---------------|---------------------------------------|
| Format | <code>no telnetcon maxsessions</code> |
| Mode | Privileged EXEC |

3.4.7 telnetcon timeout


This command sets the telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value you set, which ranges from 1-160 minutes.

| | |
|---|--|
|  | Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration. |
|---|--|

| | |
|----------------|--|
| Default | 5 |
| Format | <code>telnetcon timeout <1-160></code> |
| Mode | Privileged EXEC |

3.4.7.1 no telnetcon timeout

This command sets the telnet connection session timeout value to the default.

| | |
|---|--|
|  | Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration. |
|---|--|

| | |
|---------------|-----------------------------------|
| Format | <code>no telnetcon timeout</code> |
| Mode | Privileged EXEC |

3.4.8 show telnet

This command displays the current outbound telnet settings.

| | |
|--------------------------------------|---|
| Format | <code>show telnet</code> |
| Modes | Privileged EXEC User EXEC |
| Outbound Telnet Login Timeout | Indicates the number of minutes an outbound telnet session is allowed to remain inactive before being logged off. |

**Maximum Number
of Outbound
Telnet Sessions**

Indicates the number of simultaneous outbound telnet connections allowed.

**Allow New
Outbound Telnet
Sessions**

Indicates whether outbound telnet sessions are allowed.

3.4.9 show telnetcon

This command displays telnet settings.

Format

show telnetcon

Modes

Privileged EXEC
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. May be specified as a number from 1 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.

3.5 Secure Shell (SSH) Command

This section describes the commands you use to configure SSH access to the switch. Use SSH to access the switch from a remote management host.



Note: The system allows a maximum of 5 SSH sessions.

3.5.1 ip ssh

This command is used to enable SSH.

| | |
|----------------|---------------------|
| Default | disabled |
| Format | <code>ip ssh</code> |
| Mode | Privileged EXEC |

3.5.1.1 no ip ssh

This command is used to disable SSH.

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

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

3.5.3 sshcon maxsessions

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

| | |
|----------------|---|
| Default | 5 |
| Format | <code>sshcon maxsessions <0-5></code> |
| Mode | Privileged EXEC |

3.5.3.1 no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

| | |
|---------------|------------------------------------|
| Format | <code>no sshcon maxsessions</code> |
| Mode | Privileged EXEC |

3.5.4 sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

| | |
|----------------|---|
| Default | 5 |
| Format | <code>sshcon timeout <1-160></code> |
| Mode | Privileged EXEC |

3.5.4.1 no sshcon timeout

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

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

| | |
|---------------|--------------------------------|
| Format | <code>no sshcon timeout</code> |
| Mode | Privileged EXEC |

3.5.5 show ip ssh

This command displays the ssh settings.

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

3.6 Hypertext Transfer Protocol (HTTP) Commands

This section describes the commands you use to configure HTTP access to the switch. Access to the switch by using a Web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the Web.

3.6.1 ip http secure-port

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

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

3.6.1.1 no ip http secure-port

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

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

3.6.2 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 | <code>ip http secure-protocol [SSL3] [TLS1]</code> |
| Mode | Privileged EXEC |

3.6.3 ip http secure-server

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

| | |
|----------------|------------------------------------|
| Default | disabled |
| Format | <code>ip http secure-server</code> |
| Mode | Privileged EXEC |

3.6.3.1 no ip http secure-server

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

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

3.6.4 ip http server

This command enables access to the switch through the Web interface. When access is enabled, you can login to the switch from the Web interface. When access is disabled, you cannot login to the switch's Web server. Disabling the Web interface takes effect immediately and affects all interfaces.

| | |
|----------------|-----------------------------|
| Default | enabled |
| Format | <code>ip http server</code> |
| Mode | Privileged EXEC |

3.6.4.1 no ip http server

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

| | |
|---------------|--------------------------------|
| Format | <code>no ip http server</code> |
| Mode | Privileged EXEC |

3.6.5 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 |

3.6.5.1 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 |

3.6.6 show ip http

This command displays the http settings for the switch.

| | |
|--|--|
| Format | show ip http |
| Mode | Privileged EXEC |
| Secure-Server Administrative Mode | Indicates whether the administrative mode of secure HTTP is enabled or disabled. |
| Secure Protocol Level | Possible values are 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. |

3.7 User Account Commands

This section describes the commands you use to add, manage, and delete system users. The 7200 Series Managed Switch has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.



Note: You cannot delete the admin user, and there is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

3.7.1 users name

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

You can define up to six user names.

Format `users name <username>`

Mode Global Config

3.7.1.1 no users name

This command removes a user account.

Format `no users name <username>`

Mode Global Config



Note: You cannot delete the “admin” user account.

3.7.2 users passwd

Use this command to change a password. Passwords are a maximum of eight alphanumeric characters. If a user is authorized for authentication or encryption is enabled, the password length must be at least eight alphanumeric characters. The username and password are not case-sensitive. When you change a password, a prompt asks for the old password. If there is no password, press enter.

| | |
|----------------|--------------------------------|
| Default | no password |
| Format | users passwd <username> |
| Mode | Global Config |

3.7.2.1 no users passwd

This command sets the password of an existing user to blank. When you change a password, a prompt asks for the old password. If there is no password, press enter.

| | |
|---------------|-----------------------------------|
| Format | no users passwd <username> |
| Mode | Global Config |

3.7.3 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 applies. The default is **readwrite** for the “admin” user and **readonly** for all other users

| | |
|----------------|--|
| Default | admin - readwrite; other - readonly |
| Format | users snmpv3 accessmode <username> {readonly / readwrite} |
| Mode | Global Config |

3.7.3.1 no users snmpv3 accessmode

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

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

3.7.4 users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are **none**, **md5** or **sha**. If you specify **md5** or **sha**, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The *<username>* is the user name associated with the authentication protocol.

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

3.7.4.1 no users snmpv3 authentication

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

| | |
|---------------|--|
| Format | users snmpv3 authentication <i><username></i> |
| Mode | Global Config |

3.7.5 users snmpv3 encryption

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

If you select **des**, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the **des** protocol but do not provide a key, the user is prompted for the key. When you use the **des** protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select **none**, you do not need to provide a key.

The *<username>* value is the login user name associated with the specified encryption.

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

3.7.5.1 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 | <code>no users snmpv3 encryption <username></code> |
| Mode | Global Config |

3.7.6 show login session

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

| | |
|------------------------|--|
| Format | <code>show login session</code> |
| Mode | Privileged EXEC |
| ID | Login Session ID |
| User Name | The name the user will use to login using the serial port or Telnet. |
| 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. |

3.7.7 show users

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

| | |
|--------------------|---|
| Format | <code>show users</code> |
| Mode | Privileged EXEC |
| User Name | The name the user enters to login using the serial port, Telnet or Web. |
| Access Mode | Shows whether the user 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 Access
Mode**

This field displays the SNMPv3 Access Mode. If the value is set to **ReadWrite**, the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to **Read-only**, the SNMPv3 user is only 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.

3.7.8 disconnect

This command closes a telnet session.

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

Chapter 4

Port and System Setup Commands

This section describes general port and system setup commands available in the 7200 Series Managed Switch CLI.

This section contains the following topics:

- [Section 4.1 “Port Configuration Commands” on page 4-1](#)
- [Section 4.2 “Pre-login Banner and System Prompt Commands” on page 4-9](#)
- [Section 4.3 “Simple Network Time Protocol \(SNTP\) Commands” on page 4-11](#)
- [Section 4.4 “MAC Address and MAC Database Commands” on page 4-16](#)
- [Section 4.5 “DNS Client Commands” on page 4-25](#)

The commands in this section are in one of three 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.

4.1 Port Configuration Commands

This section describes the commands you use to view and configure port settings.

4.1.1 interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface.

| | |
|---------------|--|
| Format | <code>interface <slot/port></code> |
| Mode | Global Config |

4.1.2 interface range

This command gives you access to a range of port interfaces, allowing the same port configuration to be applied to a set of ports.

| | |
|---------------|--|
| Format | interface range <slot/port>-<slot/port> |
| Mode | Global Config |

4.1.3 interface vlan

This command gives you access to to the vlan virtual interface mode, which allows certain port configurations (for example, the IP address) to be applied to the VLAN interface. Type a question mark (?) after entering the interface configuration mode to see the available options.

| | |
|---------------|---------------------------------|
| Format | interface vlan <vlan id> |
| Mode | Global Config |

4.1.4 interface lag

This command gives you access to the LAG (link aggregation, or port channel) virtual interface, which allows certain port configurations to be applied to the LAG interface. Type a question mark (?) after entering the interface configuration mode to see the available options.



Note: The IP address cannot be assigned to a LAG virtual interface. The interface must be put under a VLAN group and an IP address assigned to the VLAN group.

| | |
|---------------|-------------------------------|
| Format | interface lag <lag id> |
| Mode | Global Config |

4.1.5 cablestatus

This command tests the status of the cable attached to an interface.

| | |
|---------------|--------------------------------|
| Format | cablestatus <slot/port> |
| Mode | Privileged EXEC |


4.1.6 auto-negotiate

This command enables automatic negotiation on a port.

| | |
|----------------|-----------------------|
| Default | enabled |
| Format | auto-negotiate |
| Mode | Interface Config |

4.1.6.1 no auto-negotiate

This command disables automatic negotiation on a port.

| | |
|---|--|
|  | Note: Automatic sensing is disabled when automatic negotiation is disabled. |
|---|--|

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

4.1.7 auto-negotiate all

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

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

4.1.7.1 no auto-negotiate all

This command disables automatic negotiation on all ports.

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

4.1.8 mtu

This command sets the maximum transmission unit (MTU) size, in bytes, for physical and port-channel (LAG) interfaces. For the standard implementation, the MTU size is a valid integer between 1522 - 9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.



Note: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see [Section 14.2.9 “ip mtu” on page 14-11](#).

| | |
|----------------|------------------------------------|
| Default | 1518 (untagged) |
| Format | <code>mtu <1518-9216></code> |
| Mode | Interface Config |

4.1.8.1 no mtu

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

| | |
|---------------|---------------------|
| Format | <code>no mtu</code> |
| Mode | Interface Config |

4.1.9 shutdown

This command disables a port.




Note: You can use the **shutdown** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

| | |
|----------------|-----------------------|
| Default | enabled |
| Format | <code>shutdown</code> |
| Mode | Interface Config |

4.1.9.1 no shutdown


This command enables a port.

| | |
|---|--|
|  | Note: You can use the no shutdown command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces. |
|---|--|

| | |
|---------------|--------------------|
| Format | no shutdown |
| Mode | Interface Config |

4.1.10 shutdown all


This command disables all ports.

| | |
|---|---|
|  | Note: You can use the shutdown command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces. |
|---|---|

| | |
|----------------|---------------------|
| Default | enabled |
| Format | shutdown all |
| Mode | Global Config |

4.1.10.1 no shutdown all

This command enables all ports.

| | |
|---|---|
|  | Note: You can use the shutdown command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces. |
|---|---|

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

4.1.11 speed

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

| | |
|---------------|---|
| Format | speed {<100 10> <half-duplex full-duplex>} |
| Mode | Interface Config |

Acceptable values are:

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

4.1.12 speed all

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

| | |
|---------------|---|
| Format | speed all {<100 10> <half-duplex full-duplex>} |
| Mode | Global Config |

Acceptable values are:

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

4.1.13 monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). To enable port monitoring, you must add a source interface, destination interface, and enable the mode. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

| | |
|---------------|---|
| Format | monitor session <session-id> {source interface <slot/port> destination interface <slot/port> mode} |
| Mode | Global Config |

4.1.13.1 no monitor session

This command removes the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, the user must manually add the port to any desired VLANs.




Note: This command sets the monitor session (port monitoring) mode to disable and removes the source and destination interfaces.

| | |
|---------------|--|
| Format | <code>no monitor session <session-id></code> |
| Mode | Global Config |

4.1.14 no monitor

This command removes all the source ports and a destination port and restores the default value for mirroring session mode for all the configured sessions.

| | |
|---|---|
|  | <p>Note: This is a stand-alone “no” command. This command does not have a “normal” form.</p> |
|---|---|

| | |
|----------------|-------------------------|
| Default | enabled |
| Format | <code>no monitor</code> |
| Mode | Global config |

4.1.15 show monitor session

This command displays the port monitoring information for the system. The *<sessionid>* parameter is an integer.

| | |
|----------------------|---|
| Format | <code>show monitor session <sessionid></code> |
| Mode | Privileged EXEC |
| Session ID | The session identifying number. |
| Admin Mode | Indicates whether the Port Monitoring feature is enabled or disabled. The possible values are enable and disable. |
| Probe Port | The interface configured as the probe port. |
| Mirrored Port | The interface configured as the mirrored port. |

4.1.16 show port

This command displays port information.

| | |
|------------------|---|
| Format | <code>show port {<slot/port> all}</code> |
| Mode | Privileged EXEC |
| Interface | Valid slot and port number separated by forward slashes. |
| 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 is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines 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. |

4.1.17 show port protocol

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

| | |
|---------------------|---|
| Format | <code>show port protocol {<groupid> all}</code> |
| Mode | Privileged EXEC |
| Group Name | This field displays the group name of an entry in the Protocol-based VLAN table. |
| Group ID | This field displays the group identifier of the protocol group. |
| Protocol(s) | This field indicates the type of protocol(s) for this group. |
| VLAN | This field indicates the VLAN associated with this Protocol Group. |
| Interface(s) | This field lists the slot/port interface(s) that are associated with this Protocol Group. |

4.1.18 show port status

This command displays the output with current port attributes and operational status.

| | |
|-----------------------------|--|
| Format | show port status {<slot/port> all} |
| Mode | Privileged Exec |
| Interface | Valid slot and port number separated by forward slashes. |
| Media Type | “Copper” or “Fiber” for combo port. |
| Physical Mode | Either “Auto” or fixed speed and duplex mode. |
| Physical Status | The actual speed and duplex mode |
| Link Status | Whether the link is Up or Down. |
| Loop Status | Whether the port is in loop state or not. |
| Partner Flow Control | Whether the remote side is using flow control or not. |

4.2 Pre-login Banner and System Prompt Commands

This section describes the commands you use configure the pre-login banner and the system prompt. The pre-login banner is the text that displays before you login at the **user:** prompt.

4.2.1 copy

The **copy** command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using TFTP, Xmodem, Ymodem, or Zmodem.

| | |
|----------------|---|
| Default | none |
| Format | copy <Code Sample Variable><tftp://<ipaddr>/<filepath>/<filename>><Code Sample Variable> nvrn:clibanner copy nvrn:clibanner <Code Sample Variable><tftp://<ipaddr>/<filepath>/<filename>><Code Sample Variable> |
| Mode | Privileged EXEC |

4.2.2 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

4.3 Simple Network Time Protocol (SNTP) Commands

This section describes the commands you use to automatically configure the system time and date by using SNTP.

4.3.1 sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where `<poll-interval>` can be a value from 6 to 16.

| | |
|----------------|--|
| Default | 6 |
| Format | <code>sntp broadcast client poll-interval <poll-interval></code> |
| Mode | Global Config |

4.3.1.1 no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

| | |
|---------------|---|
| Format | <code>no sntp broadcast client poll-interval</code> |
| Mode | Global Config |

4.3.2 sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

| | |
|----------------|---|
| Default | disabled |
| Format | <code>sntp client mode [broadcast unicast]</code> |
| Mode | Global Config |

4.3.2.1 sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

| | |
|---------------|----------------------------------|
| Format | <code>no sntp client mode</code> |
| Mode | Global Config |

4.3.3 sntp client port

This command sets the SNTP client port id to a value from 1-65535.

| | |
|----------------|--|
| Default | 123 |
| Format | <code>sntp client port <portid></code> |
| Mode | Global Config |

4.3.3.1 no sntp client port

This command resets the SNTP client port back to its default value.

| | |
|---------------|----------------------------------|
| Format | <code>no sntp client port</code> |
| Mode | Global Config |

4.3.4 sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where *<poll-interval>* can be a value from 6 to 16. When the value of the poll interval is from 17 to 16284, the value is interpreted to be in units of seconds.

| | |
|----------------|--|
| Default | 6 |
| Format | <code>sntp unicast client poll-interval <poll-interval></code> |
| Mode | Global Config |

4.3.4.1 no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

| | |
|---------------|---|
| Format | <code>no sntp unicast client poll-interval</code> |
| Mode | Global Config |

4.3.5 sntp unicast client poll-timeout

This command sets the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

| | |
|----------------|--|
| Default | 5 |
| Format | <code>sntp unicast client poll-timeout <poll-timeout></code> |
| Mode | Global Config |

4.3.5.1 no sntp unicast client poll-timeout

This command resets the poll timeout for SNTP unicast clients to its default value.

| | |
|---------------|--|
| Format | <code>no sntp unicast client poll-timeout</code> |
| Mode | Global Config |

4.3.6 sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

| | |
|----------------|--|
| Default | 1 |
| Format | <code>sntp unicast client poll-retry <poll-retry></code> |
| Mode | Global Config |

4.3.6.1 no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

| | |
|---------------|--|
| Format | <code>no sntp unicast client poll-retry</code> |
| Mode | Global Config |

4.3.7 sntp multicast client poll-interval

This command will set the poll interval for SNTP multicast clients in seconds as a power of two where *<poll-interval>* can be a value from 6 to 16.

| | |
|----------------|--|
| Default | 6 |
| Format | <code>sntp multicast client poll-interval <poll-interval></code> |
| Mode | Global Config |

4.3.7.1 no sntp multicast client poll-interval

This command resets the poll interval for SNTP multicast clients to its default value.

| | |
|---------------|---|
| Format | <code>no sntp multicast client poll-interval</code> |
| Mode | Global Config |

4.3.8 sntp server

This command configures an SNTP server (a maximum of three). The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

| | |
|---------------|--|
| Format | sntp server <ipaddress> [<priority> [<version> [<portid>]]] |
| Mode | Global Config |

4.3.8.1 no sntp server

This command deletes an server from the configured SNTP servers.

| | |
|---------------|--|
| Format | no sntp server remove <ipaddress> |
| Mode | Global Config |

4.3.9 show sntp

This command is used to display SNTP settings and status.

| | |
|----------------------------|--|
| Format | show sntp |
| Mode | Privileged EXEC |
| Last Update Time | Time of last clock update. |
| Last Attempt Time | Time of last transmit query (in unicast mode). |
| Last Attempt Status | Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode). |
| Broadcast Count | Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot. |
| Multicast Count | Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot |

4.3.10 show sntp client

This command is used to display SNTP client settings.

| | |
|---------------|-------------------------|
| Format | show sntp client |
| Mode | Privileged EXEC |

Client Supported Modes

Supported SNTP Modes (Broadcast, Unicast, or Multicast).

SNTP Version

The highest SNTP version the client supports

Port

SNTP Client Port

Client Mode

Configured SNTP Client Mode

Poll Interval

Poll interval value for SNTP clients in seconds as a power of two.

Poll Timeout

Poll timeout value in seconds for SNTP clients.

Poll Retry

Poll retry value for SNTP clients.

4.3.11 show sntp server

This command is used to display SNTP server settings and configured servers.

Format

show sntp server

Mode

Privileged EXEC

Server IP

Address

IP Address of configured SNTP Server

Server Type

Address Type of Server.

Server Stratum

Claimed stratum of the server for the last received valid packet.

Server Reference

ID

Reference clock identifier of the server for the last received valid packet.

Server Mode

SNTP Server mode.

Server Max

Entries

Total number of SNTP Servers allowed.

Server Current

Entries

Total number of SNTP configured.

For each configured server:

IP Address

IP Address of configured SNTP Server.

Address Type

Address Type of configured SNTP server.

Priority

IP priority type of the configured server.

Version

SNTP Version number of the server. The protocol version used to query the server in unicast mode.

| | |
|--------------------------------|--|
| Port | Server Port Number |
| Last Attempt Time | Last server attempt time for the specified server. |
| Last Attempt Status | Last server attempt status for the server. |
| Total Unicast Requests | Number of requests to the server. |
| Failed Unicast Requests | Number of failed requests from server. |

4.3.12 clock timezone

When using SNTP/NTP time servers to update the switch's clock, the time data received from the server is based on Coordinated Universal Time (UTC) which is the same as Greenwich Mean Time (GMT). This may not be the time zone in which the switch is located. Use the **clock timezone** command to configure a time zone specifying the number of hours and optionally the number of minutes difference from UTC. To set the switch clock to UTC, use the **no** form of the command.

| | |
|-------------------|---|
| Format | <code>clock timezone zone-name +/-hours-offset [+/-minutes-offset]</code> <code>[no] clock timezone</code> |
| Parameters | <i>Zone name</i> A name to associate with the time zone <i>Hours-offset</i> Number of hours difference with UTC <i>Minutes-offset</i> Number of minutes difference with UTC |
| Mode | Global Config |
| Default | <code>[no] clock timezone</code> |

4.4 MAC Address and MAC Database Commands

This section describes the commands you use to configure and view information about the system MAC address and the MAC address table.

4.4.1 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 | <code>network mac-address <macaddr></code> |
| Mode | Privileged EXEC |

4.4.2 network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

| | |
|----------------|--|
| Default | burnedin |
| Format | <code>network mac-type {local burnedin}</code> |
| Mode | Privileged EXEC |

4.4.2.1 no network mac-type

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

| | |
|---------------|----------------------------------|
| Format | <code>no network mac-type</code> |
| Mode | Privileged EXE |

4.4.3 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 |

4.4.3.1 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 |

4.4.4 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 |

4.4.4.1 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 |

4.4.5 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 |
| Mode | Global Config |

4.4.5.1 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 |
| Mode | Global Config |

4.4.6 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 |

4.4.6.1 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 | <code>no macfilter addsrc <macaddr> <vlanid></code> |
| Mode | Interface Config |

4.4.7 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>. You must specify the <macaddr> parameter 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 | <code>macfilter addsrc all</code> |
| Mode | Global Config |

4.4.7.1 no macfilter addsrc all

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 | <code>no macfilter addsrc all</code> |
| Mode | Global Config |

4.4.8 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 | The forwarding database ID (<i>fdbid</i>) indicates which forwarding database's aging timeout is being configured. Use the <i>all</i> option to configure the agetime of all forwarding databases. |

4.4.8.1 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. |

4.4.9 show forwardingdb agetime

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

| | |
|-------------------------|---|
| Default | all |
| Format | <code>show forwardingdb agetime [fdbid / all]</code> |
| Mode | Privileged EXEC |
| Forwarding DB ID | 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. |
| Agetime | In an IVL system, this parameter displays the address aging timeout for the associated forwarding database. |

4.4.10 show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

| | |
|--------------------|---|
| Format | <code>show mac-address-table multicast <macaddr></code> |
| Mode | Privileged EXEC |
| MAC Address | A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as a MAC address and VLAN ID combination of 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. |

4.4.11 show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you select *<all>*, all the Static MAC Filters in the system are displayed. If you supply a value for *<macaddr>*, you must also enter a value for *<vlanid>*, and the system displays Static MAC Filter information only for that MAC address and VLAN.

| | |
|----------------------------|---|
| Format | <code>show mac-address-table static {<macaddr> <vlanid> / all}</code> |
| Mode | Privileged EXEC |
| MAC Address | Is the MAC Address of the static MAC filter entry. |
| VLAN ID | Is the VLAN ID of the static MAC filter entry. |
| Source Port(s) | Indicates the source port filter set's slot and port(s). |
| Destination Port(s) | Indicates the destination port filter set's slot and port(s). |

4.4.12 show mac-address-table staticfiltering

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

| | |
|--------------------|--|
| Format | <code>show mac-address-table staticfiltering</code> |
| Mode | Privileged EXEC |
| Mac Address | A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. |
| Type | 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:). |

4.4.13 show mac-address-table stats

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

| | |
|------------------------------------|---|
| Format | <code>show mac-address-table stats</code> |
| Mode | Privileged EXEC |
| Total Entries | Displays the total number of entries that can possibly be in the Multicast Forwarding Database table. |
| Most MFDB Entries Ever Used | 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 | Displays the current number of entries in the MFDB. |

4.5 DNS Client Commands

The Domain Name System (DNS) is an Internet directory service. DNS is used to translate domain names to IP addresses. A DNS Client (often referred to as a resolver) uses a defined protocol to obtain resource data from name servers on its network.

The DNS Client component must be globally enabled or disabled. When the client is enabled, it provides a hostname lookup service to other components in the switch. The client contacts one or more DNS servers to resolve a hostname to an IP address. The DNS servers list is configured by providing an IP address for each DNS name server, and server precedence is determined by the order in which the servers are added to this list. A default domain name can be configured, which defines the domain to use when performing a lookup on an unqualified hostname. Static hostname-to-address mappings can be added and removed from the local cache.

The DNS client supports 128 entries in the DNS cache. Any application component requiring a DNS lookup may request services from the DNS client. When the DNS client is administratively disabled the local cache is purged. Changes to the name server configuration do not affect the cache. If a stacking switchover occurs, the new Master unit begins with a cleared cache.

The following applications support domain name in addition to the IP address format:

Radius

DHCP Relay

SNTP

SNMP

TFTP

SYSLOG

Ping

UDP Relay

4.5.1 ip domain-lookup

To enable the IP Domain Naming System (DNS)-based host name-to-address translation, use the **ip domain-lookup** global configuration command. To disable the DNS, use the **no** form of this command

| | |
|----------------|------------------------------------|
| Format | <code>[no] ip domain-lookup</code> |
| Mode | Global Config |
| Default | enabled |

4.5.2 ip domain-name

To define a default domain name (*<name>*) that the software uses to complete unqualified host names (names without a dotted-decimal domain name), use the **ip domain-name** global configuration command. To remove default domain name, use the **no** form of this command.

Default domain used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name.

<name> is a string of 1 to 255 characters.

| | |
|---------------|--|
| Format | <code>ip domain-name name</code> <code>no ip domain-name</code> |
| Mode | Global Config |

4.5.3 ip name-server

To set the available name servers, use the **ip name-server** global configuration command. *<server-address>* is IP addresses of the name server. Up to 8 servers can be defined in one command, or by using multiple commands. The preference of the servers is determined by the order they were entered. To remove a name server, use the **no** form of this command.

| | |
|---------------|--|
| Format | <code>[no] ip name-server server-address1 [server-address2 ... server-address8]</code> |
| Mode | Global Config |

4.5.4 ip host

To define static host name *<name>* to IP address *<address>* mapping in the host cache, use the **ip host** global configuration command. The *<name>* string is from 1 to 255 characters. To remove the name-to-address mapping, use the **no** form of this command.

Format `[no] ip host name address`

Mode Global Config

4.5.5 clear host

To delete entries from the host name-to-address cache, use the **clear host** Privileged EXEC command.

Format `clear host [name | *]`

Mode Privileged EXEC Mode

4.5.6 show hosts

To display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses, use the **show hosts** EXEC command.

Format `show hosts [name]`

Mode Privileged EXEC Mode

Chapter 5

Spanning Tree Protocol Commands

This section describes the spanning tree protocol (STP) commands available in the 7200 Series Managed Switch CLI. STP helps prevent network loops, duplicate messages, and network instability.

The STP Commands section includes the following topics:

- [Section 5.1 “STP Configuration Commands” on page 5-1](#)
- [Section 5.2 “STP Show Commands” on page 5-10](#)

The commands in this section are in one of two 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.

5.1 STP Configuration Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP).



Note: STP is enabled by default. If STP is disabled, the system does not generate BPDU messages.

5.1.1 spanning-tree

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

| | |
|----------------|----------------------|
| Default | enabled |
| Format | spanning-tree |
| Mode | Global Config |

5.1.1.1 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 |

5.1.2 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 |

5.1.2.1 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 |

5.1.3 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 up to 32 characters.

| | |
|----------------|--|
| Default | base MAC address in hexadecimal notation |
| Format | spanning-tree configuration name <name> |
| Mode | Global Config |

5.1.3.1 no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

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

5.1.4 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 | <code>spanning-tree configuration revision <0-65535></code> |
| Mode | Global Config |

5.1.4.1 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 | <code>no spanning-tree configuration revision</code> |
| Mode | Global Config |

5.1.5 spanning-tree edgeport

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

| | |
|---------------|-------------------------------------|
| Format | <code>spanning-tree edgeport</code> |
| Mode | Interface Config |

5.1.5.1 no spanning-tree edgeport

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

| | |
|---------------|--|
| Format | <code>no spanning-tree edgeport</code> |
| Mode | Interface Config |

5.1.6 spanning-tree edgeport all

This command specifies that every port is an Edge Port within the common and internal spanning tree. This allows all ports to transition to Forwarding State without delay.

| | |
|---------------|---|
| Format | <code>spanning-tree edgeport all</code> |
| Mode | Global Config |

5.1.6.1 no spanning-tree edgeport all

This command disables Edge Port mode for all ports within the common and internal spanning tree.

| | |
|---------------|---|
| Format | <code>spanning-tree edgeport all</code> |
| Mode | Global Config |

5.1.7 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 | <code>spanning-tree forceversion <802.1d 802.1w 802.1s></code> |
| Mode | Global Config |

5.1.7.1 no spanning-tree forceversion

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

| | |
|---------------|--|
| Format | <code>no spanning-tree forceversion</code> |
| Mode | Global Config |

5.1.8 spanning-tree forward-time

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

| | |
|----------------|--|
| Default | 15 |
| Format | <code>spanning-tree forward-time <4-30></code> |
| Mode | Global Config |

5.1.8.1 no spanning-tree forward-time

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

| | |
|---------------|--|
| Format | <code>no spanning-tree forward-time</code> |
| Mode | Global Config |

5.1.9 spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree. The hello time *<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 | <code>spanning-tree hello-time <1-10></code> |
| Mode | Interface Config |

5.1.9.1 no spanning-tree hello-time

This command sets the admin Hello Time parameter for the common and internal spanning tree to the default value.

| | |
|---------------|--|
| Format | <code>no spanning-tree hello-time</code> |
| Mode | Interface Config |

5.1.10 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 | <code>spanning-tree max-age <6-40></code> |
| Mode | Global Config |

5.1.10.1 no spanning-tree max-age

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

| | |
|---------------|---------------------------------------|
| Format | <code>no spanning-tree max-age</code> |
| Mode | Global Config |

5.1.11 spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

| | |
|----------------|---|
| Default | 20 |
| Format | <code>spanning-tree max-hops <1-127></code> |
| Mode | Global Config |

5.1.11.1 no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

| | |
|---------------|--|
| Format | <code>no spanning-tree max-hops</code> |
| Mode | Global Config |

5.1.12 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 you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the 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. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **external-cost** option, this command sets the external-path cost for MST instance '0' i.e. CIST instance. You can set the external cost as a number in the range of 1 to 200000000 or **auto**. If you specify **auto**, the external path cost value is set based on Link Speed.

If you specify the **port-priority** option, 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; external-cost: auto; port-priority: 128 |
| Format | <code>spanning-tree mst <mstid> {{cost <1-200000000> auto} </code> |

```
{external-cost <1-200000000> | auto} | port-priority <0-240>}
```

Mode

Interface Config

5.1.12.1 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 you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, 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 path cost value based on the Link Speed.

If you specify **external-cost**, this command sets the external path cost for this port for mst '0' instance, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **port-priority**, 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 | external-cost  
| port-priority>
```

Mode

Interface Config

5.1.13 spanning-tree mst instance

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

Format

```
spanning-tree mst instance <mstid>
```

Mode

Global Config

5.1.13.1 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 parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

| | |
|---------------|--|
| Format | <code>no spanning-tree mst instance <mstid></code> |
| Mode | Global Config |

5.1.14 spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter *<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 you specify 0 (defined as the default CIST ID) as the *<mstid>*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

| | |
|----------------|---|
| Default | 32768 |
| Format | <code>spanning-tree mst priority <mstid> <0-61440></code> |
| Mode | Global Config |

5.1.14.1 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 parameter *<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>*, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value, i.e. 32768.

| | |
|---------------|---|
| Format | <code>spanning-tree mst priority <mstid></code> |
| Mode | Global Config |

5.1.15 spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN so that the VLAN is no longer associated with the common and internal spanning tree.

The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

| | |
|---------------|--|
| Format | <code>spanning-tree mst vlan <mstid> <vlanid></code> |
| Mode | Global Config |

5.1.15.1 no spanning-tree mst vlan

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

| | |
|---------------|---|
| Format | <code>no spanning-tree mst vlan <mstid> <vlanid></code> |
| Mode | Global Config |

5.1.16 spanning-tree port mode

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

| | |
|----------------|--------------------------------------|
| Default | disabled |
| Format | <code>spanning-tree port mode</code> |
| Mode | Interface Config |

5.1.16.1 no spanning-tree port mode

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

| | |
|---------------|---|
| Format | <code>no spanning-tree port mode</code> |
| Mode | Interface Config |

5.1.17 spanning-tree port mode all

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

| | |
|----------------|--|
| Default | disabled |
| Format | <code>spanning-tree port mode all</code> |
| Mode | Global Config |

5.1.17.1 no spanning-tree port mode all

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

| | |
|---------------|---|
| Format | <code>no spanning-tree port mode all</code> |
| Mode | Global Config |

5.1.18 spanning-tree bpduforwarding

Normally a switch will not forward Spanning Tree Protocol (STP) BPDU packets if STP is disabled. However, if in some network setup, the user wishes to forward BPDU packets received from other network devices, this command can be used to enable the forwarding.

| | |
|----------------|---|
| Default | disabled |
| Format | <code>spanning-tree bpduforwarding</code> |
| Mode | Global Config |

5.1.18.1 no spanning-tree bpduforwarding

This command will cause the STP BPDU packets received from the network to be dropped if STP is disabled.

| | |
|---------------|--|
| Format | <code>no spanning-tree bpduforwarding</code> |
| Mode | Global Config |

5.2 STP Show Commands

This section describes the commands you use to view information about STP configuration and status.

5.2.1 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 | <code>show spanning-tree <brief></code> |
| Modes | Privileged EXEC User EXEC |

| | |
|---------------------------------------|---|
| Bridge Priority | Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096. |
| Bridge Identifier | The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge. |
| Time Since Topology Change | Time 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 | The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge. |
| Root Path Cost | Value of the Root Path Cost parameter for the common and internal spanning tree. |
| Root Port Identifier | Identifier of the port to access the Designated Root for the CST. |
| Root Port Max Age | Derived value. |
| Root Port Bridge Forward Delay | Derived value. |
| Hello Time | Configured value of the parameter for the CST. |
| Bridge Hold Time | Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs) |
| Bridge Max Hops | Bridge max-hops count for the device. |
| CST Regional Root | Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge. |
| Regional Root Path Cost | Path Cost to the CST Regional Root. |

Associated FIDs List of forwarding database identifiers currently associated with this instance.

Associated VLANs List of VLAN IDs currently associated with this instance.

When you include the **brief** keyword, this command displays spanning tree settings for the bridge and the following information appears.

Bridge Priority Configured value.

Bridge Identifier The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.

Bridge Max Age Configured value.

Bridge Max Hops Bridge max-hops count for the device.

Bridge Hello Time Configured value.

Bridge Forward Delay Configured value.

Bridge Hold Time Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

5.2.2 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`

Modes Privileged EXEC
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 Identifier used to identify the configuration currently being used.

| | |
|-------------------------------------|---|
| Configuration Revision Level | Identifier used to identify the configuration currently being used. |
| Configuration Digest Key | Identifier used to identify the configuration currently being used. |
| MST Instances | List of all multiple spanning tree instances configured on the switch |

5.2.3 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 | <code>show spanning-tree interface <slot/port></code> |
| Modes | Privileged EXEC User EXEC |
| Hello Time | Admin hello time for this port. |
| Port mode | Enabled or disabled. |
| Port Up Time Since Counters Last Cleared | Time since port was reset, displayed in days, hours, minutes, and seconds. |
| STP BPDUs Transmitted | Spanning Tree Protocol Bridge Protocol Data Units sent |
| STP BPDUs Received | Spanning Tree Protocol Bridge Protocol Data Units received. |
| RST BPDUs Transmitted | Rapid Spanning Tree Protocol Bridge Protocol Data Units sent |
| RST BPDUs Received | Rapid Spanning Tree Protocol Bridge Protocol Data Units received. |
| MSTP BPDUs Transmitted | Multiple Spanning Tree Protocol Bridge Protocol Data Units sent |

MSTP BPDUs

Received

Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

5.2.4 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 parameter `<mstid>` is a number that corresponds to the desired existing multiple spanning tree instance. The `<slot/port>` is the desired switch port.

| | |
|---|---|
| Format | <code>show spanning-tree mst port detailed <mstid> <slot/port></code> |
| Mode | Privileged EXEC User EXEC |
| MST Instance ID | The ID of the existing MST instance. |
| Port Identifier | The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port. |
| Port Priority | The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16. |
| Port Forwarding State | Current spanning tree state of this port. |
| Port Role | Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port |
| Auto-Calculate Port Path Cost | This indicates whether auto calculation for port path cost is enabled. |
| Port Path Cost | Configured value of the Internal Port Path Cost parameter. |
| Auto-Calculate External Port Path Cost | This indicates whether auto calculation for external port path cost is enabled. |
| External Port Path Cost | Configured value of the external Port Path Cost parameter. |
| Designated Root | The Identifier of the designated root for this port. |

| | |
|-----------------------------------|---|
| Designated Port Cost | Path Cost offered to the LAN by the Designated Port |
| Designated Bridge | Bridge Identifier of the bridge with the Designated Port. |
| Designated Port Identifier | Port on the Designated Bridge that offers the lowest cost to the LAN. |

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, 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.

5.2.5 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 you specify 0 (defined as the default CIST ID) as the *<mstid>*, the status summary displays for one or all ports within the common and internal spanning tree.

Format

show spanning-tree mst port summary *<mstid>* *{<slot/port> | all}*

Modes

Privileged EXEC
User EXEC

MST Instance ID

The MST instance associated with this port.

Interface

Valid slot and port number separated by forward slashes.

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.

5.2.6 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

Modes

Privileged EXEC
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. |

5.2.7 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 | <code>show spanning-tree vlan <vlanid></code> |
| Modes | Privileged EXEC User EXEC |
| VLAN Identifier | The VLANs associated with the selected MST instance. |
| Associated Instance | Identifier for the associated multiple spanning tree instance or “CST” if associated with the common and internal spanning tree. |

Chapter 6

VLAN Commands

This section describes the VLAN commands available in the 7200 Series Managed Switch CLI. VLANs allow users located on different physical networks to be on the same logical network.

The VLAN Commands section includes the following topics:

- [Section 6.1 “VLAN Configuration Commands” on page 6-1](#)
- [Section 6.2 “VLAN Show Commands” on page 6-11](#)
- [Section 6.3 “Provisioning \(IEEE 802.1p\) Commands” on page 6-14](#)

The commands in this section are in one of two 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.

6.1 VLAN Configuration Commands

This section describes the commands you use to configure VLAN settings.

6.1.1 vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

| | |
|---------------|----------------------------|
| Format | <code>vlan database</code> |
| Mode | Privileged EXEC |

6.1.2 network mgmt_vlan

This command configures the Management VLAN ID.

| | |
|----------------|-----------------------------------|
| Default | 1 |
| Format | network mgmt_vlan <1-4069> |
| Mode | Privileged EXEC |

6.1.2.1 no network mgmt_vlan

This command sets the Management VLAN ID to the default.

| | |
|---------------|-----------------------------|
| Format | no network mgmt_vlan |
| Mode | Privileged EXEC |

6.1.3 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 Config |

6.1.3.1 no vlan

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

| | |
|---------------|-------------------------|
| Format | no vlan <2-4094> |
| Mode | VLAN Config |

6.1.4 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 | all |
| Format | vlan acceptframe {vlanonly all} |
| Mode | Interface Config |

6.1.4.1 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 { <i>vlanonly</i> <i>all</i> } |
| Mode | Interface Config |

6.1.5 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 |

6.1.5.1 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 |

6.1.6 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 Config |

6.1.7 vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4094.

| | |
|----------------|--|
| Default | VLAN ID 1 - default; other VLANs - blank string |
| Format | <code>vlan name <2-4094> <name></code> |
| Mode | VLAN Config |

6.1.7.1 no vlan name

This command sets the name of a VLAN to a blank string.

| | |
|---------------|--|
| Format | <code>no vlan name <2-4094></code> |
| Mode | VLAN Config |

6.1.8 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 | <code>vlan participation {exclude include auto} <1-4094></code> |
| 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. |

6.1.9 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. |

6.1.10 vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces. The modes defined as follows:

- VLAN Only mode - Untagged frames or priority frames received on this interface are discarded.
- 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 all

Format `vlan port acceptframe all {vlanonly | all}`

Mode Global Config

6.1.10.1 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 | <code>no vlan port acceptframe all</code> |
| Mode | Global Config |

6.1.11 vlan port pvid all

This command changes the VLAN ID for all interface.

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

6.1.11.1 no vlan port pvid all

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

| | |
|---------------|------------------------------------|
| Format | <code>no vlan port pvid all</code> |
| Mode | Global Config |

6.1.12 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 | <code>vlan port tagging all <1-4094></code> |
| Mode | Global Config |

6.1.12.1 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 | <code>no vlan port tagging all</code> |
| Mode | Global Config |

6.1.13 vlan port ingressfilter all

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

| | |
|----------------|--|
| Default | disabled |
| Format | <code>vlan port ingressfilter all</code> |
| Mode | Global Config |

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

6.1.15 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 | <code>vlan protocol group <groupname></code> |
| Mode | Global Config |

6.1.16 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 | <code>vlan protocol group add protocol <groupid> <protocol></code> |
| Mode | Global Config |

6.1.16.1 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

6.1.17 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

6.1.18 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.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

Default none

Format `protocol group <groupid> <vlanid>`

Mode VLAN Config

6.1.18.1 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 Config

6.1.19 protocol vlan group

This command adds the physical interface to the protocol-based VLAN identified by *<groupid>*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group.

Create the referenced VLAN before you create the protocol-based VLAN except when you configure GVRP to create the VLAN.

| | |
|---------------|--|
| Format | <code>protocol vlan group <groupid></code> |
| Mode | Interface Config |

6.1.19.1 no protocol vlan group

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

| | |
|---------------|---|
| Format | <code>no protocol vlan group <groupid></code> |
| Mode | Interface Config |

6.1.20 protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by *<groupid>*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination 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.

Create the referenced VLAN before you create the protocol-based VLAN except when you configure GVRP to create the VLAN.

| | |
|---------------|--|
| Format | <code>protocol vlan group all <groupid></code> |
| Mode | Global Config |

6.1.20.1 no protocol vlan group all

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

| | |
|---------------|---|
| Format | <code>no protocol vlan group all <groupid></code> |
| Mode | Global Config |

6.1.21 vlan pvid

This command changes the VLAN ID per interface. When an untagged packet comes to the switch, it will be tagged with the PVID value as the VLAN ID for further processing. By default, every port belongs to VLAN 1 and the PVID value is set to 1.

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

6.1.21.1 no vlan pvid

This command sets the VLAN ID per interface to 1.

| | |
|---------------|---------------------|
| Format | no vlan pvid |
| Mode | Interface Config |

6.1.22 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 |

6.1.22.1 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 |

6.2 VLAN Show Commands

This section describes the commands you use to view VLAN settings.

6.2.1 show vlan

This command displays a list of all configured VLANs.

| | |
|------------------|---|
| Format | <code>show vlan</code> |
| Modes | Privileged EXEC User EXEC |
| VLAN ID | There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4094. |
| VLAN Name | A string associated with this VLAN as a convenience. It can be up to 32 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) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration). |

6.2.2 show vlan <vlan_id>

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number.

| | |
|------------------|---|
| Format | <code>show vlan <vlanid></code> |
| Modes | Privileged EXEC 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 32 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) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration). |

| | |
|-------------------|--|
| Interface | Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line. |
| Current | <p>Determines the degree of participation of this port in this VLAN. The permissible values are:</p> <p>Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</p> <p>Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</p> <p>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.</p> |
| Configured | <p>Determines the configured degree of participation of this port in this VLAN. The permissible values are:</p> <p>Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</p> <p>Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</p> <p>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.</p> |
| Tagging | <p>Select the tagging behavior for this port in this VLAN.</p> <p>Tagged - specifies to transmit traffic for this VLAN as tagged frames.</p> <p>Untagged - specifies to transmit traffic for this VLAN as untagged frames.</p> |

6.2.3 show vlan port

This command displays VLAN port information.

| | |
|-------------------------------|--|
| Format | <code>show vlan port {<slot/port> all}</code> |
| Modes | Privileged EXEC User EXEC |
| Interface | Valid slot and port number separated by forward slashes. 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. |

6.3 Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning, which allows you to prioritize ports.

6.3.1 vlan port priority all

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

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

6.3.2 vlan priority

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

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

Chapter 7

DHCP Commands

This section describes the DHCP commands available in the 7200 Series Managed Switch CLI. DHCP automatically allocates and manages client TCP/ IP configurations. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

The DHCP Server Commands section includes the following topics:

- [Section 7.1 “DHCP Server Commands \(DHCP Config Pool Mode\)” on page 7-2](#)
- [Section 7.2 “DHCP Server Commands \(Global Config Mode\)” on page 7-9](#)
- [Section 7.3 “DHCP Server Clear and Show Commands” on page 7-12](#)
- [Section 7.4 “DHCP and BOOTP Relay Commands” on page 7-15](#)

The commands in this section are in one of three functional groups:

- 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.
- Show commands are used to display switch settings, statistics and other information.
- Clear commands clear some or all of the settings to factory defaults.

7.1 DHCP Server Commands (DHCP Config Pool Mode)

This section describes the commands you to configure the DHCP server settings for the switch.

7.1.1 ip dhcp pool

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

| | |
|----------------|--|
| Default | none |
| Format | <code>ip dhcp pool <name></code> |
| Mode | Global Config |



Note: The CLI mode changes to DHCP Pool Config mode when you successfully execute this command.

7.1.1.1 no ip dhcp pool

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

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

7.1.2 client-identifier

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique-identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the “Address Resolution Protocol Parameters” section of RFC 1700, Assigned Numbers for a list of media type codes.

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

7.1.2.1 no client-identifier

This command deletes the client identifier.

| | |
|---------------|-----------------------------|
| Format | no client-identifier |
| Mode | DHCP Pool Config |

7.1.3 client-name

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

| | |
|----------------|---------------------------|
| Default | none |
| Format | client-name <name> |
| Mode | DHCP Pool Config |

7.1.3.1 no client-name

This command removes the client name.

| | |
|---------------|-----------------------|
| Format | no client-name |
| Mode | DHCP Pool Config |

7.1.4 default-router

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

| | |
|----------------|---|
| Default | none |
| Format | default-router <address1> [<address2>...<address8>] |
| Mode | DHCP Pool Config |

7.1.4.1 no default-router

This command removes the default router list.

| | |
|---------------|--------------------------|
| Format | no default-router |
| Mode | DHCP Pool Config |

7.1.5 dns-server

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

| | |
|----------------|--|
| Default | none |
| Format | dns-server <address1> [<address2>...<address8>] |
| Mode | DHCP Pool Config |

7.1.5.1 no dns-server

This command removes the DNS Server list.

| | |
|---------------|----------------------|
| Format | no dns-server |
| Mode | DHCP Pool Config |

7.1.6 hardware-address

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

| | |
|----------------|--|
| Default | ethernet |
| Format | hardware-address <hardwareaddress> [type] |
| Mode | DHCP Pool Config |

7.1.6.1 no hardware-address

This command removes the hardware address of the DHCP client.

| | |
|---------------|----------------------------|
| Format | no hardware-address |
| Mode | DHCP Pool Config |

7.1.7 host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32

| | |
|----------------|------|
| Default | none |
|----------------|------|

| | |
|---------------|--|
| Format | host <address> [mask prefix-length] |
| Mode | DHCP Pool Config |

7.1.7.1 no host

This command removes the IP address of the DHCP client.

| | |
|---------------|------------------|
| Format | no host |
| Mode | DHCP Pool Config |

7.1.8 lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If *infinite* is specified, lease is set for 60 days. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 1439. *Minutes* is an integer from 0 to 86399.

| | |
|----------------|--|
| Default | 1 (day) |
| Format | lease {[<days> [hours] [minutes]] [infinite]} |
| Mode | DHCP Pool Config |

7.1.8.1 no lease

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

| | |
|---------------|------------------|
| Format | no lease |
| Mode | DHCP Pool Config |

7.1.9 network

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

| | |
|----------------|--|
| Default | none |
| Format | network <networknumber> [mask / prefixlength] |
| Mode | DHCP Pool Config |

7.1.9.1 no network

This command removes the subnet number and mask.

| | |
|---------------|-------------------|
| Format | no network |
| Mode | DHCP Pool Config |

7.1.10 bootfile

The command specifies the name of the default boot image for a DHCP client. The <filename> specifies the boot image file.

| | |
|----------------|----------------------------|
| Default | none |
| Format | bootfile <filename> |
| Mode | DHCP Pool Config |

7.1.10.1 no bootfile

This command deletes the boot image name.

| | |
|---------------|--------------------|
| Format | no bootfile |
| Mode | DHCP Pool Config |

7.1.11 domain-name

This command specifies the domain name for a DHCP client. The <domain> specifies the domain name string of the client.

| | |
|----------------|-----------------------------|
| Default | none |
| Format | domain-name <domain> |
| Mode | DHCP Pool Config |

7.1.11.1 no domain-name

This command removes the domain name.

| | |
|---------------|-----------------------|
| Format | no domain-name |
| Mode | DHCP Pool Config |

7.1.12 netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

| | |
|----------------|---|
| Default | none |
| Format | netbios-name-server <address> [<address2>...<address8>] |
| Mode | DHCP Pool Config |

7.1.12.1 no netbios-name-server

This command removes the NetBIOS name server list.

| | |
|---------------|-------------------------------|
| Format | no netbios-name-server |
| Mode | DHCP Pool Config |

7.1.13 netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients.type Specifies the NetBIOS node type. Valid types are:

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed
- h-node—Hybrid (recommended)

| | |
|----------------|---------------------------------|
| Default | none |
| Format | netbios-node-type <type> |
| Mode | DHCP Pool Config |

7.1.13.1 no netbios-node-type

This command removes the NetBIOS node Type.

| | |
|---------------|-----------------------------|
| Format | no netbios-node-type |
| Mode | DHCP Pool Config |

7.1.14 next-server

This command configures the next server in the boot process of a DHCP client.

Address is the IP address of the next server in the boot process, which is typically a TFTP server.

| | |
|----------------|------------------------------------|
| Default | inbound interface helper addresses |
| Format | next-server <address> |
| Mode | DHCP Pool Config |

7.1.14.1 no next-server

This command removes the boot server list.

| | |
|---------------|-----------------------|
| Format | no next-server |
| Mode | DHCP Pool Config |

7.1.15 option

The command configures DHCP Server options. The <code> parameter specifies the DHCP option code. Ascii string specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. Hex string specifies hexadecimal data. in hexadecimal character strings is two hexadecimal digits—each byte can be separated by a period, colon, or white space.

Example:a3:4f:22:0c / a3 4f 22 0c / a34f.220c.9fed

| | |
|----------------|---|
| Default | none |
| Format | option <code> {ascii string hex <string1> [<string2>...<string8>] ip <address1> [<address2>...<address8>]} |
| Mode | DHCP Pool Config |

7.1.15.1 no option

This command removes the options.

| | |
|---------------|--------------------------------------|
| Format | no option <i><code></i> |
| Mode | DHCP Pool Config |

7.2 DHCP Server Commands (Global Config Mode)

This section describes the commands you to configure the DHCP server settings for the switch. You must be in Global Config mode to execute these commands.

7.2.1 ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

| | |
|----------------|--|
| Default | none |
| Format | ip dhcp excluded-address <i><lowaddress></i> [<i>highad-</i> <i>dress</i>] |
| Mode | Global Config |

7.2.1.1 no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

| | |
|---------------|---|
| Format | no ip dhcp excluded-address <i><lowaddress></i> [<i>highad-</i> <i>dress</i>] |
| Mode | Global Config |

7.2.2 ip dhcp ping packets

This command is used to specify the number, in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2 (the smallest allowed number when sending packets). Setting the number of packets to 0 disables this command.



Note: The no form of this command sets the number of packets sent to a pool address to 0 and therefore prevents the server from pinging pool addresses.

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

7.2.2.1 no ip dhcp ping packets

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

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

7.2.3 service dhcp

This command enables the DHCP server.

| | |
|----------------|---------------------------|
| Default | disabled |
| Format | <code>service dhcp</code> |
| Mode | Global Config |

7.2.3.1 no service dhcp

This command disables the DHCP server.

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

7.2.4 ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

| | |
|----------------|--------------------------------------|
| Default | disabled |
| Format | <code>ip dhcp bootp automatic</code> |
| Mode | Global Config |

7.2.4.1 no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

| | |
|---------------|---|
| Format | <code>no ip dhcp bootp automatic</code> |
| Mode | Global Config |

7.2.5 ip dhcp conflict logging

This command enables conflict logging on DHCP server.

| | |
|----------------|---------------------------------------|
| Default | enabled |
| Format | <code>ip dhcp conflict logging</code> |
| Mode | Global Config |

7.2.5.1 no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

| | |
|---------------|--|
| Format | <code>no ip dhcp conflict logging</code> |
| Mode | Global Config |

7.3 DHCP Server Clear and Show Commands

This section describes the commands you use to delete various DHCP information and the commands you use to view DHCP configuration information and statistics.

7.3.1 clear ip dhcp binding

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

| | |
|----------------|--|
| Default | none |
| Format | <code>clear ip dhcp binding {address *}</code> |
| Mode | Privileged EXEC |

7.3.2 clear ip dhcp server statistics

This command clears DHCP server statistics counters.

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

7.3.3 clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If the asterisk (*) character is used as the address parameter.

| | |
|----------------|---|
| Default | none |
| Format | <code>clear ip dhcp conflict {<address> *}</code> |
| Mode | Privileged EXEC |

7.3.4 show ip dhcp binding

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

| | |
|---------------|---|
| Format | <code>show ip dhcp binding [address]</code> |
| Modes | Privileged EXEC User EXEC |

| | |
|-------------------------|---|
| IP address | The IP address of the client. |
| Hardware Address | The MAC Address or the client identifier. |
| Lease expiration | The lease expiration time of the IP Address assigned to the client. |
| Type | The manner in which IP Address was assigned to the client. |

7.3.5 show ip dhcp global configuration

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

| | |
|-------------------------------|--|
| Format | <code>show ip dhcp global configuration</code> |
| Modes | Privileged EXEC User EXEC |
| Service DHCP | The field to display the status of dhcp protocol. |
| Number of Ping Packets | The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned. |
| Conflict Logging | Shows whether conflict logging is enabled or disabled. |
| BootP Automatic | Shows whether BootP for dynamic pools is enabled or disabled. |

7.3.6 show ip dhcp pool configuration

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

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

The following additional field is displayed for Dynamic pool type:

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

The following additional fields are displayed for Manual pool type:

| | |
|------------------------------|--|
| Client Name | The name of a DHCP client. |
| Client Identifier | The unique identifier of a DHCP client. |
| Hardware Address | The hardware address of a DHCP client. |
| Hardware Address Type | The protocol of the hardware platform. |
| Host | The IP address and the mask for a manual binding to a DHCP client. |

7.3.7 show ip dhcp server statistics

This command displays DHCP server statistics.

| | |
|---------------------------|---|
| Format | <code>show ip dhcp server statistics</code> |
| Modes | Privileged EXEC User EXEC |
| Automatic Bindings | The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database. |
| Expired Bindings | The number of expired leases. |
| Malformed Bindings | The number of truncated or corrupted messages that were received by the DHCP server. |

Message Received:

| | |
|----------------------|--|
| DHCP DISCOVER | The number of DHCPDISCOVER messages the server has received. |
| DHCP REQUEST | The number of DHCPREQUEST messages the server has received. |
| DHCP DECLINE | The number of DHCPDECLINE messages the server has received. |

| | |
|---------------------|---|
| DHCP RELEASE | The number of DHCPRELEASE messages the server has received. |
|---------------------|---|

| | |
|--------------------|--|
| DHCP INFORM | The number of DHCPINFORM messages the server has received. |
|--------------------|--|

Message Sent:

| | |
|-------------------|---|
| DHCP OFFER | The number of DHCPOFFER messages the server sent. |
|-------------------|---|

| | |
|-----------------|---|
| DHCP ACK | The number of DHCPACK messages the server sent. |
|-----------------|---|

| | |
|------------------|--|
| DHCP NACK | The number of DHCPNACK messages the server sent. |
|------------------|--|

7.3.8 show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

| | |
|---------------|--|
| Format | show ip dhcp conflict [<i>ip-address</i>] |
|---------------|--|

| | |
|--------------|------------------------------|
| Modes | Privileged EXEC User EXEC |
|--------------|------------------------------|

| | |
|-------------------|--|
| IP address | The IP address of the host as recorded on the DHCP server. |
|-------------------|--|

| | |
|-------------------------|---|
| Detection Method | The manner in which the IP address of the hosts were found on the DHCP Server |
|-------------------------|---|

| | |
|-----------------------|---------------------------------------|
| Detection time | The time when the conflict was found. |
|-----------------------|---------------------------------------|

7.4 DHCP and BOOTP Relay Commands

This section describes the commands you use to configure BootP/DHCP Relay on the switch. A DHCP relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

7.4.1 ip dhcp relay information option

This command enables option 82 (RFC 3046) for BootP/DHCP Relay on the system. Once enabled, the DHCP request forwarded to the DHCP server will contain two optional fields: Circuit ID and Remote ID. The circuit ID option contains the port information where the DHCP client request originated. The remote ID option contains the MAC address of the relay agent (the switch management CPU's own MAC address).

| | |
|----------------|---|
| Default | disabled |
| Format | <code>ip dhcp relay information option</code> |
| Mode | Global Config |

7.4.1.1 no ip dhcp relay information option

This command disables the relay information option mode for BootP/DHCP Relay on the system.

| | |
|---------------|--|
| Format | <code>no ip dhcp relay information option</code> |
| Mode | Global Config |

7.4.2 bootpdhcprelay

This command enables the forwarding of relay requests for BootP/DHCP Relay on the system.

| | |
|----------------|-----------------------------|
| Default | disabled |
| Format | <code>bootpdhcprelay</code> |
| Mode | Global Config |

7.4.2.1 no bootpdhcprelay enable

This command disables the forwarding of relay requests for BootP/DHCP Relay on the system.

| | |
|---------------|---------------------------------------|
| Format | <code>no bootpdhcprelay enable</code> |
| Mode | Global Config |

7.4.3 bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The *<hops>* parameter has a range of 1 to 16.

| | |
|----------------|--|
| Default | 4 |
| Format | <code>bootpdhcprelay maxhopcount <1-16></code> |
| Mode | Global Config |

7.4.3.1 no bootpdhcprelay maxhopcount

This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

| | |
|---------------|--|
| Format | <code>no bootpdhcprelay maxhopcount</code> |
| Mode | Global Config |

7.4.4 bootpdhcprelay minwaittime

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

| | |
|----------------|---|
| Default | 0 |
| Format | <code>bootpdhcprelay minwaittime <0-100></code> |
| Mode | Global Config |

7.4.4.1 no bootpdhcprelay minwaittime

This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

| | |
|---------------|--|
| Format | <code>no bootpdhcprelay minwaittime</code> |
| Mode | Global Config |

7.4.5 bootpdhcprelay serverip

This command configures the server IP Address for BootP/DHCP Relay on the system. The *<ipaddr>* parameter is an IP address in a 4-digit dotted decimal format.

| | |
|----------------|---|
| Default | 0.0.0.0 |
| Format | <code>bootpdhcprelay serverip <ipaddr></code> |
| Mode | Global Config |

7.4.5.1 no bootpdhcprelay serverip

This command configures the default server IP Address for BootP/DHCP Relay on the system.

| | |
|---------------|---|
| Format | <code>no bootpdhcprelay serverip</code> |
| Mode | Global Config |

7.4.6 show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

| | |
|------------------------------------|---|
| Format | <code>show bootpdhcprelay</code> |
| Modes | Privileged EXEC User EXEC |
| Maximum Hop Count | Is the maximum allowable relay agent hops. |
| Minimum Wait Time (Seconds) | Is the minimum wait time. |
| Admin Mode | Represents whether relaying of requests is enabled or disabled. |
| Server IP Address | Is the IP Address for the BootP/DHCP Relay server. |
| Circuit Id Option Mode | Is the DHCP circuit Id option which may be enabled or disabled. |
| Requests Received | Is the number of requests received. |
| Requests Relayed | Is the number of requests relayed. |
| Packets Discarded | Is the number of packets discarded. |
| Default | |

Chapter 8

GARP, GVRP, and GMRP Commands

This section describes the Generic Attribute Registration Protocol (GARP), GARP VLAN Registration Protocol (GVRP), and Garp Multicast Registration Protocol (GVMP) commands available in the 7200 Series Managed Switch CLI. GARP is a protocol that allows client stations to register with the switch for membership in VLANs (by using GVMP) or multicast groups (by using GMRP).

This section contains the following topics:

- [Section 8.1 “GARP Commands” on page 8-2](#)
- [Section 8.2 “GVRP Commands” on page 8-5](#)
- [Section 8.3 “GMRP Commands” on page 8-7](#)

The commands in this section are in one of two 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.

8.1 GARP Commands

This section describes the commands you use to configure GARP and view GARP status. The commands in this section affect both GVMP and GMRP.

8.1.1 set garp timer join

This command sets the GVRP join time for one or 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). The value 20 centiseconds is 0.2 seconds.

| | |
|----------------|-----------------------------------|
| Default | 20 |
| Format | set garp timer join <10-100> |
| Modes | Interface Config Global Config |

8.1.1.1 no set garp timer join

This command sets the GVRP join time (for one or all ports and per GARP) to the default.



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

| | |
|---------------|-----------------------------------|
| Format | no set garp timer join |
| Modes | Interface Config Global Config |

8.1.2 set garp timer leave

This command sets the GVRP leave time. 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). The value 60 centiseconds is 0.6 seconds.



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

| | |
|----------------|--|
| Default | 60 |
| Format | <code>set garp timer leave <20-600></code> |
| Modes | Interface Config Global Config |

8.1.2.1 no set garp timer leave

This command sets the GVRP leave time to the default.



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

| | |
|---------------|--------------------------------------|
| Format | <code>no set garp timer leave</code> |
| Modes | Interface Config Global Config |

8.1.3 set garp timer leaveall

This command sets how frequently *Leave All PDUs* are generated. 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). The value 1000 centiseconds is 10 seconds.



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

| | |
|----------------|---|
| Default | 1000 |
| Format | <code>set garp timer leaveall <200-6000></code> |
| Modes | Interface Config Global Config |

8.1.3.1 no set garp timer leaveall

This command sets how frequently *Leave All PDUs* are generated the default.



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

| | |
|---------------|---|
| Format | <code>no set garp timer leaveall</code> |
| Modes | Interface Config Global Config |

8.1.4 show garp

This command displays GARP information.

| | |
|------------------------|---|
| Format | <code>show garp</code> |
| Modes | Privileged EXEC User EXEC |
| GMRP Admin Mode | This displays the administrative mode of GMRP for the system. |

GVRP Admin Mode

This displays the administrative mode of GVRP for the system

8.2 GVRP Commands

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.



Note: If GVRP is disabled, the system does not forward GVRP messages.

8.2.1 set gvrp adminmode

This command enables GVRP.

| | |
|----------------|---------------------------------|
| Default | disabled |
| Format | <code>set gvrp adminmode</code> |
| Mode | Privileged EXEC |

8.2.1.1 no set gvrp adminmode

This command disables GVRP.

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

8.2.2 set gvrp interfacemode

This command enables GVRP.

| | |
|----------------|-------------------------------------|
| Default | disabled |
| Format | <code>set gvrp interfacemode</code> |
| Modes | Interface Config Global Config |

8.2.2.1 no set gvrp interfacemode

This command disables GVRP. If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

| | |
|---------------|--|
| Format | <code>no set gvrp interfacemode</code> |
| Modes | Interface Config Global Config |

8.2.3 show gvrp configuration

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

| | |
|-----------------------|---|
| Format | <code>show gvrp configuration {<slot/port> all}</code> |
| Modes | Privileged EXEC User EXEC |
| Interface | Valid slot and port number separated by forward slashes. |
| 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 one 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). |
| 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).

Port GMRP Mode

Indicates the GARP Multicast Registration Protocol (GMRP) administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

8.3 GMRP Commands

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP snooping, GMRP helps control the flooding of multicast packets. GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.



Note: If GMRP is disabled, the system does not forward GMRP messages.

8.3.1 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

8.3.1.1 no set gmrp adminmode

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

Format `no set gmrp adminmode`

Mode Privileged EXEC

8.3.2 set gmrp interfacemode

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

| | |
|----------------|-----------------------------------|
| Default | disabled |
| Format | set gmrp interfacemode |
| Modes | Interface Config Global Config |

8.3.2.1 no set gmrp interfacemode

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

| | |
|---------------|-----------------------------------|
| Format | no set gmrp interfacemode |
| Modes | Interface Config Global Config |

8.3.3 show gmrp configuration

This command displays GARP information for one or all interfaces.

| | |
|-------------------|---|
| Format | show gmrp configuration {<slot/port> all} |
| Modes | Privileged EXEC 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. |

onds (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).

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).

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.

8.3.4 show mac-address-table gmpr

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

Format `show mac-address-table gmpr`

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 is displayed as 8 bytes.

Type 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:).

Chapter 9

Port-Based Traffic Control Commands

This section describes the port-based traffic control commands available in the 7200 Series Managed Switch CLI.

This section includes the following topics:

- [Section 9.1 “Port Security Commands” on page 9-1](#)
- [Section 9.2 “Storm Control Commands” on page 9-5](#)

This section provides a detailed explanation of the security commands. The commands are divided into the following groups:

- 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.
- Show commands are used to display switch settings, statistics and other information.

9.1 Port Security Commands

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.



Note: To enable the SNMP trap specific to port security, see [Section 10.1.8 “snmp-server traps violation” on page 10-4](#).

9.1.1 port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config)

| | |
|----------------|-----------------------------------|
| Default | disabled |
| Format | <code>port-security</code> |
| Modes | Global Config Interface Config |

9.1.1.1 no port-security

This command disables port locking at the system level (Global Config) or port level (Interface Config).

| | |
|---------------|-----------------------------------|
| Format | <code>no port-security</code> |
| Modes | Global Config Interface Config |

9.1.2 port-security max-dynamic

This command sets the maximum of dynamically locked MAC addresses allowed on a specific port.

| | |
|----------------|---|
| Default | 600 |
| Format | <code>port-security max-dynamic <maxvalue></code> |
| Mode | Interface Config |

9.1.2.1 no port-security max-dynamic

This command resets the maximum of dynamically locked MAC addresses allowed on a specific port to its default value.

| | |
|---------------|---|
| Format | <code>no port-security max-dynamic</code> |
| Mode | Interface Config |

9.1.3 port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a specific port.

| | |
|----------------|--|
| Default | 20 |
| Format | <code>port-security max-static <maxvalue></code> |
| Mode | Interface Config |

9.1.3.1 no port-security max-static

This command resets the maximum of statically locked MAC addresses allowed on a specific port to its default value.

| | |
|---------------|--|
| Format | <code>no port-security max-static</code> |
| Mode | Interface Config |

9.1.4 port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses. The <vid> is the VLAN ID.

| | |
|---------------|--|
| Format | <code>port-security mac-address <mac-address> <vid></code> |
| Mode | Interface Config |

9.1.4.1 no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

| | |
|---------------|---|
| Format | <code>no port-security mac-address <mac-address> <vid></code> |
| Mode | Interface Config |

9.1.5 port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses.

| | |
|---------------|---|
| Format | <code>port-security mac-address move</code> |
| Mode | Interface Config |

9.1.6 show port-security

This command displays the port-security settings for the entire system.

| | |
|-------------------|---|
| Format | <code>show port-security</code> |
| Mode | Privileged EXEC |
| Admin Mode | Port Locking mode for the entire system |

9.1.7 show port-security

This command displays the port-security settings for a particular interface or all interfaces.

| | |
|-----------------------------|---|
| Format | <code>show port-security <interface / all></code> |
| Mode | Privileged EXEC |
| Interface Admin Mode | Port Locking mode for the Interface. |
| Dynamic Limit | Maximum dynamically allocated MAC Addresses. |
| Static Limit | Maximum statically allocated MAC Addresses. |
| Violation Trap Mode | Whether violation traps are enabled. |

9.1.8 show port-security dynamic

This command displays the dynamically locked MAC addresses for port.

| | |
|--------------------|---|
| Format | <code>show port-security dynamic <interface></code> |
| Mode | Privileged EXEC |
| MAC Address | MAC Address of dynamically locked MAC. |

9.1.9 show port-security static

This command displays the statically locked MAC addresses for port.

| | |
|--------------------|--|
| Format | <code>show port-security static <interface></code> |
| Mode | Privileged EXEC |
| MAC Address | MAC Address of statically locked MAC. |

9.1.10 show port-security violation

This command displays the source MAC address of the last packet that was discarded on a locked port.

| | |
|--------------------|---|
| Format | <code>show port-security violation <interface></code> |
| Mode | Privileged EXEC |
| MAC Address | MAC Address of discarded packet on locked port. |

9.2 Storm Control Commands

This section describes commands you use to configure storm control and view storm-control configuration information. The storm-control feature measures traffic activity on the physical ports and blocks traffic on the port when the amount of traffic reaches the threshold. Blocking the port helps maintain network performance.

9.2.1 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 [Table 9-1](#)) 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 [Table 9-1](#).

Table 9-1. Broadcast Storm Recovery Thresholds

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

| | |
|----------------|--------------------------------------|
| Default | enabled |
| Format | <code>storm-control broadcast</code> |
| Mode | Config |

9.2.1.1 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 [Table 9-1](#)) 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 [Table 9-1](#).

| | |
|---------------|---|
| Format | <code>no storm-control broadcast</code> |
| Mode | Global Config |

9.2.2 storm-control multicast all

This command enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery with high and low thresholds is implemented. The thresholds are defined in the same way as for broadcast.

| | |
|----------------|--|
| Default | disable |
| Format | <code>storm-control multicast all</code> |
| Mode | Config |

9.2.2.1 no storm-control multicast all

This command disables multicast storm recovery mode.

| | |
|---------------|---|
| Format | <code>no storm-control multicast all</code> |
| Mode | Global Config |

9.2.3 storm-control unicast all

This command enables unknown unicast packet storm recovery mode. If the mode is enabled, the unknown storm recovery with high and low thresholds is implemented. The thresholds are defined same as the one for broadcast.

| | |
|----------------|--|
| Default | disable |
| Format | <code>storm-control unicast all</code> |
| Mode | Config |

9.2.3.1 no storm-control unicast all

This command disables multicast storm recovery mode.

| | |
|---------------|---|
| Format | <code>no storm-control unicast all</code> |
| Mode | Global Config |

9.2.4 storm-control broadcast

This command enables broadcast storm recovery mode in per-port level. If the mode is enabled, broadcast storm recovery with high and low thresholds is implemented. The *<level>* value is in a range of 0 to 100 (in percentage). A value of 0 means no storm control. If the *<level>* value is not specified, the thresholds are defined the same as the ones for broadcast storm control in Global mode.

| | |
|----------------|--|
| Default | enable |
| Format | <code>storm-contol broadcast [<i><level></i>]</code> |
| Mode | Interface Config |

9.2.4.1 no storm-control broadcast

This command disables broadcast storm recovery mode.

| | |
|---------------|--|
| Format | <code>no storm-control broadcast [<i><level></i>]</code> |
| Mode | Interface Config |

9.2.5 storm-control multicast

This command enables multicast packet storm recovery mode on the port level. If the mode is enabled, multicast storm recovery with high and low thresholds is implemented. The *<level>* value is in a range of 0 to 100 (in percentage). Value of 0 means no storm control. If *<level>* value is not specified, the thresholds are defined same as the ones for broadcast storm control in Global mode.

| | |
|----------------|---|
| Default | enable |
| Format | <code>storm-control multicast [<i><level></i>]</code> |
| Mode | Interface Config |

9.2.5.1 no storm-control multicast

This command disables multicast storm recovery mode.

| | |
|---------------|---|
| Format | <code>no storm-control multicast [<level>]</code> |
| Mode | Interface Config |

9.2.6 storm-control unicast

This command enables unknown unicast packet storm recovery mode in per-port level. If the mode is enabled, storm recovery with high and low thresholds is implemented. The <level> value is in a range of 0 to 100 (in percentage). A value of 0 means no storm control. If the <level> value is not specified, the thresholds are defined the same as the ones for broadcast storm control in Global mode.

| | |
|----------------|--|
| Default | enable |
| Format | <code>storm-control unicast [<level>]</code> |
| Mode | Interface Config |

9.2.6.1 no storm-control unicast

This command disables unicast storm recovery mode.

| | |
|---------------|---|
| Format | <code>no storm-control unicast [<level>]</code> |
| Mode | Interface Config |

9.2.7 storm-control flowcontrol

This command enables 802.3x flow control for the switch and only applies to full-duplex mode ports.




Note: 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

| | |
|----------------|--|
| Default | disabled |
| Format | <code>storm-control flowcontrol</code> |
| Mode | Global Config |

9.2.7.1 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 | <code>no storm-control flowcontrol</code> |
| Mode | Global Config |

9.2.8 show storm-control

This command displays switch configuration information.

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

Chapter 10

SNMP Commands

This section describes the SNMP commands available in the 7200 Series Managed Switch CLI. You can configure the switch to act as a Simple Network Management Protocol (SNMP) agent so that it can communicate with SNMP managers on your network.

The SNMP Commands section contains the following topics:

- [Section 10.1 “SNMP Configuration Commands” on page 10-1](#)
- [Section 10.2 “SNMP Show Commands” on page 10-10](#)

The commands in this section are in one of two 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.

10.1 SNMP Configuration Commands

This section describes the commands you use to configure SNMP on switch.

10.1.1 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>*, *<loc>* and *<con>* is from 1 to 31 alphanumeric characters.

| | |
|----------------|--|
| Default | none |
| Format | <code>snmp-server {sysname <name> / location <loc> / contact <con>}</code> |
| Mode | Global Config |

10.1.2 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. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

| | |
|----------------|---|
| Default | public and private, which you can rename; default values for the remaining four community names are blank |
| Format | <code>snmp-server community <name></code> |
| Mode | Global Config |

10.1.2.1 no snmp-server community

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

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

10.1.3 snmp-server community ipaddr

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

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

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

10.1.4 snmp-server community ipmask

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

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

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

10.1.5 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 | private and public communities - enabled; other four - disabled |
| Format | <code>snmp-server community mode <name></code> |
| Mode | Global Config |

10.1.5.1 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

10.1.6 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

10.1.7 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

10.1.8 snmp-server traps violation

This command enables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.



Note: For other port security commands, see [Section 9.1 “Port Security Commands” on page 9-1](#).

Default disabled

Format `snmp-server traps violation`

Mode Interface Config

10.1.8.1 no snmp-server traps violation

This command disables the sending of new violation traps.

| | |
|---------------|---|
| Format | <code>no snmp-server traps violation</code> |
| Mode | Interface Config |

10.1.9 snmp-server traps

This command enables the Authentication Flag.

| | |
|----------------|--------------------------------|
| Default | enabled |
| Format | <code>snmp-server traps</code> |
| Mode | Global Config |

10.1.9.1 no snmp-server traps

This command disables the Authentication Flag.

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

10.1.10 snmp-server 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 | <code>snmp-server traps bcaststorm</code> |
| Mode | Global Config |

10.1.10.1 no snmp-server 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 | <code>no snmp-server traps bcaststorm</code> |
| Mode | Global Config |

10.1.11 snmp-server 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. [Section 10.1.18 “snmp trap link-status” on page 10-9](#)

| | |
|----------------|---|
| Default | enabled |
| Format | <code>snmp-server traps linkmode</code> |
| Mode | Global Config |

10.1.11.1 no snmp-server traps linkmode

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

| | |
|---------------|--|
| Format | <code>no snmp-server traps linkmode</code> |
| Mode | Global Config |

10.1.12 snmp-server 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 | <code>snmp-server traps multiusers</code> |
| Mode | Global Config |

10.1.12.1 no snmp-server traps multiusers

This command disables Multiple User traps.

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

10.1.13 snmp-server traps stpmode

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

| | |
|----------------|--|
| Default | enabled |
| Format | <code>snmp-server traps stpmode</code> |
| Mode | Global Config |

10.1.13.1 no snmp-server traps stpmode

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

| | |
|---------------|-------------------------------------|
| Format | no snmp-server traps stpmode |
| Mode | Global Config |

10.1.14 snmptrap

This command adds an SNMP trap receiver. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* is the version of SNMP. The version parameter options are snmpv1 or snmpv2.

The *<name>* parameter does not need to be unique, however; the *<name>* and *<ipaddr>* pair must be unique. Multiple entries can exist with the same *<name>* as long as they are associated with a different *<ipaddr>*.

The reverse scenario is also acceptable. The *<name>* is the community name used when sending the trap to the receiver, but the *<name>* is not directly associated with the SNMP Community Table. For more information, see [Section 10.1.2 “snmp-server community” on page 10-2](#).

| | |
|----------------|---|
| Default | snmpv2 |
| Format | snmptrap <i><name></i> <i><ipaddr></i> [<i>snmpversion</i> <i><snmpversion></i>] |
| Mode | Global Config |

10.1.14.1 no snmptrap

This command deletes trap receivers for a community.

| | |
|---------------|--|
| Format | no snmptrap <i><name></i> <i><ipaddr></i> |
| Mode | Global Config |

10.1.15 snmptrap snmpversion

This command modifies the SNMP version of a trap. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* can be snmpv1 or snmpv2.



Note: This command does not support a “no” form.

Default

snmpv2

Format

snmptrap snmpversion *<name>* *<ipaddr>* *<snmpversion>*

Mode

Global Config

10.1.16 snmptrap ipaddr

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



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

Format

snmptrap ipaddr *<name>* *<ipaddrold>* *<ipaddrnew>*

Mode

Global Config

10.1.17 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

10.1.17.1 no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are inactive.

Format


no snmptrap mode *<name>* *<ipaddr>*

Mode

Global Config

10.1.18 snmp trap link-status

This command enables link status traps by interface.


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

Format `snmp trap link-status`

Mode Interface Config

10.1.18.1 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 ‘snmp-server enable traps linkmode’ command). |
|---|--|

Format `no snmp trap link-status`

Mode Interface Config

10.1.19 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 Section 10.1.11 “snmp-server traps linkmode” on page 10-6 |
|---|--|

Format `snmp trap link-status all`

Mode Global Config

10.1.19.1 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 [Section 10.1.11 “snmp-server traps linkmode” on page 10-6](#)

Format

`no snmp trap link-status all`

Mode

Global Config

10.2 SNMP Show Commands

This section describes the commands you use to view SNMP status and configuration information.

10.2.1 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 Versions 1, 2 or 3. For more information 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: 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. |

10.2.2 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 | <code>show snmptrap</code> |
| Mode | Privileged EXEC |
| SNMP Trap Name | The community string of the SNMP trap packet sent to the trap manager. The string is case sensitive and can be up to 16 alphanumeric characters. |
| IP Address | The IP address to receive SNMP traps from this device. |
| Status | Indicates the receiver's status (enabled or disabled). |

10.2.3 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 SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

| | |
|---------------|-----------------------------|
| Format | <code>show trapflags</code> |
| Mode | Privileged EXEC |

Authentication

Flag

Can be enabled or disabled. The factory default is enabled.
Indicates whether authentication failure traps will be sent.

Link Up/Down

Flag

Can be enabled or disabled. The factory default is enabled.
Indicates whether link status traps will be sent.

Multiple Users

Flag

Can 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

Can be enabled or disabled. The factory default is enabled.
Indicates whether spanning tree traps will be sent.

Broadcast Storm

Flag

Can be enabled or disabled. The factory default is enabled.
Indicates whether broadcast storm traps will be sent.

DVMRP Traps

Can be enabled or disabled. The factory default is disabled.
Indicates whether DVMRP traps will be sent.

OSPF Traps

Can be enabled or disabled. The factory default is disabled.
Indicates whether OSPF traps will be sent.

PIM Traps

Can be enabled or disabled. The factory default is disabled.
Indicates whether PIM traps are sent.

Chapter 11

Port-Based Access and Authentication Commands

This section describes the port-based access and authentication commands available in the 7200 Series Managed Switch CLI.

The Port-Based Access and Authentication Commands section includes the following topics:

- [Section 11.1 “Port-Based Network Access Control Commands” on page 11-1](#)
- [Section 11.2 “RADIUS Commands” on page 11-13](#)

The commands in this section lie in one of two functional groups:

- 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.
- Show commands are used to display switch settings, statistics and other information.

11.1 Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (802.1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

11.1.1 authentication login

This command creates an authentication login list. The *<listname>* is any character string 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 the user is never authenticated.

To authenticate a user, the first authentication method in the user’s login (authentication login list) is attempted. The 7200 Series Managed Switch software does not utilize multiple entries in the user’s login. If the first entry returns a timeout, the user authentication attempt fails.



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

Format

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

Mode

Global Config

11.1.1.1 no authentication login

This command deletes the specified authentication login list. The attempt to delete fails 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 non configured 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

11.1.2 clear dot1x statistics

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

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

11.1.3 clear radius statistics

This command is used to clear all RADIUS statistics.

| | |
|---------------|--------------------------------------|
| Format | <code>clear radius statistics</code> |
| Mode | Privileged EXEC |

11.1.4 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 | <code>dot1x defaultlogin <listname></code> |
| Mode | Global Config |

11.1.5 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 | <code>dot1x initialize <slot/port></code> |
| Mode | Privileged EXEC |

11.1.6 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 | <code>dot1x login <user> <listname></code> |
| Mode | Global Config |

11.1.7 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 | <code>dot1x max-req <count></code> |
| Mode | Interface Config |

11.1.7.1 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.

| | |
|---------------|-------------------------------|
| Format | <code>no dot1x max-req</code> |
| Mode | Interface Config |

11.1.8 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 | <code>dot1x port-control {force-unauthorized force-authorized auto}</code> |
| Mode | Interface Config |

11.1.8.1 no dot1x port-control

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

| | |
|---------------|------------------------------------|
| Format | <code>no dot1x port-control</code> |
| Mode | Interface Config |

11.1.9 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 modes:

- **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 | <code>dot1x port-control all {force-unauthorized force-authorized auto}</code> |
| Mode | Global Config |

11.1.9.1 no dot1x port-control all

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

| | |
|---------------|--|
| Format | <code>no dot1x port-control all</code> |
| Mode | Global Config |

11.1.10 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 | <code>dot1x re-authenticate <slot/port></code> |
| Mode | Privileged EXEC |

11.1.11 dot1x re-authentication

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

| | |
|----------------|-------------------------|
| Default | disabled |
| Format | dot1x re-authentication |
| Mode | Interface Config |

11.1.11.1 no dot1x re-authentication

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

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

11.1.12 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 |

11.1.12.1 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 |

11.1.13 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 | <code>dot1x timeout {{reauth-period <seconds>} {quiet-period <seconds>} {tx-period <seconds>} {supp-timeout <seconds>} {server-timeout <seconds>}}</code> |
| Mode | Interface Config |

11.1.13.1 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 | <code>no dot1x timeout {reauth-period quiet-period tx-period supp-timeout server-timeout}</code> |
| Mode | Interface Config |

11.1.14 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 | <code>dot1x user <user> {<slot/port> all}</code> |
| Mode | Global Config |

11.1.14.1 no dot1x user

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

| | |
|---------------|---|
| Format | <code>no dot1x user <user> {<slot/port> all}</code> |
| Mode | Global Config |

11.1.15 users defaultlogin

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

| | |
|---------------|--|
| Format | <code>users defaultlogin <listname></code> |
| Mode | Global Config |

11.1.16 users login

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

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete.

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

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

11.1.17 show authentication

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

| | |
|----------------------------------|--|
| Format | <code>show authentication</code> |
| Mode | Privileged EXEC |
| Authentication Login List | This displays the authentication login listname. |

| | |
|-----------------|---|
| Method 1 | This displays the first method in the specified authentication login list, if any. |
| Method 2 | This displays the second method in the specified authentication login list, if any. |
| Method 3 | This displays the third method in the specified authentication login list, if any. |

11.1.18 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. |

11.1.19 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 you use the optional [summary {<slot/port> | all}] parameter, 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 you use the optional `[detail <slot/port>]` parameter, 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, in seconds, has a range of 1 - 65535. |

| | |
|---------------------------------|--|
| Supplicant Timeout | The timer used by the authenticator state machine on this port to timeout the supplicant. The value, in seconds, has a range of 1 - 65535. |
| Server Timeout | The timer used by the authenticator on this port to timeout the authentication server. The value, in seconds, has a range of 1 - 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, in seconds, has a range of 1 - 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 you use the optional parameter *[statistics <slot/port>]*, the following dot1x statistics for the specified port appear.

| | |
|------------------------------------|---|
| 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.

11.1.20 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. |

11.1.21 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 | Lists every user that has an authentication login list assigned. |
| System Login | Displays the authentication login list assigned to the user for system login. |
| 802.1x Port Security | Displays the authentication login list assigned to the user for 802.1x port security. |

11.2 RADIUS Commands

This section describes the commands you use to configure the 7200 Series Managed Switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

11.2.1 radius accounting mode

Use this command to enable the RADIUS accounting function.

| | |
|----------------|-------------------------------|
| Default | disabled |
| Format | radius accounting mode |
| Mode | Global Config |

11.2.1.1 no radius accounting mode

Use this command to disable the RADIUS accounting function.

| | |
|---------------|----------------------------------|
| Format | no radius accounting mode |
| Mode | Global Config |

11.2.2 radius server host

Use this command to configure the RADIUS authentication and accounting server. If you use the *<auth>* parameter, the command configures the IP address to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the “no” form of the command.

If you use the optional *<port>* parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The *<port>* number range is 1 - 65535, with 1812 being the default value.



Note: To re-configure a RADIUS authentication server to use the default UDP *<port>*, set the *<port>* parameter to 1812.

If you use the *<acct>* parameter, the command configures the IP address to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the “no” form of the command to remove it from the configuration. The IP address you specify must match that of a previously configured accounting server.

If you use the optional *<port>* parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a *<port>* is already configured for the accounting server, the new *<port>* replaces the previously configured *<port>*. The *<port>* must be a value in the range 1 - 65535, with 1813 being the default.



Note: To re-configure a RADIUS accounting server to use the default UDP *<port>*, set the *<port>* parameter to 1813.

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

11.2.2.1 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 | <code>no radius server host {auth acct} <ipaddress></code> |
| Mode | Global Config |

11.2.3 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 is 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 is prompted.



Note: The secret must be an alphanumeric value not exceeding 16 characters.

| | |
|---------------|---|
| Format | <code>radius server key {auth acct} <ipaddr></code> |
| Mode | Global Config |

11.2.4 radius server msgauth

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

| | |
|---------------|---|
| Format | <code>radius server msgauth <ipaddr></code> |
| Mode | Global Config |

11.2.4.1 no radius server msgauth

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

| | |
|---------------|--|
| Format | <code>no radius server msgauth <ipaddr></code> |
| Mode | Global Config |

11.2.5 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 | <code>radius server primary <ipaddr></code> |
| Mode | Global Config |

11.2.6 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 | 4 |
| Format | <code>radius server retransmit <retries></code> |
| Mode | Global Config |

11.2.6.1 no radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted, to the default value.

| | |
|---------------|--|
| Format | <code>no radius server retransmit</code> |
| Mode | Global Config |

11.2.7 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 | 5 |
| Format | <code>radius server timeout <seconds></code> |
| Mode | Global Config |

11.2.7.1 no radius server timeout

This command sets the timeout value to the default value.

| | |
|---------------|---------------------------------|
| Format | no radius server timeout |
| Mode | Global Config |

11.2.8 show radius

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. Format

| | |
|-------------------------------------|--|
| | show radius [<i>servers</i>] |
| Mode | Privileged EXEC |
| Primary Server IP Address | Shows 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 you include the optional [*servers*] parameter, 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. |
| Message Authenticator | Enables or disables. the message authenticator attribute for the selected server. |

11.2.9 show radius accounting

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

Format `show radius 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 you include the optional `[statistics <ipaddr>]` parameter, 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. |

11.2.10 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 | <code>show radius statistics [ipaddr]</code> |
| Mode | Privileged EXEC |

If you do not specify an IP address, then only the Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

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

Chapter 12

Port-Channel/LAG (802.3ad) Commands

This section describes the Link Aggregation/Port-Channel (802.3ad) commands available in the 7200 Series Managed Switch CLI. Port channels are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address.

The Port-Channel/LAG Command section includes the following topics:

- [Section 12.1 “Port-Channel Configuration Commands” on page 12-1](#)
- [Section 12.2 “Port-Channel Show Commands” on page 12-6](#)

The commands in this section are in one of three 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.
- Clear commands clear some or all of the settings to factory defaults.

12.1 Port-Channel Configuration Commands

This section describes the commands you use to configure port-channels. Assign the LAG VLAN membership after you create a LAG. If you do not assign VLAN membership, the LAG might become a member of the management VLAN which can result in learning and switching issues.

12.1.1 addport

This command adds one port to the port-channel (LAG). The first interface is a logical unit, 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. For more information, see [Section 4.1.11 “speed” on page 4-5](#).

Format

addport <logical slot/port>

Mode

Interface Config

12.1.2 deleteport (Interface Config)

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

12.1.3 deleteport (Global Config)

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

Format

deleteport {<logical slot/port> | all}

Mode

Global Config

12.1.4 port-channel

This command configures a new port-channel and generates a logical slot/port number for the port-channel. The *<name>* field is a character string which allows the dash “-” character as well as alphanumeric characters. Display this number using the **show port channel** command.



Note: Before you include a port in a port-channel, set the port physical mode. For more information, see [Section 4.1.11 “speed” on page 4-5](#).

| | |
|---------------|---|
| Format | port-channel <i><name></i> |
| Mode | Global Config |

12.1.4.1 no port-channel

This command deletes a port-channel (LAG).

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

12.1.5 clear port-channel

Use this command to clear all configured port channels.

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

12.1.6 port-channel staticcapability

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

| | |
|----------------|--------------------------------------|
| Default | disabled |
| Format | port-channel staticcapability |
| Mode | Global Config |

12.1.6.1 no port-channel staticcapability

This command disables the support of static port-channels on the device.

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

12.1.7 port lacpmode

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

| | |
|----------------|----------------------------|
| Default | enabled |
| Format | <code>port lacpmode</code> |
| Mode | Interface Config |

12.1.7.1 no port lacpmode

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

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

12.1.8 port lacpmode all

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

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

12.1.8.1 no port lacpmode all

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

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

12.1.9 port-channel adminmode

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

| | |
|---------------|---|
| Format | <code>port-channel adminmode [all]</code> |
| Mode | Global Config |

12.1.9.1 no port-channel adminmode

This command disables a port-channel (LAG). The option **all** sets every configured port-channel with the same administrative mode setting.

| | |
|---------------|--|
| Format | <code>no port-channel adminmode [all]</code> |
| Mode | Global Config |

12.1.10 port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel, and *<name>* is an alphanumeric string up to 15 characters.

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

12.1.11 port-channel linktrap

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

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

12.1.11.1 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 | <code>no port-channel linktrap {<logical slot/port> all}</code> |
| Mode | Global Config |

12.2 Port-Channel Show Commands

This section describes the commands you use to view port-channel status and configuration information.

12.2.1 show port-channel

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

| | |
|--------------------------|--|
| Format | <code>show port-channel</code> |
| Modes | Privileged EXEC 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 <code><slot/port></code> notation. |
| Active Ports | This field lists the ports that are actively participating in this port-channel. |

12.2.2 show port-channel

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

| | |
|--------------------------|--|
| Format | <code>show port-channel {<logical slot/port> all}</code> |
| Modes | Privileged EXEC User EXEC |
| Logical Interface | Valid slot and port number separated by forward slashes. |
| Port-Channel Name | The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters. |
| Link State | Indicates whether the Link is up or down. |
| Admin Mode | May be enabled or disabled. The factory default is enabled. |

| | |
|-----------------------|---|
| Link Trap Mode | This object determines whether or not to send a trap when link status changes. The factory default is enabled. |
| STP Mode | The Spanning Tree Protocol Administrative Mode associated with the port or port-channel (LAG). The possible values are: Disable - Spanning tree is disabled for this port. Enable - Spanning tree is enabled for this port. |
| Mbr Ports | A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG). |
| Port Speed | Speed of the port-channel port. |
| Type | This field displays the status designating whether a particular port-channel (LAG) is statically or dynamically maintained. Static - The port-channel is statically maintained. Dynamic - The port-channel is dynamically maintained. |
| Active Ports | This field lists ports that are actively participating in the port-channel (LAG). |

Chapter 13

IGMP Snooping Commands

This section describes the Internet Group Management Protocol (IGMP) snooping commands available in the 7200 Series Managed Switch CLI.

The 7200 Series Managed Switch supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

This section contains the following topics:

- [Section 13.1 “IGMP Snooping Configuration Commands” on page 13-1](#)
- [Section 13.2 “IGMP Snooping Show Commands” on page 13-6](#)
- [Section 13.3 “IGMP Querier Commands” on page 13-9](#)

The commands in this section are in one of two groups:

- Show commands are used to display switch 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.

13.1 IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping.

13.1.1 ip igmpsnooping

This command enables IGMP Snooping on the system (Global Config Mode) or an interface (Interface Config Mode). This command also enables IGMP snooping on a particular VLAN and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

| | |
|----------------|--|
| Default | disabled |
| Format | <code>ip igmpsnooping <vlanId></code> |
| Modes | Global Config Interface Config VLAN Mode |

13.1.1.1 no ip igmpsnooping

This command disables IGMP Snooping on the system.

| | |
|---------------|--|
| Format | <code>no ip igmpsnooping <vlanId></code> |
| Modes | Global Config Interface Config VLAN Mode |

13.1.2 ip igmpsnooping interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

| | |
|----------------|--|
| Default | disabled |
| Format | <code>ip igmpsnooping interfacemode</code> |
| Mode | Global Config |

13.1.2.1 no ip igmpsnooping interfacemode

This command disables IGMP Snooping on all interfaces.

| | |
|---------------|---|
| Format | <code>no ip igmpsnooping interfacemode</code> |
| Mode | Global Config |

13.1.3 ip igmpsnooping groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

| | |
|----------------|---|
| Default | 260 seconds |
| Format | <code>ip igmpsnooping groupmembership-interval <vlanId> <2-3600></code> |
| Modes | Interface Config Global Config VLAN Mode |

13.1.3.1 no ip igmpsnooping groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

| | |
|---------------|--|
| Format | <code>no ip igmpsnooping groupmembership-interval</code> |
| Modes | Interface Config Global Config VLAN Mode |

13.1.4 ip igmpsnooping maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3599 seconds.

| | |
|----------------|---|
| Default | 10 seconds |
| Format | <code>ip igmpsnooping maxresponse <1-3599></code> |
| Modes | Global Config Interface Config VLAN Mode |

13.1.4.1 no ip igmpsnooping maxresponse

This command sets the IGMP Maximum Response time (on the interface or VLAN) to the default value.

| | |
|---------------|--|
| Format | <code>no ip igmpsnooping maxresponse</code> |
| Modes | Global Config Interface Config VLAN Mode |

13.1.5 ip igmpsnooping mcrtexptime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN.

This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

| | |
|----------------|--|
| Default | 0 |
| Format | <code>ip igmpsnooping mcrtexptime <vlanId> <0-3600></code> |
| Modes | Global Config Interface Config |

13.1.5.1 no ip igmpsnooping mcrtexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

| | |
|---------------|---|
| Format | <code>no ip igmpsnooping mcrtexpiretime <vlanId></code> |
| Modes | Global Config Interface Config |

13.1.6 ip igmp mrouter

This command configures the interface to only forward the snooped IGMP packets that come from VLAN ID (<vlanId>) to the multicast router mode attached to this interface. The command is not needed most of the time since the switch will automatically detect the presence of a multicast router and forward IGMP packets accordingly. It is only needed when you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

| | |
|----------------|---|
| Default | Disabled |
| Format | <code>ip igmp mrouter <vlanId></code> |
| Mode | Interface Config |

13.1.6.1 no ip igmp mrouter

This command disables the forwarding of IGMP packets to this interface.

| | |
|---------------|--|
| Format | <code>no ip igmp mrouter <vlanId></code> |
| Mode | Interface Config |

13.1.7 ip igmp mrouter interface

This command configures the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch will be forwarded to the multicast router reachable from this interface. The command is not needed most of the time since the switch will automatically detect the presence of multicast router and forward IGMP packet accordingly. It is only needed when you want to make sure the multicast router always receives IGMP packets from the switch in a complex network.

| | |
|----------------|--|
| Default | Disabled |
| Format | <code>ip igmp mrouter interface</code> |
| Mode | Interface Config |

13.1.7.1 no ip igmp mrouter interface

This command disables the forwarding of IGMP packets to a multicast router via this interface.

| | |
|---------------|---|
| Format | <code>no ip igmp mrouter interface</code> |
| Mode | Interface Config |

13.1.8 ip igmpsnooping unknown-multicast

This command enables the filtering of unknown multicast packets to the VLAN. Packets with an unknown mulicast address in the destination field will be dropped. This command is mainly used when IGMP snooping is enabled, to prevent flooding of unwanted multicast packets to every port.

| | |
|---------------|--|
| Format | <code>ip igmpsnooping unknown-multicast</code> |
| Mode | Global Config |

13.1.8.1 no ip igmpsnooping unknown-multicast

This command disables the filtering of unknown multicast packets. Unknown multicast packets will be flooded to all ports in the same VLAN.

| | |
|---------------|---|
| Format | <code>no ip igmpsnooping unknown-multicast</code> |
| Mode | Global Config |

13.2 IGMP Snooping Show Commands

This section describes the commands you use to view IGMP snooping status and information.

13.2.1 show ip igmp

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

| | |
|---------------|--|
| Format | <code>show ip igmp [<slot/port> <vlanId>]</code> |
| Mode | Privileged EXEC |

When the optional arguments <slot/port> or <vlanId> are not used, the command displays the following information:

| | |
|---|---|
| Admin Mode | This indicates whether or not IGMP Snooping is active on the switch. |
| Interfaces Enabled for IGMP Snooping | This is the list of interfaces on which IGMP Snooping is enabled. |
| Multicast Control Frame Count | This displays the number of multicast control frames that are processed by the CPU. |
| VLANS Enabled for IGMP Snooping | This is the list of VLANS on which IGMP Snooping is enabled. |

When you specify the *<slot/port>* values, the following information appears:

| | |
|---|--|
| IGMP Snooping Admin Mode | This indicates whether IGMP Snooping is active on the interface. |
| Fast Leave Mode | Indicates whether IGMP Snooping Fast-leave is active on the VLAN. |
| Group Membership Interval | Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured |
| Max Response Time | Displays the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured. |
| Multicast Router Present Expiration Time | Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured. |

When you specify a value for *<vlanid>*, the following additional information appears:

| | |
|------------------------|--|
| VLAN Admin Mode | Indicates whether IGMP Snooping is active on the VLAN. |
|------------------------|--|

13.2.2 show ip igmp mrouter interface

This command displays information about statically configured ports.

| | |
|----------------------------------|--|
| Format | <code>show ip igmp mrouter interface <slot/port></code> |
| Mode | Privileged EXEC |
| Interface | Shows the port on which multicast router information is being displayed. |
| Multicast Router Attached | Indicates whether multicast router is statically enabled on the interface. |
| VLAN ID | Displays the list of VLANs of which the interface is a member. |

13.2.3 show ip igmp mrouter vlan

This command displays information about statically configured ports.

| | |
|------------------|--|
| Format | <code>show ip igmp mrouter vlan <slot/port></code> |
| Mode | Privileged EXEC |
| Interface | Shows the port on which multicast router information is being displayed. |
| VLAN ID | Displays the list of VLANs of which the interface is a member. |

13.2.4 show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

| | |
|--------------------|--|
| Format | <code>show mac-address-table igmpsnooping</code> |
| Mode | Privileged EXEC |
| MAC Address | A multicast MAC address for which the switch has forwarding or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is |

| | |
|--------------------|---|
| | displayed as a MAC address and VLAN ID combination of 8 bytes. |
| Type | Displays the type of the entry, which is either static (added by the user) or dynamic (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:). |

13.3 IGMP Querier Commands

A switch configured as a querier will send general queries periodically to request group membership information from an attached network. These queries will invoke client response that can be used to build and refresh the multicast group membership state of systems (snooping entries of MFDB table) on the attached networks. Interested hosts shall respond to these queries by reporting their group membership state and this will result in creation of snooping entry in MFDB table.

The IGMP querier function supports IGMP Version 2.

The IGMP querier function must be enabled on VLAN basis.

IGMP snooping must be enabled on the switch for the querier function to be enabled.

When a VLAN is configured as a querier, IGMP query packets will be sent on every port, which is a member of the VLAN. If a multicast router is attached on a port (either detected dynamically or configured statically by the user) then the IGMP general query packet will not be sent to that port. A physical port on which IGMP query message is to be sent should fulfill the following criteria:

- Multicast router is not attached.
- Must not be the probe port of a mirroring session.
- Must not be a LAG member.
- Must not be enabled for routing.
- Must be in the Forwarding state.

The query packets that are sent periodically will have one of the following IP addresses for the source IP address field:

- VLAN Interface Address (for L3 switches only) 'or'

- IGMP Snooping Querier Address (a configurable globally) 'or'
- Switch Management Interface Address 'or'
- First configured interface address (for L3 switches only)

The switch will check for each of these IP addresses not being 0.0.0.0 in the specified order and choose the first such address. If all these IP addresses are found to be 0.0.0.0, no query packets are sent.

If multiple IGMP queriers reside on the VLAN the switch with lower IP address will remain active. Note that if the other querier is a multicast router it will continue sending queries and will not back off. The interval for the IGMP queries sent by the switch is configurable. Default is 60 seconds. Valid range shall be 1 to 18000 seconds. If the global querier mode is disabled IGMP querier function shall not be operational on any of the VLANs.

13.3.1 ip igmpsnooping querier

To enable IGMP querier function, use the **ip igmpsnooping querier** command. The command applies to the context in which it is executed (global or per VLAN). The <vlan-id> is the VLAN where IGMP querier will be sent.

| | |
|----------------|---|
| Format | <code>[no] ip igmpsnooping querier [<vlan-id>]</code> |
| Mode | Global Config, VLAN Database |
| Default | Disabled |

13.3.2 ip igmpsnooping querier ip-address

To configure the IP address <ipaddr> used by the IGMP querier function, use the **ip igmpsnooping querier ip-address** command and **no ip igmpsnooping querier ip-address** <ipaddr>. The <ipaddr> cannot be a class D or E address.

| | |
|----------------|--|
| Format | <code>ip igmpsnooping querier ip-address <ipaddr></code> <code>no ip igmpsnooping querier ip-address</code> |
| Mode | Global Config |
| Default | 0.0.0.0 |

13.3.3 ip igmpsnooping querier query-interval

To configure the IGMP querier query interval *<interval>* for a VLAN *<vlan-id>*, use the **ip igmpsnooping querier query-interval** command. Valid range for *<interval>* is 1 to 18000 seconds. *<Vlan-id>* must be a defined VLAN.

| | |
|----------------|---|
| Format | <code>[no] ip igmpsnooping querier query-interval <vlan-id> <interval></code> |
| Mode | Global Config |
| Default | interval, 60 |

13.3.4 show ip igmpsnooping querier

To display IGMP querier configuration information use **show ip igmpsnooping querier** command. To display global querier information use **show ip igmpsnooping querier**. To display VLAN specific querier information with the *<vlan-id>* option,

| | |
|---------------|---|
| Format | <code>show ip igmpsnooping querier [<vlan-id>]</code> |
| Mode | Privileged EXEC Mode |

Chapter 14

Quality of Service (QoS) Commands

This section describes the Quality of Service (QoS) commands available in the 7200 Series Managed Switch CLI.

This section contains the following topics:

- [Section 14.1 “Class of Service \(CoS\) Commands \(GSM7248 only\)” on page 14-2](#)
- [Section 14.2 “Differentiated Services \(DiffServ\) Commands” on page 14-8](#)
- [Section 14.3 “DiffServ Class Commands \(GSM7248 only\)” on page 14-9](#)
- [Section 14.4 “DiffServ Policy Commands \(GSM7248 only\)” on page 14-17](#)
- [Section 14.5 “DiffServ Service Commands \(GSM7248 only\)” on page 14-23](#)
- [Section 14.6 “DiffServ Show Commands” on page 14-25](#)
- [Section 14.7 “MAC Access Control List \(ACL\) Commands \(GSM7248 only\)” on page 14-31](#)
- [Section 14.8 “IP Access Control List \(ACL\) Commands \(GSM7248 only\)” on page 14-35](#)

The commands in this section are in one of two functional groups:

- 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.
- Show commands are used to display device settings, statistics and other information.

14.1 Class of Service (CoS) Commands (GSM7248 only)

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.



Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode apply to all interfaces.

14.1.1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *<userpriority>* and *<trafficclass>* values can both range from 0-7, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see [Section 6.3 “Provisioning \(IEEE 802.1p\) Commands” on page 6-14](#).

| | |
|---------------|---|
| Format | <code>classofservice dot1p-mapping <userpriority> <trafficclass></code> |
| Modes | Global Config Interface Config |

14.1.1.1 no classofservice dot1p-mapping

This command maps an 802.1p priority to a default internal traffic class value.

| | |
|---------------|--|
| Format | <code>no classofservice dot1p-mapping</code> |
| Modes | Global Config Interface Config |

14.1.2 classofservice ip-precedence-mapping

This command maps an IP precedence value to an internal traffic class. The *<ip-precedence>* and *<trafficclass>* values can both range from 0-7, although the actual number of available traffic classes depends on the platform.

| | |
|---------------|--|
| Format | <code>classofservice ip-precedence-mapping <ip-precedence> <trafficclass></code> |
| Modes | Global Config Interface Config |

14.1.2.1 no classofservice ip-precedence-mapping

This command maps an IP precedence value to a default internal traffic class value

| | |
|---------------|--|
| Format | <code>no classofservice ip-precedence-mapping</code> |
| Modes | Global Config Interface Config |

14.1.3 classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The `<ipdscp>` 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.

The `<trafficclass>` range is from 0-7.

| | |
|---------------|--|
| Format | <code>classofservice ip-dscp-mapping <ipdscp> <traffic-class></code> |
| Mode | Global Config |

14.1.3.1 no classofservice ip-dscp-mapping

This command maps an IP DSCP value to a default internal traffic class value.

| | |
|---------------|--|
| Format | <code>no classofservice ip-dscp-mapping</code> |
| Mode | Global Config |

14.1.4 classofservice trust

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings.

| | |
|---------------|---|
| Format | <code>classofservice trust <dot1p ip-dscp ip-precedence></code> |
| Mode | Global Config Interface Config |

14.1.4.1 no classofservice trust

This command sets the interface mode to untrusted.

| | |
|---------------|--------------------------------------|
| Format | <code>no classofservice trust</code> |
| Modes | Global Config Interface Config |

14.1.5 cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The total number of queues supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

| | |
|---------------|---|
| Format | cos-queue min-bandwidth <bw-0> <bw-1> ... <bw-n> |
| Modes | Global Config Interface Config |

14.1.5.1 no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

| | |
|---------------|-----------------------------------|
| Format | no cos-queue min-bandwidth |
| Modes | Global Config Interface Config |

14.1.6 cos-queue strict

This command activates the strict priority scheduler mode for each specified queue.

| | |
|---------------|--|
| Format | cos-queue strict <queue-id-1> [<queue-id-2> ... <queue-id-n>] |
| Modes | Global Config Interface Config |

14.1.6.1 no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

| | |
|---------------|---|
| Format | no cos-queue strict <queue-id-1> [<queue-id-2> ... <queue-id-n>] |
| Modes | Global Config Interface Config |

14.1.7 traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

| | |
|---------------|-----------------------------------|
| Format | traffic-shape <bw> |
| Modes | Global Config Interface Config |

14.1.7.1 no traffic-shape

This command restores the interface shaping rate to the default value.

| | |
|---------------|-----------------------------------|
| Format | no traffic-shape |
| Modes | Global Config Interface Config |

14.1.8 show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The unit/slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed. For more information, see [Section 6.3 “Provisioning \(IEEE 802.1p\) Commands” on page 6-14](#).

| | |
|---------------|---|
| Format | show classofservice dot1p-mapping [unit/slot/port] |
| Mode | Privileged EXEC |

The following information is repeated for each user priority.

| | |
|----------------------|---|
| User Priority | The 802.1p user priority value. |
| Traffic Class | The traffic class internal queue identifier to which the user priority value is mapped. |

14.1.9 show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The unit/slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show classofservice ip-precedence-mapping [unit/
slot/port]`

Mode Privileged EXEC

The following information is repeated for each user priority.

IP Precedence The IP Precedence value.

Traffic Class The traffic class internal queue identifier to which the IP Precedence value is mapped.



Note: This command is only supported on the GSM7248.

14.1.10 show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format `show classofservice ip-dscp-mapping`

Mode Privileged EXEC

The following information is repeated for each user priority.

IP DSCP The IP DSCP value.

Traffic Class The traffic class internal queue identifier to which the IP DSCP value is mapped.

14.1.11 show classofservice trust

This command displays the current trust mode setting for a specific interface. The unit/slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the port trust mode of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show classofservice trust [unit/slot/port]`

Mode Privileged EXEC

Non-IP Traffic Class

The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust ip-precedence.

**Untrusted Traffic
Class**

The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

14.1.12 show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The unit/slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

| | |
|------------------------------|---|
| Format | <code>show interfaces cos-queue [unit/slot/port]</code> |
| Mode | Privileged EXEC |
| Queue Id | An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent. |
| Minimum Bandwidth | The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value. |
| Scheduler Type | Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value. |
| Queue Management Type | The queue depth management technique used for this queue (tail drop). |

If you specify the interface, the following information also appears:

| | |
|-------------------------------|---|
| Interface | This displays the unit/slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication. |
| Interface Shaping Rate | The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value. |

14.2 Differentiated Services (DiffServ) Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
 - Creating and deleting classes.
 - Defining match criteria for a class.
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 an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference 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 switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.



Note: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

14.2.1 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 |

14.2.1.1 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 |

14.3 DiffServ Class Commands (GSM7248 only)

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)


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 that belongs to the class.

| | |
|---|---|
|  | Note: Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class. |
|---|---|


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

14.3.1 class-map

This command defines a DiffServ class of type match-all. When used without any match condition, this command enters the class-map mode. The *<class-map-name>* is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

| | |
|---|---|
|  | Note: The class-map-name 'default' is reserved and must not be used. |
|---|---|

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.

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

| | |
|---------------|--|
| Format | class-map match-all <i><class-map-name></i> |
| Mode | Global Config |

14.3.1.1 no class-map

This command eliminates an existing DiffServ class. The *<class-map-name>* is the name of an existing DiffServ class (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, the delete action fails.

| | |
|---------------|---|
| Format | no class-map <i><class-map-name></i> |
| Mode | Global Config |

14.3.2 class-map rename

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

| | |
|---------------|---|
| Format | class-map rename <code><class-map-name></code> <code><new-class-map-name></code> |
| Mode | Global Config |

14.3.3 match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The `<ethertype>` value is specified as one of the following keywords: `appletalk`, `arp`, `ibmsna`, `ipv4`, `ipv6`, `ipx`, `mplsmcast`, `mplsucast`, `netbios`, `novell`, `pppoe`, `rarp` or as a custom ethertype value in the range of 0x0600-0xFFFF.

| | |
|---------------|--|
| Format | match ethertype <code>{<keyword> / custom <0x0600-0xFFFF>}</code> |
| Mode | Class-Map Config |

14.3.4 match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

| | |
|---------------|------------------|
| Format | match any |
| Mode | Class-Map Config |

14.3.5 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.

| | |
|---------------|--|
| Format | match class-map <code><refclassname></code> |
| Mode | Class-Map Config |

The following rules apply to this command:

- The parameters `<refclassname>` and `<class-map-name>` can not be the same.
- Only one other class may be referenced by a class.

- Any attempts to delete the `<refclassname>` class while the class is still referenced by any `<class-map-name>` fails.
- The combined match criteria of `<class-map-name>` 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 fails.
- The total number of class rules formed by the complete reference class chain (including 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.

14.3.5.1 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.

| | |
|---------------|--|
| Format | <code>no match class-map <refclassname></code> |
| Mode | Class-Map Config |

14.3.6 match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

| | |
|----------------|------------------------------------|
| Default | none |
| Format | <code>match cos <0-7></code> |
| Mode | Class-Map Config |

14.3.7 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).

| | |
|----------------|---|
| Default | none |
| Format | <code>match destination-address mac <macaddr> <mac-mask></code> |
| Mode | Class-Map Config |

14.3.8 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 and must consist of a contiguous set of leading 1 bits.

| | |
|---------------|--|
| Format | <code>match dstip <ipaddr> <ipmask></code> |
| Mode | Class-Map Config |

14.3.9 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.

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*, *tftp*, *www*. Each of these translates into its equivalent port number. 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.

| | |
|---------------|--|
| Format | <code>match dstl4port {portkey <0-65535>}</code> |
| Mode | Class-Map Config |

14.3.10 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 *<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.

Format

match ip dscp *<dscpval>*

Mode

Class-Map Config

14.3.11 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.



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.

Format

match ip precedence *<0-7>*

Mode

Class-Map Config

14.3.12 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 *<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: This “free form” version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

Format

match ip tos *<tosbits>* *<tosmask>*

Mode

Class-Map Config

14.3.13 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. A value of ip matches 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.

Format

match protocol {*protocol-name* | <0-255>}

Mode

Class-Map Config

14.3.14 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 may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Default

none

Format

match source-address mac <address> <macmask>

Mode

Class-Map Config

14.3.15 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 and must consist of a contiguous set of leading 1 bits.

Format

match srcip <ipaddr> <ipmask>

Mode

Class-Map Config

14.3.16 match srcl4port

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.

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.

| | |
|---------------|--|
| Format | match srcl4port { <i>portkey</i> <i><0-65535></i> } |
| Mode | Class-Map Config |

14.3.17 match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 1 to 4095.

| | |
|----------------|---|
| Default | none |
| Format | match vlan <i><1-4095></i> |
| Mode | Class-Map Config |


14.4 DiffServ Policy Commands (GSM7248 only)

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

| | |
|---|--|
|  | <p>Note: 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.</p> |
|---|--|


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


To enter “Config-policy-map” mode, use the **policy-map** *<policy-name>* **in** command from Global Config mode.

To enter “Config-policy-classmap” mode, use the **class** *<class-name>* command from “Config-policy-map” mode.

14.4.1 policy-map

This command establishes a new DiffServ policy. The *<polycyname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the **in** parameter.

| | |
|---|--|
|  | <p>Note: The policy type dictates which of the individual policy attribute commands are valid within the policy definition.</p> |
|---|--|

| | |
|---|--|
|  | <p>Note: The CLI mode is changed to Policy-Map Config when this command is successfully executed.</p> |
|---|--|

| | |
|---------------|---|
| Format | policy-map <i><polycyname></i> in |
| Mode | Global Config |

14.4.1.1 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 delete attempt fails.

| | |
|---------------|--|
| Format | no policy-map <i><polycyname></i> |
| Mode | Global Config |

14.4.2 assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The queueid is an integer from 0 to n-1, where n is the number of egress queues supported by the device.

| | |
|--------------------------|--|
| Format | assign-queue <i><queueid></i> |
| Mode | Policy-Class-Map Config |
| Incompatibilities | Drop |

14.4.3 drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

| | |
|--------------------------|--|
| Format | drop |
| Mode | Policy-Class-Map Config |
| Incompatibilities | Assign Queue, Mark (all forms), Police |

14.4.4 conform-color

This command is used to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The `<class-map-name>` parameter is the name of an existing Diffserv class map.



Note: This command may only be used after specifying a police command for the policy-class instance.

Format

conform-color `<class-map-name>`

Mode

Policy-Class-Map Config

14.4.5 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: 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

14.4.5.1 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: This command removes the reference to the class definition for the specified policy.

| | |
|---------------|--|
| Format | no class <i><classname></i> |
| Mode | Policy-Map Config |

14.4.6 mark cos

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer in the range of 0 to 7.

| | |
|--------------------------|---|
| Default | 1 |
| Format | mark-cos <i><0-7></i> |
| Mode | Policy-Class-Map Config |
| Incompatibilities | Drop, Mark IP DSCP, IP Precedence, Police |

14.4.7 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 <i><dscpval></i> |
| Mode | Policy-Class-Map Config |
| Incompatibilities | Drop, Mark CoS, Mark IP Precedence, Police |

14.4.8 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 | Drop, Mark CoS, Mark IP DSCP, Police |

14.4.9 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 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) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-transmit, 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.

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. It is an integer from 0-7.

For set-cos-transmit an 802.1p priority value is required. It is 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> set-cos-transmit <0-7> transmit} [violate-action {drop set-prec-transmit <0-7> set-dscp-transmit <0-63> set-cos-transmit <0-7> transmit}]} |
| Mode | Policy-Class-Map Config |
| Incompatibilities | Drop, Mark (all forms) |

14.4.10 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

14.5 DiffServ Service Commands (GSM7248 only)

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

The CLI command root is `service-policy`.

14.5.1 service-policy

This command attaches a policy to an interface in the inbound direction. The `<polycyname>` parameter is the name of an existing DiffServ policy; it is defined by the **Policy-Map** command. This command causes a service to create a reference to the policy.



Note: This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.



Note: This command fails 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, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Format

service-policy in `<polycyname>`

Modes

Global Config
Interface Config



Note: You can only attach a single policy to a particular interface at any time.

14.5.1.1 no service-policy

This command detaches a policy from an interface in the inbound direction. The `<polycyname>` parameter is the name of an existing DiffServ policy; it is defined by the **Policy-Map** command.



Note: This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format

no service-policy in `<polycyname>`

Modes

Global Config
Interface Config

14.6 DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

14.6.1 show class-map (GSM7248 only)

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

| | |
|---------------|---|
| Format | show class-map <i><class-name></i> |
| Modes | Privileged EXEC User EXEC |

If the class-name is specified the following fields are displayed:

| | |
|-----------------------|---|
| Class Name | The name of this class. |
| Class Type | A class type of 'all' means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match. |
| Match Criteria | The Match Criteria fields are only displayed if they have been configured. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port. |
| Values | This field displays the values of the Match Criteria. |

If you do not specify the Class Name, 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 | A class type of 'all' means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match. |

| | |
|-----------------------|---|
| Ref Class Name | The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition. |
|-----------------------|---|

14.6.2 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 | Current number of entries (rows) in the Policy Instance Table. |
| Policy Instance Table Max | Maximum allowed entries (rows) for the Policy Instance Table. |
| Policy Attribute Table Size | Current number of entries (rows) in the Policy Attribute Table. |
| Policy Attribute Table Max | 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.

14.6.3 show policy-map (GSM7248 only)

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

Format

show 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 (Only inbound policy definitions are supported for this platform.)

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

Assign Queue

Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.

Class Name

The name of this class.

Committed Burst Size (KB)

This field displays the committed burst size, used in simple policing.

Committed Rate (Kbps)

This field displays the committed rate, used in simple 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 COS

This field shows the CoS mark value if the conform action is set-cos-transmit.

Conform DSCP Value

This field shows the DSCP mark value if the conform action is set-dscp-transmit.

**Conform IP
Precedence
Value**

This field shows the IP Precedence mark value if the conform action is set-prec-transmit.

Drop

Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.

Mark CoS

Denotes the class of service value that is set in the 802.1p header of inbound 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.

**Mark IP
Precedence**

Denotes the mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.

**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
COS**

This field displays the CoS mark value if the non-conform action is set-cos-transmit.

**Non-Conform
DSCP Value**

This field displays the DSCP mark value if the non-conform action is set-dscp-transmit.

**Non-Conform IP
Precedence
Value**

This field displays the IP Precedence mark value if the non-conform action is set-prec-transmit.

**Policing Style
Redirect**

This field denotes the style of policing, if any, used (simple). Forces a classified traffic stream to a specified egress port (physical port). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

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. (The order in which the policies are displayed is not necessarily the same order in which they were created.) |
| Policy Type | The policy type (Only inbound is supported). |
| Class Members | List of all class names associated with this policy. |

14.6.4 show diffserv service (GSM7248 only)

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

| | |
|----------------------------|---|
| Format | <code>show diffserv service <unit/slot/port> in</code> |
| 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 | Valid slot and port number separated by forward slashes. |
| Direction | The traffic direction of this interface service. |
| 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 <code>show policy-map <polycymapname></code> command (content not repeated here for brevity). |

14.6.5 show diffserv service brief (GSM7248 only)

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

| | |
|---------------|---|
| Format | <code>show diffserv service brief [in]</code> |
| 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 | Valid slot and port number separated by forward slashes. |
| Direction | The traffic direction of this interface service. |
| 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. |

14.6.6 show policy-map interface (GSM7248 only)

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



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

| | |
|---------------------------|--|
| Format | <code>show policy-map interface <unit/slot/port> [in]</code> |
| Mode | Privileged EXEC |
| Interface | Valid slot and port number separated by forward slashes. |
| Direction | The traffic direction of this interface service. |
| 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. |

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

| | |
|-----------------------------|---|
| Class Name | The name of this class instance. |
| In Discarded Packets | A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class. |

14.6.7 show service-policy (GSM7248 only)

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

| | |
|---------------|-------------------------------------|
| Format | <code>show service-policy in</code> |
| Mode | Privileged EXEC |

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

| | |
|---------------------------|--|
| Interface | Valid slot and port number separated by forward slashes. |
| Operational Status | The current operational status of this DiffServ service interface. |
| Policy Name | The name of the policy attached to the interface. |

14.7 MAC Access Control List (ACL) Commands (GSM7248 only)

This section describes the commands you use to configure MAC ACL settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IP ACL is hardware dependent.
- If you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

14.7.1 mac access-list extended

This command creates a MAC Access Control List (ACL) identified by `<name>`, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The `<name>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.



Note: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format

mac access-list extended <name>

Mode

Global Config

14.7.1.1 no mac access-list extended

This command deletes a MAC ACL identified by <name> from the system.

Format

no mac access-list extended <name>

Mode

Global Config

14.7.2 mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The <name> parameter is the name of an existing MAC ACL. The <newname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name <newname> already exists.

Format

mac access-list extended rename <name> <newname>

Mode

Global Config

14.7.3 {deny|permit}

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.



Note: The 'no' form of this command is not supported since the rules within a MAC ACL cannot be deleted individually. Instead, you must delete and re-specify the entire MAC ACL.



Note: An implicit 'deny all' MAC rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword `any` to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

You can specify the Ethertype value as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported `<ethertypekey>` values are: `appletalk`, `arp`, `ibmsna`, `ipv4`, `ipv6`, `ipx`, `mplsmcast`, `mplsucast`, `netbios`, `novell`, `pppoe`, `rarp`. Each of these translates into its equivalent Ethertype value(s), as shown in [Table 14-1](#).

Table 14-1. Ethertype Keyword and 4-digit Hexadecimal Value

| Ethertype Keyword | Corresponding Value |
|-------------------|---------------------|
| appletalk | 0x809B |
| arp | 0x0806 |
| ibmsna | 0x80D5 |
| ipv4 | 0x0800 |
| ipv6 | 0x86DD |
| ipx | 0x8037 |
| mplsmcast | 0x8848 |
| mplsucast | 0x8847 |
| netbios | 0x8191 |
| novell | 0x8137, 0x8138 |
| pppoe | 0x8863, 0x8864 |
| rarp | 0x8035 |

The `vlan` and `cos` parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed `<queue-id>` value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The `assign-queue` parameters are only valid for a 'permit' rule.



Note: The special command form `{deny|permit} any any` is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

| | |
|---------------|---|
| Format | <code>{deny permit} {<srcmac> any} {<dstmac> any} [<i><ethertypekey></i> <0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [assign-queue <queue-id>]</code> |
| Mode | Mac-Access-List Config |

14.7.4 mac access-group

This command attaches a specific MAC Access Control List (ACL) identified by *<name>* to an interface in a given direction. The *<name>* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

| | |
|---------------|---|
| Format | <code>mac access-group <name> in [sequence <1-4294967295>]</code> |
| Modes | Global Config Interface Config |

14.7.4.1 no mac access-group

This command removes a MAC ACL identified by *<name>* from the interface in a given direction.

| | |
|---------------|---|
| Format | <code>no mac access-list <name> in</code> |
| Modes | Global Config Interface Config |

14.7.5 show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. The [name] parameter is used to identify a specific MAC ACL to display.

| | |
|--------------------------------|--|
| Format | <code>show mac access-lists [name]</code> |
| Mode | Privileged EXEC |
| Rule Number | The ordered rule number identifier defined within the MAC ACL. |
| Action | Displays the action associated with each rule. The possible values are Permit or Deny. |
| Source MAC Address | Displays the source MAC address for this rule. |
| Destination MAC Address | Displays the destination MAC address for this rule. |
| Ethertype | Displays the Ethertype keyword or custom value for this rule. |
| VLAN ID | Displays the VLAN identifier value or range for this rule. |
| COS | Displays the COS (802.1p) value for this rule. |
| Assign Queue | Displays the queue identifier to which packets matching this rule are assigned. |
| Redirect Interface | Displays the unit/slot/port to which packets matching this rule are forwarded. |

14.8 IP Access Control List (ACL) Commands (GSM7248 only)

This section describes the commands you use to configure IP ACL settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- The 7200 Series Managed Switch does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is 100, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- If you configure a MAC ACL on an interface, you cannot configure an IP ACL on the same interface.

- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored.

14.8.1 access-list

This command creates an IP Access Control List (ACL) that is identified by the ACL number.

The IP ACL number is an integer from 1 to 99 for an IP standard ACL and from 100 to 199 for an IP extended ACL.

The IP ACL rule is specified with either a *permit* or *deny* action.

The protocol to filter for an IP ACL rule is specified by giving the protocol to be used like *icmp, igmp, ip, tcp, udp*.

The command specifies a source IP address and source mask for match condition of the IP ACL rule specified by the *srcip* and *srcmask* parameters.

The source layer 4 port match condition for the IP ACL rule is specified by the *port value* parameter. The range of values is from 0 to 65535.

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 IP address and destination mask for match condition of the IP ACL rule specified by the *dstip* and *dstmask* parameters.

The command specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp, precedence, tos/tosmask*.

The command specifies the assign-queue which is the queue identifier to which packets matching this rule are assigned.

Default none

IP Standard ACL:

Format `access-list <1-99> {deny | permit} {every | <srcip> <srcmask>} [assign-queue <queue-id>]`

Mode Global Config

IP Extended ACL:

| | |
|---------------|--|
| Format | access-list <100-199> {deny permit} {every {icmp igmp ip tcp udp <number>}} <srcip> <srcmask> [{eq {<portkey> <portvalue>}} <dstip> <dstmask> [{eq {<portkey> <portvalue>}}] [prece- dence <precedence> tos <tos> <tosmask> dscp <dscp>] [assign-queue <queue-id>] |
| Mode | Global Config |

14.8.1.1 no access-list

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

| | |
|---------------|--|
| Format | no access-list <accesslistnumber> |
| Mode | Global Config |

14.8.2 ip access-group

This command attaches a specified IP ACL to one interface or to all interfaces.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

| | |
|----------------|---|
| Default | none |
| Format | ip access-group <accesslistnumber> in [sequence <1-4294967295>] |
| Modes | Interface Config Global Config |

14.8.2.1 no ip access-group

This command removes a specified IP ACL from an interface.

| | |
|----------------|---|
| Default | none |
| Format | no ip access-group <accesslistnumber> in |
| Mode | Interface Config |

14.8.3 show ip access-lists

This command displays an IP ACL *<accesslistnumber>* is the number used to identify the IP ACL.

| | |
|---------------------------------|--|
| Format | show ip access-lists <i><accesslistnumber></i> |
| Mode | Privileged EXEC |
| Rule Number | This displays the number identifier for each rule that is defined for the IP 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 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 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). |

14.8.4 show access-lists

This command displays IP ACLs and MAC access control lists information for a designated interface and direction.

| | |
|-----------------|--|
| Format | show access-lists interface <i><unit/slot/port></i> in |
| Mode | Privileged EXEC |
| ACL Type | Type of access list (IP or MAC). |

ACL ID

Access List name for a MAC access list or the numeric identifier for an IP access list.

**Sequence
Number**

An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

Chapter 15

System Maintenance Commands

This section describes the system maintenance commands available in the 7200 Series Managed Switch CLI.

The System Maintenance Commands section includes the following subsections:

- [Section 15.1 “System Information and Statistics Commands” on page 15-1](#)
- [Section 15.2 “System Utility Commands” on page 15-17](#)
- [Section 15.3 “Logging Commands” on page 15-22](#)
- [Section 15.4 “CLI Command Logging Command” on page 15-27](#)
- [Section 15.5 “Configuration Scripting Commands” on page 15-28](#)

The commands in this section are in one of 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.

15.1 System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

15.1.1 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 | <code>show arp switch</code> |
| Mode | Privileged EXEC |
| MAC Address | A unicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB |
| IP Address | The IP address assigned to each interface. |
| Interface | Valid slot and port number separated by forward slashes. |

15.1.2 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. The [unit] is the switch identifier.

| | |
|----------------|---|
| Format | <code>show eventlog [unit]</code> |
| Mode | Privileged EXEC |
| File | The file in which the event originated. |
| Line | The line number of the event |
| Task Id | The task ID of the event. |
| Code | The event code. |
| Time | The time this event occurred. |
| Unit | The unit for the event. |



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

15.1.3 show hardware

This command displays inventory information for the switch.

| | |
|---------------|----------------------------|
| Format | <code>show hardware</code> |
| 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.revision number of the code currently running on the switch. |
| Operating System | The operating system currently running on the switch. |
| Network Processing Device | The type of the processor microcode. |
| Additional Packages | This displays the additional packages incorporated into this system. |

15.1.4 show interface

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

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



Note: For information about the format and output for **show interface ethernet**, see [Section 15.1.5 “show interface ethernet” on page 15-5](#).

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

**Packets Received
Without Error**

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

**Packets Received
With Error**

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

**Broadcast
Packets
Received**

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

**Packets
Transmitted
Without Error**

Total number of packets transmitted out the interface.

**Transmit Packets
Errors**

Number of outbound packets that could not be transmitted because of errors.

**Collisions
Frames**

Best estimate of the total number of collisions on this Ethernet segment.

**Time Since
Counters Last
Cleared**

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

If you use the `switchport` parameter, the following information appears:

**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 | Total number of packets transmitted out 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. |

15.1.5 show interface ethernet

This command displays detailed statistics for a specific interface 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>, are 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 Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled |
|-------------------------|---|

before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.

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

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

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

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

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

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

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

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

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

Packets Received Successfully

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

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

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

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

Packets Received with MAC Errors

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

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

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

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

Rx FCS Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a

bad Frame Check Sequence (FCS) with an integral number of octets

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

Received Packets Not Forwarded

Total - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process.

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

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

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

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

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

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

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

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

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

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

**Packets
Transmitted
Octets**

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

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

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

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

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

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

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

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

**Packets
Transmitted
Successfully**

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

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 sub-network-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.

Protocol Statistics

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.

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

Dot1x Statistics

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

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.

If you specify the *switchport* value, the following information appears:

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 sub-network-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.

15.1.6 show logging

This command displays the trap log that the switch maintains. The trap log contains a maximum of 256 entries that wrap.

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

| | |
|---|--|
| Format | <code>show logging</code> |
| Mode | Privileged EXEC |
| Number of Traps since last reset | The number of traps that have occurred since the last reset. |
| 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.) sets the counter 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. |

15.1.7 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 | <code>show mac-addr-table [<macaddr> all]</code> |
| Mode | Privileged EXEC |
| Mac Address | A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. |
| Interface | The port which this address was learned. |
| Interface 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 port number one 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 was learned via GMRP and applies to Multicast. |
| Other | The value of the instance does not fall into one of the other categories. |

15.1.8 clear mac-addr-table

This command clears the dynamically learned MAC addresses of the switch.

| | |
|---------------|-----------------------------------|
| Format | <code>clear mac-addr-table</code> |
| Mode | Privileged EXEC |

15.1.9 show running-config

Use this command to display/capture the current setting of different protocol packages supported on the switch. This command displays/captures commands with settings/configurations that differ from the default value. To display/capture the commands with settings/configurations that are equal to the default value, include the *[all]* option.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional *<scriptname>* is provided with a file name extension of “.scr”, the output is redirected to a script file.

If option *<changed>* is used, this command displays/capture commands with settings/configurations that differ from the default value.

| | |
|---------------|--|
| Format | show running-config <i>[all <scriptname> changed]</i> |
| Mode | Privileged EXEC |

15.1.10 terminal length

This command controls the number of lines to be displayed when running the **show running-config** command.

| | |
|---------------|--|
| Format | terminal length <i><1-24></i> |
| Mode | Privileged EXEC |

15.1.10.1 terminal no length

This command resets the number of lines displayed when running the **show running-config** command to the default value (18).

| | |
|---------------|---------------------------|
| Format | terminal no length |
| Mode | Privileged EXEC |

15.1.11 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. The factory default is blank. To configure the system name, see Section 10.1.1 “snmp-server” on page 10-1 . |
| System Location | Text used to identify the location of the switch. The factory default is blank. To configure the system location, see Section 10.1.1 “snmp-server” on page 10-1 . |
| System Contact | Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see Section 10.1.1 “snmp-server” on page 10-1 . |
| 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. |

15.2 System Utility Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

15.2.1 traceroute

Use the **traceroute** command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The *<ipaddr>* value should be a valid IP address. The [port] value should be a valid decimal integer in the range of 0(zero) to 65535. The default value is 33434.

The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system.

| | |
|---------------|--|
| Format | traceroute <i><ipaddr></i> [port] |
| Mode | Privileged EXEC |

15.2.2 clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter **y**, you automatically reset the switch.

| | |
|---------------|---------------------|
| Format | clear config |
| Mode | Privileged EXEC |

15.2.3 clear counters

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

| | |
|---------------|---|
| Format | clear counters { <i><slot/port></i> <i>all</i> } |
| Mode | Privileged EXEC |

15.2.4 clear igmpsnooping

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

| | |
|---------------|---------------------------|
| Format | clear igmpsnooping |
| Mode | Privileged EXEC |

15.2.5 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 |

15.2.6 enable passwd

This command prompts you to change the Privileged EXEC password.

| | |
|---------------|----------------------|
| Format | enable passwd |
| Mode | User EXEC |

15.2.7 clear port-channel

This command clears all port-channels (LAGs).

Format `clear port-channel`
Mode Privileged EXEC

15.2.8 clear traplog

This command clears the trap log.

Format `clear traplog`
Mode Privileged EXEC

15.2.9 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format `clear vlan`
Mode Privileged EXEC

15.2.10 copy

The `copy` command uploads and downloads files to and from the switch. You can upload and download files from a server by using TFTP, Xmodem, Ymodem, or Zmodem.

Format `copy <source> <destination>`
Mode Global Config

Replace the `<source>` and `<destination>` parameters with the options in [Table 15-1](#). For the `<url>` source or destination, use one of the following values:

`xmodem` | `ymodem` | `zmodem` | `tftp://<ipaddr>/<filepath>/<filename>`

For TFTP, the `<ipaddr>` parameter is the IP address of the server, `<filepath>` is the path to the file, and `<filename>` is the name of the file you want to upload or download.

Table 15-1. Copy Parameters


| Source | Destination | Description |
|--|--------------------------|---|
| <code>nvr:clibanner</code> | <code><url></code> | Copies the CLI banner to a server. |
| <code>nvr:errorlog</code> | <code><url></code> | Copies the error log file to a server. |
| <code>nvr:log</code> | <code><url></code> | Copies the log file to a server. |
| <code>nvr:script</code> <code><scriptname></code> | <code><url></code> | Copies a specified configuration script file to a server. |

Table 15-1. Copy Parameters (continued)

| Source | Destination | Description |
|--|---|--|
| nvr^{am}:startup-config | <code><url></code> | Copies the startup configuration to a server. |
| nvr^{am}:traplog | <code><url></code> | Copies the trap log file to a server. |
| system:running-config | nvr^{am}:startup-config | Saves the running configuration to nvr ^{am} . |
| <code><url></code> | nvr^{am}:clibanner | Downloads the CLI banner to the system. |
| <code><url></code> | nvr^{am}:script <code><destfilename></code> | Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file. |
| <code><url></code> | nvr^{am}:sshkeydsa | Downloads an SSH key file. For more information, see Section 3.5 “Secure Shell (SSH) Command” on page 3-15 . |
| <code><url></code> | nvr^{am}:sshkeyrsa1 | Downloads an SSH key file. |
| <code><url></code> | nvr^{am}:sshkeyrsa1 | Downloads an SSH key file. |
| <code><url></code> | nvr^{am}:sslpemroot | Downloads an HTTP secure-server certificate. For more information, see Section 3.6 “Hypertext Transfer Protocol (HTTP) Commands” on page 3-17 . |
| <code><url></code> | nvr^{am}:sslpemserver | Downloads an HTTP secure-server certificate. |
| <code><url></code> | nvr^{am}:sslpemdhweak | Downloads an HTTP secure-server certificate. |
| <code><url></code> | nvr^{am}:sslpemdhstrong | Downloads an HTTP secure-server certificate. |
| <code><url></code> | nvr^{am}:startup-config | Downloads the startup configuration file to the system. |
| <code><url></code> | system:image | Downloads a code image to the system. |

15.2.11 logout

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

| | |
|---|---|
|  | Note: Save configuration changes before logging out. |
|---|---|

| | |
|---------------|---------------------|
| Format | <code>logout</code> |
| Mode | Privileged EXEC |

15.2.12 ping

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. You can ping the switch from any IP workstation the switch is connected to 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 | <code>ping <ipaddr></code> |
| Modes | Privileged EXEC, User EXEC |

15.2.13 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. The LEDs on the switch indicate a successful reset.

| | |
|---------------|---------------------|
| Format | <code>reload</code> |
| Mode | Privileged EXEC |

15.3 Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

15.3.1 logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

| | |
|----------------|-------------------------------|
| Default | disabled; critical |
| Format | <code>logging buffered</code> |
| Mode | Global Config |

15.3.1.1 no logging buffered

This command disables logging to in-memory log.

| | |
|---------------|----------------------------------|
| Format | <code>no logging buffered</code> |
| Mode | Global Config |

15.3.2 logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

| | |
|----------------|------------------------------------|
| Default | enabled |
| Format | <code>logging buffered wrap</code> |
| Mode | Privileged EXEC |

15.3.2.1 no logging wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

| | |
|---------------|---------------------------------------|
| Format | <code>no logging buffered wrap</code> |
| Mode | Privileged EXEC |

15.3.3 logging console

This command enables logging to the console. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **informational** (6), or **debug** (7).

| | |
|----------------|---|
| Default | disabled; critical |
| Format | logging console [<i>severitylevel</i>] |
| Mode | Global Config |

15.3.3.1 no logging console

This command disables logging to the console.

| | |
|---------------|---------------------------|
| Format | no logging console |
| Mode | Global Config |

15.3.4 logging host

This command enables logging to a host. You can configure up to eight hosts. The *<ipaddr>* is the IP address of the logging host. The *<port>* value is a port number from 1 to 65535. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **informational** (6), or **debug** (7).

| | |
|----------------|---|
| Default | port - 514; level - critical; |
| Format | logging host <i><ipaddr></i> [<i><port></i>][<i><severitylevel></i>] |
| Mode | Global Config |

15.3.5 logging host remove

This command disables logging to host. See [Section 15.3.11 “show logging hosts” on page 15-26](#) for a list of host indexes.

| | |
|---------------|---|
| Format | logging host remove <i><hostindex></i> |
| Mode | Global Config |

15.3.6 logging port

This command sets the local port number of the LOG client for logging messages. The `<portid>` can be in the range from 1 to 65535.

| | |
|----------------|--|
| Default | 514 |
| Format | <code>logging port <portid></code> |
| Mode | Global Config |

15.3.6.1 no logging port

This command resets the local logging port to the default.

| | |
|---------------|------------------------------|
| Format | <code>no logging port</code> |
| Mode | Global Config |

15.3.7 logging syslog

This command enables syslog logging.

| | |
|----------------|-----------------------------|
| Default | disabled; local0 |
| Format | <code>logging syslog</code> |
| Mode | Global Config |

15.3.7.1 no logging syslog

This command disables syslog logging.

| | |
|---------------|--------------------------------|
| Format | <code>no logging syslog</code> |
| Mode | Global Config |

15.3.8 show logging

This command displays logging.

| | |
|--|--|
| Format | <code>show logging</code> |
| Mode | Privileged EXEC |
| Client Local Port | The port on the collector/relay to which syslog messages are sent. |
| Console Logging Administrative Mode | The mode for console logging. |

**Console Logging
Severity Filter**

The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.

**Buffered Logging
Administrative
Mode**

The mode for buffered logging.

**Buffered Logging
Severity Filter**

The minimum severity to log to the buffered log. Messages with an equal or lower numerical severity are logged.

**Historical Logging
Administrative
Mode**

The mode for historical logging.

**Historical Logging
Severity Filter**

The minimum severity to log to the historical log. Messages with an equal or lower numerical severity are logged.

**Syslog Logging
Administrative
Mode**

The mode for logging to configured syslog hosts. If set to disable logging stops to all syslog hosts.

**Log Messages
Received**

The number of messages received by the log process. This includes messages that are dropped or ignored

**Log Messages
Dropped**

The number of messages that could not be processed.

15.3.9 show logging buffered

This command displays buffered logging (system startup and system operation logs).

| | |
|--------------------------|---|
| Format | show logging buffered |
| Mode | Privileged EXEC |
| Admin Status | The current state of the in-memory log. |
| Component Filter | The component(s) from which received messages are to be logged to the in memory log. Either a single component id or “all components” may be specified. |
| Wrapping Behavior | The behavior of the In Memory log when faced with a log full situation. |
| Log Count | The count of valid entries in the buffered log. |

15.3.10 clear logging buffered

This command clears the messages maintained in the system log.

| | |
|---------------|-------------------------------|
| Format | clear logging buffered |
| Mode | Privileged EXEC |

15.3.11 show logging hosts

This command displays all configured logging hosts.

| | |
|-----------------------|---|
| Format | show logging hosts |
| Mode | Privileged EXEC |
| Host Index | (Used for deleting hosts) |
| Severity Level | The minimum severity to log to the specified address. |
| Port | Displays the server port number, which is the port on the local host from which syslog messages are sent. |
| Host Status | The state of logging to configured syslog hosts. If the status is disable, no logging occurs. |

15.3.12 show logging traplogs

This command displays SNMP trap events and statistics.

| | |
|--|---|
| Format | <code>show logging traplogs</code> |
| Mode | Privileged EXEC |
| Number of Traps Since Last Reset | Shows the number of traps since the last boot. |
| Trap Log Capacity | Shows the number of traps the system can retain. |
| Number of Traps Since Log Last Viewed | Shows the number of new traps since the command was last executed. |
| Log | Shows the log number. |
| System Time Up | Shows how long the system had been running at the time the trap was sent. |
| Trap | Shows the text of the trap message. |

15.4 CLI Command Logging Command

This section describes the commands you use to configure CLI Command Logging.

15.4.1 logging cli-command

This command enables the CLI command logging feature, which enables the 7200 Series Managed Switch software to log all CLI commands issued on the system.

| | |
|----------------|----------------------------------|
| Default | enabled |
| Format | <code>logging cli-command</code> |
| Mode | Global Config |

15.4.1.1 no logging cli-command

This command disables the CLI command Logging feature.

| | |
|---------------|-------------------------------------|
| Format | <code>no logging cli-command</code> |
| Mode | Global Config |

15.5 Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the **show running-config** command (see [Section 15.1.9 “show running-config” on page 15-16](#)) to capture the running configuration into a script. Use the **copy** command (see [Section 15.2.10 “copy” on page 15-19](#)) to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- Script files are not distributed across the stack, and only live in the unit that is the master unit at the time of the file download.
- The file extension must be “.scr”.
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script 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.

The following lines show an example of a script:

```
! Script file for displaying the ip interface
! Display information about interfaces
show ip interface 1/0/1 !Displays the information about the first
interface
! Display information about the next interface
show ip interface 1/0/2
! End of the script file
```

15.5.1 script apply

This command applies the commands in the script to the switch. The *<scriptname>* parameter is the name of the script to apply.

| | |
|---------------|---|
| Format | script apply <i><scriptname></i> |
| Mode | Global Config |

15.5.2 script delete

This command deletes a specified script where the *<scriptname>* parameter is the name of the script to delete. The *<all>* option deletes all the scripts present on the switch.

| | |
|---------------|---|
| Format | script delete { <i><scriptname></i> <i>all</i> } |
| Mode | Global Config |

15.5.3 script list

This command lists all scripts present on the switch as well as the remaining available space.

| | |
|-----------------------------|---------------------|
| Format | script list |
| Mode | Global Config |
| Configuration Script | Name of the script. |
| Size | Size of the script. |

15.5.4 show script

This command displays the contents of a script file, which is named *<scriptname>*.

| | |
|----------------------|--|
| Format | show script <i><scriptname></i> |
| Mode | Global Config |
| Output Format | line <i><number></i> : <i><line contents></i> |

15.5.5 script validate

This command validates a script file by parsing each line in the script file where *<scriptname>* is the name of the script to validate. The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

| | |
|---------------|---|
| Format | <code>script validate <scriptname></code> |
| Mode | Global Config |

15.6 Packet Capture

Packet capture commands assist in troubleshooting protocol-related problems with the management CPU. The packets to and from the management CPU can be captured in an internally allocated buffer area for export to a PC host for protocol analysis. Public domain packet analysis tools like Ethereal can be used to decode and review the packets in detail. Capturing can be performed in a variety of modes, either transmit-side only, receive-side only, or both. The number of packets captured will depend on the size of the captured packets.

15.6.1 capture transmit packet

This command enables the capturing of transmit packets.

| | |
|---------------|--------------------------------------|
| Format | <code>capture transmit packet</code> |
| Mode | Global Config |

15.6.1.1 no capture transmit packet

This command disables the capturing of transmit packets.

| | |
|---------------|---|
| Format | <code>no capture transmit packet</code> |
| Mode | Global Config |

15.6.2 capture receive packet

This command enables the capturing of receive packets.

| | |
|---------------|-------------------------------------|
| Format | <code>capture receive packet</code> |
| Mode | Global Config |

15.6.2.1 no capture transmit packet

This command disables the capturing of transmit packets.

| | |
|---------------|--|
| Format | <code>no capture receive packet</code> |
| Mode | Global Config |

15.6.3 capture all packets

This command enables the capturing of both transmit and receive packets.

| | |
|---------------|----------------------------------|
| Format | <code>capture all packets</code> |
| Mode | Global Config |

15.6.3.1 no capture all packets

This command disables the capturing of transmit and receive packets.

| | |
|---------------|-------------------------------------|
| Format | <code>no capture all packets</code> |
| Mode | Global Config |

15.6.4 capture wrap

This command enables the Buffer Wrapping configuration. Once the capture buffer is full, writes to the buffer will wrap around to allow continuous packet capture.

| | |
|----------------|---------------------------|
| Format | <code>capture wrap</code> |
| Mode | Global Config |
| Default | Enabled |

15.6.4.1 no capture all packets

This command disables the Buffer Wrapping configuration.

| | |
|---------------|------------------------------|
| Format | <code>no capture wrap</code> |
| Mode | Global Config |

15.6.5 show capture packets

This command displays packets being captured from the buffer. The output of the show command can be redirected to a text file. The resultant text file can be fed to the **text2pcap** utility or the Ethereal public domain packet analyzer, which can then be translated to a cap file

| | |
|---------------|-----------------------------------|
| Format | <code>show capture packets</code> |
| Mode | Global Config |

15.7 Dumping System Information

The **show tech-support** command dumps all major system information into a file that can be sent to NETGEAR product support for debugging purposes. The command output is not displayed on the console. Use the **copy** command to transfer the dumped file to the host PC.

| | |
|---------------|--------------------------|
| Format | show tech-support |
| Mode | Global Config |

15.8 Setting the Output Length of show running-config

By default, the output of the **show running-config** command pauses after every 18 lines of output. If you do not want the output to pause or you want to change the number of lines displayed, the following commands are provided to control output behavior.

15.8.1 terminal length

This command specifies how many lines of output to display on the console before pausing. When the value of 0 is used, the output will not pause.

| | |
|---------------|-------------------------------------|
| Format | terminal length <0-24> |
| Mode | Global Config |

15.8.2 terminal no length

This command resets the number of lines displayed by the **show running-config** command before pausing to the default value of 18.

| | |
|---------------|---------------------------|
| Format | terminal no length |
| Mode | Global Config |

Appendix A

Command Changes from Release 3 to Release 5

The following table summarizes the release 3.x.x.x commands that are changed on release 5.x.x.x.

| 3.0.3.4 Command | 5.0.1.9 (or newer) Equivalent Command |
|--|---|
| show igmpsnooping | show mac-address-table igmpsnooping |
| show ip brief | show ip |
| show ip interface brief | show ip interface |
| show ip ospf interface brief | show ip ospf interface |
| show ip ospf neighbor brief <unit/slot/port> | show ip ospf neighbor <unit/slot/port> |
| show ip ospf neighbor brief all | show ip ospf neighbor all |
| show ip ospf virtual-link brief | show ip ospf virtual-link |
| show ip vrrp interface brief | show ip vrrp interface |
| show monitor | show monitor session |
| show msglog | show logging buffered |
| show port-channel brief | show port-channel |
| show remotecon | show telnet |
| show service-policy | show service-policy in |
| show vlan brief | show vlan |
| copy nvram:msglog <url> | copy nvram:log <url> |
| remotecon maxsessions <0-5> | telnetcon maxsessions <0-5> |
| remotecon timeout <0-160> | telnetcon timeout <0-160> |
| vlan static <1-4094> | vlan makestatic |
| bootdhcprelay cidoptmode | ip dhcp relay information option |
| boothcprelay disable | no boothcprelay |
| set igmp | ip igmpsnooping |
| set igmp groupmembership-interval <2-3600> | ip igmpsnooping groupmembership-interval <2-3600> |
| set igmp interfacemode all | ip igmpsnooping interfacemode all |

| 3.0.3.4 Command | 5.0.1.9 (or newer) Equivalent Command |
|-------------------------------------|---------------------------------------|
| set igmp maxresponse <1-3599> | ip igmpsnooping maxresponse <1-3599> |
| set igmp mctrexpiretime <0-3600> | ip igmpsnooping minresponse <1-3599> |
| snmp-server enable traps | snmp-server traps |
| snmp-server enable traps bcaststorm | snmp-server traps bcaststorm |
| snmp-server enable traps linkmode | snmp-server traps linkmode |
| snmp-server enable traps multiusers | snmp-server traps multiusers |
| snmp-server enable traps stpmode | snmp-server traps stpmode |
| speed all 1000 full-duplex | (replaced by interface range command) |
| set igmp | ip igmpsnooping |