Command Line Interface Reference for the ProSafe 7300 Series Layer-3 Switches, Software Version 4.0

NETGEAR

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

Beta Draft 1
December 2005

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.

December 2005

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 7300 Series Layer-3 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 7300 Series Layer-3 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 dasProSafe 7300 Series Layer-3 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.

Note: Delete this note and the information below for products that are not wireless.

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter."

Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model FSM73xx/GSM73xx Cardbus Card Wireless Adapter complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

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

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

FCC Requirements for Operation in the United States

Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

ProSafe 7300 Series Layer-3 Managed Switch

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE
PY3WG111

Modifications made to the product, unless expressly approved byNETGEAR, Inc., could void the user's right to operate the equipment.

Export Restrictions

This product or software contains encryption code which may not be exported or transferred from the US or Canada without an approved US Department of Commerce export license.

Europe - EU Declaration of Conformity

CE 0560

This device is a 2.4 GHz low power RF device intended for home and office use in EU and EFTA member states. In some EU / EFTA member states some restrictions may apply. Please contact local spectrum management authorities for further details before putting this device into operation.

This product is certified for Switzerland and all EU countries. Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards: EN300 328, EN301 489-17, EN60950

Requirements For Operation in the European Community

Countries of Operation and Conditions of Use in the European Community

The user should run the client utility program provided with this product to check the current channel of operation and confirm that the device is operating in conformance with the spectrum usage rules for European Community countries as described in this section.

This device is intended to be operated in all countries of the European Community.

Operation Using 2.4 GHz Channels in France

The following radio channel usage limitations apply in France.

The radio spectrum regulator in France, Autorité de regulation des telecommunications (ART), enforces the following rules with respect to use of 2.4GHz spectrum in various locations in France. Please check ART's web site for latest requirements for use of the 2.4GHz band in France: http://www.art-telecom.fr/eng/index.htm. When operating in the following metropolitan regions (départements) in France, this device may be operated under the following conditions:

- Indoors using any channel in the 2.4-2.4835 GHz band (Channels 1-13)
- Outdoors using channels in the 2.4-2.454 GHz band (Channels 1-7)

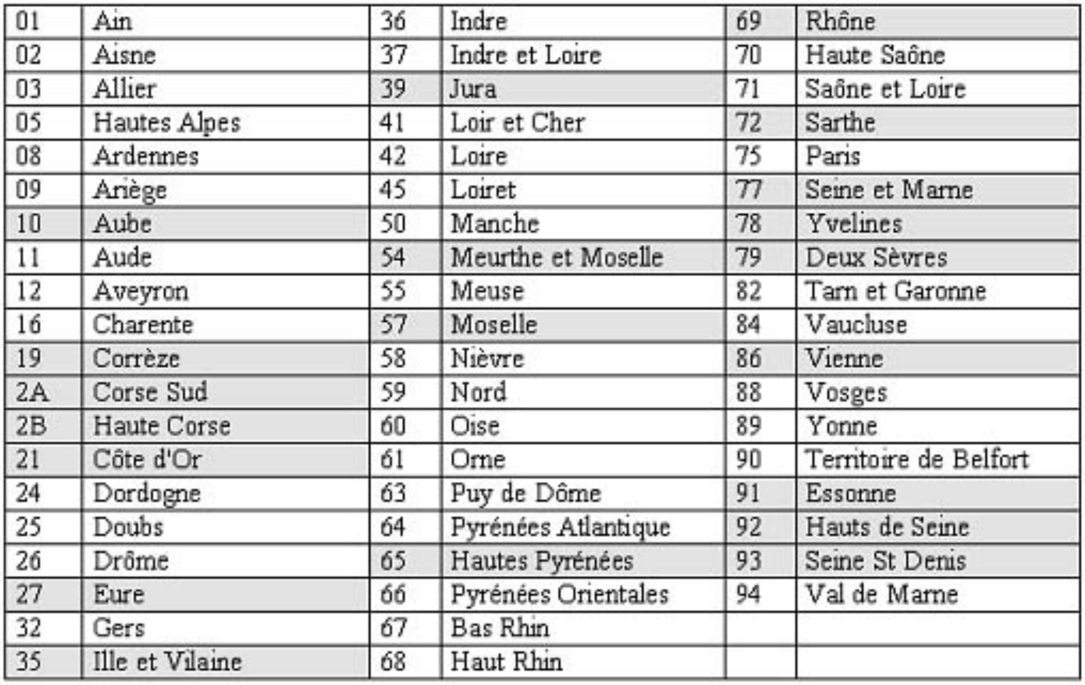
When operating outside of the following regions (départements) in France (see table below), this product must be operated under the following conditions:

- Indoors using channels in the 2.4465-2.4835 GHz band (Channels 10-13).

- Outdoor operation not permitted.

Refer to the ART web site for further details.

Metropolitan Regions with Eased Restrictions in 2.4GHz Band



01	Ain	36	Indre	69	Rhône
02	Aisne	37	Indre et Loire	70	Haute Saône
03	Allier	39	Jura	71	Saône et Loire
05	Hautes Alpes	41	Loir et Cher	72	Sarthe
08	Ardennes	42	Loire	75	Paris
09	Ariège	45	Loiret	77	Seine et Marne
10	Aube	50	Manche	78	Yvelines
11	Aude	54	Meurthe et Moselle	79	Deux Sèvres
12	Aveyron	55	Meuse	82	Tarn et Garonne
16	Charente	57	Moselle	84	Vaucluse
19	Corrèze	58	Nièvre	86	Vienne
2A	Corse Sud	59	Nord	88	Vosges
2B	Haute Corse	60	Oise	89	Yonne
21	Côte d'Or	61	Orne	90	Territoire de Belfort
24	Dordogne	63	Puy de Dôme	91	Essonne
25	Doubs	64	Pyrénées Atlantique	92	Hauts de Seine
26	Drôme	65	Hautes Pyrénées	93	Seine St Denis
27	Eure	66	Pyrénées Orientales	94	Val de Marne
32	Gers	67	Bas Rhin		
35	Ille et Vilaine	68	Haut Rhin		

Declaration of Conformity in Languages of the European Community

Finnish: Valmistaja NETGEAR, Inc. vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Dutch: Hierbij verklaart NETGEAR, Inc. dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

French: Par la présente NETGEAR, Inc. déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Swedish: Härmed intygar NETGEAR, Inc. att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Danish: Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

German: Hiermit erklärt NETGEAR, Inc., dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet.

Italian: Con la presente NETGEAR, Inc. dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Spanish: Por medio de la presente NETGEAR, Inc. declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

Portugese: NETGEAR, Inc. declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (ProSafe 7300 Series Layer-3 Managed Switch) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-WG111

Additional Copyrights

AES	Copyright (c) 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK. All rights reserved. TERMS Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission. This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.

Product and Publication Details

Model Number:	FSM73xx/GSM73xx
Publication Date:	December 2005
Product Family:	managed switch
Product Name:	ProSafe 7300 Series Layer-3 Managed Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	Beta Draft 1
Publication Version Number	1.0

Contents

Command Line Interface Reference for the ProSafe 7300 Series Layer-3 Switches, Software Version 4.0

Chapter 1
About This Manual

Chapter 2
Overview

Chapter 3
Administrative Access Commands

Chapter 4
Port and System Setup Commands

Chapter 5 Spanning Tree Protocol Commands

Chapter 6
VLAN Commands

Chapter 7
DHCP Commands

Chapter 10
SNMP Commands

Chapter 11
Port-Based Access and Authentication Commands

Chapter 12
Port-Channel/LAG (802.3ad) Commands

Chapter 13
Quality of Service (QoS) Commands

Chapter 14
Routing Commands

Chapter 15
IP Multicast Commands

Chapter 16
IGMP Snooping Commands

Chapter 17
Power Over Ethernet Commands

Chapter 18
System Maintenance Commands

Chapter 1
About This Manual

This chapter introduces the Command Line Interface Reference for the ProSafe 7300 Series Layer-3 Switches, Software Version 4.0. It describes the command-line interface (CLI) commands used to view and configure the 7300 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 7300 Series Managed Switch software. Software engineers who integrate 7300 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 7300 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 7300 Series Managed Switch according to these specifications:

Table 1-1. Manual Specifications

Product	ProSafe 7300 Series Layer-3 Managed Switch
Product Final Assembly Number	
Firmware Version Number	
Manual Part Number	Beta Draft 1
Manual Publication Date	December 2005

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

italics	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: Ignoring a warning could result in 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 [TOC] button that displays the table of contents and possibly an [Index] 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 [Knowledge Base] 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 you can choose one of the following several options, according to your needs.

- **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

Revision	Change Description

Chapter 2
Overview

The 7300 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

7300 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 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 2.2.1 “Command Syntax” on page 2-2
- Section 2.2.2 “Command Conventions” on page 2-2
- Section 2.2.3 “Unit-Slot-Port Naming Convention” on page 2-4
- Section 2.2.4 “Using the “No” Form of a Command” on page 2-5

- Section 2.2.5 "Command Modes" on page 2-5
- Section 2.2.6 "Entering CLI Commands" on page 2-8
- Section 2.2.7 "Using CLI Help" on page 2-10
- Section 2.2.8 "Accessing the CLI" on page 2-11

2.2.1 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.

2.2.2 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	*<value>*	Indicates that you must enter a value in place of the brackets and text inside them.
[] square brackets	*[value]*	Indicates an optional parameter that you can enter in place of the brackets and text inside them.
{} curly braces	*{choice1 | choice2}*	Indicates that you must select a parameter from the list of choices.
| Vertical bars	*choice1 | choice2*	Separates the mutually exclusive choices.
[{}] Braces within square brackets	*[{choice1} choice2}]*	Indicate a choice within an optional element.

2.2.2.1 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	This parameter is a valid IP address. You can enter the IP address in the following formats: **a** (32 bits) **a.b** (8.24 bits) **a.b.c** (8.8.16 bits) **a.b.c.d** (8.8.8.8) In addition to these formats, the CLI accepts decimal, hexidecimal and octal formats through the following input formats (where *n* is any valid hexidecimal, octal or decimal number): **0xn** (CLI assumes hexidecimal 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.

Table 2-2. Parameter Descriptions

Parameter	Description
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 <*routerid*> 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.
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.

2.2.3 Unit-Slot-Port Naming Convention

7300 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.

2.2.4 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.

2.2.5 Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific 7300 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.
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.

Table 2-5. CLI Command Modes (continued)

Command Mode	Prompt	Mode Description
Router RIP Config	`Switch (Config router)#`	Allows you to access the router RIP configuration commands.
Router BGP Config	`Switch (Config router)#`	Allows you to access the router BGP4 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 **`logout`**.
Privileged EXEC	From the User EXEC mode, enter **`enable`**.	To exit to the User EXEC mode, enter **`exit`** or press ***`Ctrl-Z`***.
Global Config	From the Privileged EXEC mode, enter **`configure`**.	To exit to the Privileged EXEC mode, enter **`exit`**, or press ***`Ctrl-Z`***.
VLAN Config	From the Privileged EXEC mode, enter **`vlan database`**.	To exit to the Privileged EXEC mode, enter **`exit`**, or press ***`Ctrl-Z`***.
Interface Config	From the Global Config mode, enter **`interface`** *`<slot/port>`*.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
Line Config	From the Global Config mode, enter **`lineconfig`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
Policy-Map Config	From the Global Config mode, enter **`policy-map`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
Policy-Class-Map Config	From the Policy Map mode enter **`class`**.	To exit to the Policy Map mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.

Table 2-6. CLI Mode Access and Exit

Command Mode	Access Method	Exit or Access Previous Mode
Class-Map Config	From the Global Config mode, enter **`class-map`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
Router OSPF Config	From the Global Config mode, enter **`router ospf`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
Router RIP Config	From the Global Config mode, enter **`router rip`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
Router BGP Config	From the Global Config mode, enter **`router bgp`** <*asnumber*>.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
MAC Access-list Config	From the Global Config mode enter **`mac access-list extended`** <*name*>.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
DHCP Pool Config	From the Global Config mode, enter **`ip dhcp pool`** <*name*>.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.
Stack Global Config Mode	From the Global Config mode, enter the **`stack`** command.	To exit to the Global Config mode, enter the **`exit`** command. To return to the Privileged EXEC mode, enter ***`Ctrl-Z`***.

2.2.6 Entering CLI Commands

The 7300 Series Managed Switch supports several features to help you enter commands.

2.2.6.1 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.

2.2.6.2 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.

2.2.6.3 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
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

Table 2-8. CLI Editing Conventions

Key Sequence	Description
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

2.2.7 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
```

2.2.8 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 7300 Series Managed Switch CLI.

This section contains the following topics:

- Section 3.1 “Network Interface Commands” on page 3-1
- Section 3.2 “Console Port Access Commands” on page 3-5
- Section 3.3 “Telnet Commands” on page 3-8
- Section 3.4 “Secure Shell (SSH) Command” on page 3-13
- Section 3.5 “Hypertext Transfer Protocol (HTTP) Commands” on page 3-15
- Section 3.6 “User Account Commands” on page 3-18

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.

➡	**Note:** The service port commands are for out-of-band network management using the dedicated service port on the platform. The network commands are used for in-band management using the data ports.

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	**`enable`**
Mode	User EXEC

3.1.2 serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port.

Format	**`serviceport ip`** *`<ipaddr> <netmask> [gateway]`*
Mode	Privileged EXEC

3.1.3 serviceport protocol

This command specifies the network management port configuration protocol. 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.

Format	**`serviceport protocol`** *`{none	bootp	dhcp}`*
Mode	Privileged EXEC

3.1.4 network parms

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	**`network parms`** *`<ipaddr> <netmask> [<gateway>]`*
Mode	Privileged EXEC

3.1.5 network mgmt_vlan

This command configures the Management VLAN ID.

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

3.1.5.1 no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format	**`no network mgmt_vlan`**
Mode	Privileged EXEC

3.1.6 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	**`network protocol`** *`{none	bootp	dhcp}`*
Mode	Privileged EXEC

3.1.7 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.

3.1.8 show serviceport

This command displays service port configuration information.

Format `show serviceport`

Mode Privileged 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
ServPort Configuration Protocol Current	Indicates what network protocol was used on the last, or current power-up cycle, if any.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.

3.2 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.

3.2.1 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	`configuration`
Mode	Privileged EXEC

3.2.2 lineconfig

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

Format	`lineconfig`
Mode	Global Config

3.2.3 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

3.2.3.1 no serial baudrate

This command sets the communication rate of the terminal interface.

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

3.2.4 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

3.2.4.1 no serial timeout

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

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

3.2.5 show serial

This command displays serial communication settings for the switch.

Format `show serial`

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.

3.3 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.

3.3.1 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	`telnet <host> <port> [debug] [line] [noecho]`
Modes	Privileged EXEC User EXEC

3.3.2 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	`transport input telnet`
Mode	Line Config

3.3.2.1 no transport input telnet

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

Format	`no transport input telnet`
Mode	Line Config

3.3.3 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	`transport output telnet`
Mode	Line Config

3.3.3.1 no transport output telnet

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

Format	`no transport output telnet`
Mode	Line Config

3.3.4 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	**`session-limit`** *`<0-5>`*
Mode	Line Config

3.3.4.1 no session-limit

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

Format	`no session-limit`
Mode	Line Config

3.3.5 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	**`session-timeout`** *`<0-160>`*
Mode	Line Config

3.3.5.1 no session-timeout

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

Format	**`no session-timeout`**
Mode	Line Config

3.3.6 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	**`telnetcon maxsessions`** *`<0-5>`*
Mode	Privileged EXEC

3.3.6.1 no telnetcon maxsessions

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

Format	**`no telnetcon maxsessions`**
Mode	Privileged EXEC

3.3.7 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	**`telnetcon timeout`** *`<1-160>`*
Mode	Privileged EXEC

3.3.7.1 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	**`no telnetcon timeout`**
Mode	Privileged EXEC

3.3.8 show telnet

This command displays the current outbound telnet settings.

Format	**`show telnet`**
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.

3.3.9 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.

3.4 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.

3.4.1 ip ssh

This command is used to enable SSH.

Default	disabled
Format	**`ip ssh`**
Mode	Privileged EXEC

3.4.1.1 no ip ssh

This command is used to disable SSH.

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

3.4.2 ip ssh protocol

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

Default	1 and 2
Format	**`ip ssh protocol`** *`[1] [2]`*
Mode	Privileged EXEC

3.4.3 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	**`sshcon maxsessions`** *`<0-5>`*
Mode	Privileged EXEC

3.4.3.1 no sshcon maxsessions

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

Format	**`no sshcon maxsessions`**
Mode	Privileged EXEC

3.4.4 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	**`sshcon timeout`** *`<1-160>`*
Mode	Privileged EXEC

3.4.4.1 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	**`no sshcon timeout`**
Mode	Privileged EXEC

3.4.5 show ip ssh

This command displays the ssh settings.

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

3.5 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.

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

3.5.1.1 no ip http secure-port

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

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

3.5.2 ip http secure-protocol

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

Default	SSL3 and TLS1
Format	**`ip http secure-protocol`** *`[SSL3] [TLS1]`*
Mode	Privileged EXEC

3.5.3 ip http secure-server

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

Default	disabled
Format	**`ip http secure-server`**
Mode	Privileged EXEC

3.5.3.1 no ip http secure-server

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

Format	**`no ip http secure-server`**
Mode	Privileged EXEC

3.5.4 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	**`ip http server`**
Mode	Privileged EXEC

3.5.4.1 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	**`no ip http server`**
Mode	Privileged EXEC

3.5.5 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

3.5.5.1 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

3.5.6 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.

3.6 User Account Commands

This section describes the commands you use to add, manage, and delete system users. The 7300 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.

3.6.1 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

3.6.1.1 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.

3.6.2 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

3.6.2.1 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

3.6.3 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

3.6.3.1 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

3.6.4 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** <*username*> *{none | md5 | sha}*
Mode	Global Config

3.6.4.1 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** <*username*>
Mode	Global Config

3.6.5 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** <*username*> *{none | des[key]}*
Mode	Global Config

3.6.5.1 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 `no users snmpv3 encryption <username>`

Mode Global Config

3.6.6 show loginsession

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

Format `show loginsession`

Mode Privileged EXEC

ID Login Session ID

User Name The name the user will use to login using the serial port or Telnet.

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.

3.6.7 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 `show users`

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 **`ReadOnly,`** 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.

3.6.8 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 7300 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 4-8
- Section 4.3 "Keying for Advanced Features" on page 4-9
- Section 4.4 "Simple Network Time Protocol (SNTP) Commands" on page 4-10
- Section 4.5 "MAC Address and MAC Database Commands" on page 4-15

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	**`interface`** *`<slot/port>`*
Mode	Global Config

4.1.2 cablestatus

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

Format	**`cablestatus`** *`<slot/port>`*
Mode	Privileged EXEC

4.1.3 auto-negotiate

This command enables automatic negotiation on a port.

Default	enabled
Format	**`auto-negotiate`**
Mode	Interface Config

4.1.3.1 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

4.1.4 auto-negotiate all

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

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

4.1.4.1 no auto-negotiate all

This command disables automatic negotiation on all ports.

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

4.1.5 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 14-12.

Default	1518 (untagged)
Format	**`mtu`** *<1518-9216>*
Mode	Interface Config

4.1.5.1 no mtu

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

Format	**`no mtu`**
Mode	Interface Config

4.1.6 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	**`shutdown`**
Mode	Interface Config

4.1.6.1 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

4.1.7 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

4.1.7.1 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

4.1.8 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

4.1.9 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

4.1.10 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

4.1.10.1 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 `no monitor session` *`<session-id>`*

Mode Global Config

4.1.11 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.

Note: This is a stand-alone “no” command. This command does not have a “normal” form.

Default enabled

Format `no monitor`

Mode Global config

4.1.12 show monitor session

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

Format `show monitor session` *`<sessionid>`*

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.

4.1.13 show port

This command displays port information.

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

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.

4.1.14 show port protocol

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

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

Mode Privileged EXEC

Group Name This field displays the group name of an entry in the Protocol-based VLAN table.

Group ID This field displays the group identifier of the protocol group.

Protocol(s) This field indicates the type of protocol(s) for this group.

VLAN This field indicates the VLAN associated with this Protocol Group.

Interface(s) This field lists the slot/port interface(s) that are associated with this Protocol Group.

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> **`nvram:clibanner`**

`copy nvram: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 Keying for Advanced Features

This section describes the commands you use to enter the licence key to access advanced features. You cannot access the advanced features without a valid license key.

4.3.1 license advanced

This command enables a particular feature. This command also enables the corresponding show commands for a feature.

> **Note:** If the feature is enabled, the feature is visible in the output of the **`show running-config`** command. The <*key*> parameter specifies the hexadecimal key for the feature.

Format	**`license advanced`** <*key*>
Mode	Privileged EXEC

4.3.1.1 no license advanced

This command disables a particular feature. This command also disables the corresponding show commands. The <*key*> parameter specifies the hexadecimal key for the feature.

Format	**`no license advanced`** <*key*>
Mode	Privileged EXEC

4.3.2 show key-features

This command displays the enabled or disabled status for all keyable features.

Format	**`show key-features`**
Modes	Privileged EXEC User EXEC
Function	This is the name of the keyable component or feature.
Status	Enabled or disabled.

4.4 Simple Network Time Protocol (SNTP) Commands

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

4.4.1 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	**`sntp broadcast client poll-interval`** *`<poll-interval>`*
Mode	Global Config

4.4.1.1 no sntp broadcast client poll-interval

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

Format	**`no sntp broadcast client poll-interval`**
Mode	Global Config

4.4.2 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	**`sntp client mode`** *`[broadcast | unicast]`*
Mode	Global Config

4.4.2.1 sntp client mode

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

Format	**`no sntp client mode`**
Mode	Global Config

4.4.3 sntp client port

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

Default	123
Format	**`sntp client port`** *`<portid>`*
Mode	Global Config

4.4.3.1 no sntp client port

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

Format	**`no sntp client port`**
Mode	Global Config

4.4.4 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.

Default	6
Format	**`sntp unicast client poll-interval`** *`<poll-interval>`*
Mode	Global Config

4.4.4.1 no sntp unicast client poll-interval

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

Format	**`no sntp unicast client poll-interval`**
Mode	Global Config

4.4.5 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	**`sntp unicast client poll-timeout`** *`<poll-timeout>`*
Mode	Global Config

4.4.5.1 no sntp unicast client poll-timeout

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

Format	**`no sntp unicast client poll-timeout`**
Mode	Global Config

4.4.6 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	**`sntp unicast client poll-retry`** *`<poll-retry>`*
Mode	Global Config

4.4.6.1 no sntp unicast client poll-retry

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

Format	**`no sntp unicast client poll-retry`**
Mode	Global Config

4.4.7 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	**`sntp multicast client poll-interval`** *`<poll-interval>`*
Mode	Global Config

4.4.7.1 no sntp multicast client poll-interval

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

Format	**`no sntp multicast client poll-interval`**
Mode	Global Config

4.4.8 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

4.4.8.1 no sntp server

This command deletes an server from the configured SNTP servers.

Format `no sntp server remove <ipaddress>`

Mode Global Config

4.4.9 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

4.4.10 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.

4.4.11 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.

4.5 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.

4.5.1 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	**`network mac-address`** *`<macaddr>`*
Mode	Privileged EXEC

4.5.2 network mac-type

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

Default	burnedin
Format	**`network mac-type`** *`{local	burnedin}`*
Mode	Privileged EXEC

4.5.2.1 no network mac-type

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

Format	**`no network mac-type`**
Mode	Privileged EXE

4.5.3 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

4.5.3.1 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

4.5.4 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

4.5.4.1 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

4.5.5 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 | <macaddr> <vlanid>}*
Mode	Global Config

4.5.5.1 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 | <macaddr> <vlanid>}*
Mode	Global Config

4.5.6 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`**

4.5.6.1 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	**no macfilter addsrc** *<macaddr> <vlanid>*
Mode	**Interface Config**

4.5.7 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	**macfilter addsrc** *{all | <macaddr> <vlanid>}*
Mode	**Global Config**

4.5.7.1 no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of <*macaddr*> and VLAN of <*vlanid*>. 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	**no macfilter addsrc** *{all | <macaddr> <vlanid>}*
Mode	**Global Config**

4.5.8 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 (*`fdbid`*) indicates which forwarding database's aging timeout is being configured. Use the *`all`* option to configure the agetime of all forwarding databases.

4.5.8.1 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.

4.5.9 show forwardingdb agetime

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

Default all

Format **`show forwardingdb agetime`** *`[fdbid | all]`*

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.

4.5.10 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 `show mac-address-table multicast <macaddr>`

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.

4.5.11 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 `show mac-address-table static {<macaddr> <vlanid> | all}`

Mode Privileged EXEC

MAC Address	Is the MAC Address of the static MAC filter entry.
VLAN ID	Is the VLAN ID of the static MAC filter entry.
Source Port(s)	Indicates the source port filter set's slot and port(s).
Destination Port(s)	Indicates the destination port filter set's slot and port(s).

4.5.12 show mac-address-table staticfiltering

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

Format `show mac-address-table staticfiltering`

Mode Privileged EXEC

Mac Address 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:).

4.5.13 show mac-address-table stats

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

Format `show mac-address-table stats`

Mode Privileged EXEC

Total Entries 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.

Chapter 5 Spanning Tree Protocol Commands

This section describes the spanning tree protocol (STP) commands available in the 7300 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 disabled by default. When you enable STP on the switch, STP is still disabled on each port.

If STP is disabled, the system does not forward BPDU messages.

5.1.1 spanning-tree

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

Default	disabled
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	**`spanning-tree configuration revision`** *`<0-65535>`*
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	**`no spanning-tree configuration revision`**
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	**`spanning-tree edgeport`**
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	**`no spanning-tree edgeport`**
Mode	Interface Config

5.1.6 spanning-tree forceversion

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

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

Default	802.1s
Format	**`spanning-tree forceversion`** *`<802.1d | 802.1w | 802.1s>`*
Mode	Global Config

5.1.6.1 no spanning-tree forceversion

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

Format	**`no spanning-tree forceversion`**
Mode	Global Config

5.1.7 spanning-tree forward-time

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

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

5.1.7.1 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	**`no spanning-tree forward-time`**
Mode	Global Config

5.1.8 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 *(Bridge Max Age / 2)* - *1*.

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

5.1.8.1 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	**`no spanning-tree hello-time`**
Mode	Interface Config

5.1.9 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 x (Bridge Forward Delay* - *1)*.

Default	20
Format	**`spanning-tree max-age`** *<6-40>*
Mode	Global Config

5.1.9.1 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	**`no spanning-tree max-age`**
Mode	Global Config

5.1.10 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	**`spanning-tree max-hops`** *`<1-127>`*
Mode	Global Config

5.1.10.1 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	**`no spanning-tree max-hops`**
Mode	Global Config

5.1.11 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	**`spanning-tree mst`** *`<mstid> {{cost <1-200000000>	auto} |`* *`{external-cost <1-200000000>	auto}| port-priority <0-240>}`*
Mode	Interface Config

5.1.11.1 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

5.1.12 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

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

5.1.13 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	`spanning-tree mst priority` <*mstid*> <*0-61440*>
Mode	Global Config

5.1.13.1 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	`spanning-tree mst priority` <*mstid*>
Mode	Global Config

5.1.14 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	`spanning-tree mst vlan <mstid> <vlanid>`
Mode	Global Config

5.1.14.1 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	`no spanning-tree mst vlan <mstid> <vlanid>`
Mode	Global Config

5.1.15 spanning-tree port mode

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

Default	disabled
Format	`spanning-tree port mode`
Mode	Interface Config

5.1.15.1 no spanning-tree port mode

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

Format	`no spanning-tree port mode`
Mode	Interface Config

5.1.16 spanning-tree port mode all

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

Default	disabled
Format	`spanning-tree port mode all`
Mode	Global Config

5.1.16.1 no spanning-tree port mode all

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

Format `no spanning-tree port mode all`

Mode Global Config

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 **`show spanning-tree`** <*brief*>

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 `show spanning-tree interface` <*slot/port*>

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 `show spanning-tree mst port detailed <mstid> <slot/port>`

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 `show spanning-tree vlan <vlanid>`

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 7300 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:

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	**`vlan database`**
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` *`{vlanonly	all}`*
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	`vlan name` *<2-4094> <name>*
Mode	VLAN Config

6.1.7.1 no vlan name

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

Format	`no vlan name` *<2-4094>*
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	`vlan participation` *{exclude | include | auto} <1-4094>*
Mode	Interface Config

Participation options are:

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

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	**`no vlan port acceptframe all`**
Mode	Global Config

6.1.11 vlan port pvid all

This command changes the VLAN ID for all interface.

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

6.1.11.1 no vlan port pvid all

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

Format	**`no vlan port pvid`** *`all`*
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	**`vlan port tagging all`** *`<1-4094>`*
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	**`no vlan port tagging all`**
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	**`vlan port ingressfilter all`**
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	**`no vlan port ingressfilter all`**
Mode	**6.1.14 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	**`vlan protocol group`** <*groupname*>
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	**`vlan protocol group add protocol`** <*groupid*> <*protocol*>
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	**`protocol vlan group`** <*groupid*>
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	**`no protocol vlan group`** <*groupid*>
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	**`protocol vlan group all`** <*groupid*>
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	**`no protocol vlan group all`** <*groupid*>
Mode	Global Config

6.1.21 vlan pvid

This command changes the VLAN ID per interface.

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

Format `show vlan <vlanid>`

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

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

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

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

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

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

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

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

Tagging Select the tagging behavior for this port in this VLAN.

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

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

6.2.2 show vlan brief

This command displays a list of all configured VLANs.

Format `show vlan brief`

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).

6.2.3 show vlan port

This command displays VLAN port information.

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

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	**`vlan port priority all`** *`<priority>`*
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	**`vlan priority`** *`<priority>`*
Mode	Interface Config

Chapter 7
DHCP Commands

This section describes the DHCP commands available in the 7300 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 7-16

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	**`ip dhcp pool`** *<name>*
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	**`no ip dhcp pool`** *<name>*
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	**`client-identifier`** *<uniqueidentifier>*
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`** *`<code>`*
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`** *`<lowaddress> [highaddress]`*
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`** *`<lowaddress> [highaddress]`*
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	`ip dhcp ping packets <0,2-10>`
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	`no ip dhcp ping packets`
Mode	Global Config

7.2.3 service dhcp

This command enables the DHCP server.

Default	disabled
Format	`service dhcp`
Mode	Global Config

7.2.3.1 no service dhcp

This command disables the DHCP server.

Format	`no service dhcp`
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	`ip dhcp bootp automatic`
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	`no ip dhcp bootp automatic`
Mode	Global Config

7.2.5 ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default	enabled
Format	`ip dhcp conflict logging`
Mode	Global Config

7.2.5.1 no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format	`no ip dhcp conflict logging`
Mode	Global Config

7.3 DHCP Server Clear and Show Commands

This section describes the commands you 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	**`clear ip dhcp binding`** *`{address	*}`*
Mode	Privileged EXEC

7.3.2 clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format	**`clear ip dhcp server statistics`**
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	**`clear ip dhcp conflict`** *`{<address>	*}`*
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 `show ip dhcp binding` *[address]*

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 `show ip dhcp global configuration`

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 **`show ip dhcp pool configuration`** *`{<name> | all}`*

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 `show ip dhcp server statistics`

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`** *`[ip-address]`*
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 bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Default	disabled
Format	**`bootpdhcprelay cidoptmode`**
Mode	Global Config

7.4.1.1 no bootpdhcprelay cidoptmode

This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

Format	**`no bootpdhcprelay cidoptmode`**
Mode	Global Config

7.4.2 bootpdhcprelay enable

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

Default	disabled
Format	**`bootpdhcprelay enable`**
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	**`no bootpdhcprelay enable`**
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	**`bootpdhcprelay maxhopcount`** *<1-16>*
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	**`no bootpdhcprelay maxhopcount`**
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	**`bootpdhcprelay minwaittime`** *`<0-100>`*
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	**`no bootpdhcprelay minwaittime`**
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	**`bootpdhcprelay serverip`** *`<ipaddr>`*
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	**`no bootpdhcprelay serverip`**
Mode	Global Config

7.4.6 show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format `show bootpdhcprelay`

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 or requests received.

Requests Relayed Is the number of requests relayed.

Packets Discarded Is the number of packets discarded.

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 7300 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:

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	**`set garp timer leave`** *<20-600>*
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	**`no set garp timer leave`**
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	**`set garp timer leaveall`** *`<200-6000>`*
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	**`no set garp timer leaveall`**
Modes	Interface Config Global Config

8.1.4 show garp

This command displays GARP information.

Format	**`show garp`**
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	`set gvrp adminmode`
Mode	Privileged EXEC

8.2.1.1 no set gvrp adminmode

This command disables GVRP.

Format	`no set gvrp adminmode`
Mode	Privileged EXEC

8.2.2 set gvrp interfacemode

This command enables GVRP.

Default	disabled
Format	`set gvrp interfacemode`
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 `no set gvrp interfacemode`

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

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 centisec-

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 gmrp

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

Format `show mac-address-table gmrp`

Mode Privileged EXEC

Mac Address A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address 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 7300 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 enable traps violation” on page 10-5.

9.1.1 port-security

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

Default	disabled
Format	**`port-security`**
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	**`no port-security`**
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	**`port-security max-dynamic`** *`<maxvalue>`*
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	**`no port-security max-dynamic`**
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	**`port-security max-static`** *`<maxvalue>`*
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	**`no port-security max-static`**
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	**`port-security mac-address`** *`<mac-address> <vid>`*
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	**`no port-security mac-address`** *`<mac-address> <vid>`*
Mode	Interface Config

9.1.5 port-security mac-address move

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

Format	**`port-security mac-address move`**
Mode	Interface Config

9.1.6 show port-security

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

Format	`show port-security`
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	`show port-security <interface	all>`
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	`show port-security dynamic <interface>`
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	`show port-security static <interface>`
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	**`show port-security violation`** *`<interface>`*
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

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

9.2.2 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	`storm-control flowcontrol`
Mode	Global Config

9.2.2.1 no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

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

Format	`no storm-control flowcontrol`
Mode	Global Config

9.2.3 show storm-control

This command displays switch configuration information.

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

Chapter 10
SNMP Commands

This section describes the SNMP commands available in the 7300 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	`snmp-server {sysname <name> | location <loc> | contact <con>}`
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	`snmp-server community <name>`
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	`no snmp-server community <name>`
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	`snmp-server community ipaddr <ipaddr> <name>`
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	**`no snmp-server community ipaddr`** *<name>*
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	**`snmp-server community ipmask`** *<ipmask> <name>*
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	**`no snmp-server community ipmask`** *<name>*
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	**`snmp-server community mode`** <*name*>
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 enable 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 enable traps violation`
Mode	Interface Config

10.1.8.1 no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format	`no snmp-server enable traps violation`
Mode	Interface Config

10.1.9 snmp-server enable traps

This command enables the Authentication Flag.

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

10.1.9.1 no snmp-server enable traps

This command disables the Authentication Flag.

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

10.1.10 snmp-server enable traps bcaststorm

This command enables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

Default	enabled
Format	`snmp-server enable traps bcaststorm`
Mode	Global Config

10.1.10.1 no snmp-server enable traps bcaststorm

This command disables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

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

10.1.11 snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. Section 10.1.18 “snmp trap link-status” on page 10-9

Default	enabled
Format	`snmp-server enable traps linkmode`
Mode	Global Config

10.1.11.1 no snmp-server enable traps linkmode

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

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

10.1.12 snmp-server enable traps multiusers

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

Default	enabled
Format	`snmp-server enable traps multiusers`
Mode	Global Config

10.1.12.1 no snmp-server enable traps multiusers

This command disables Multiple User traps.

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

10.1.13 snmp-server enable traps stpmode

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

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

10.1.13.1 no snmp-server enable traps stpmode

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

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

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`** *`<name> <ipaddr> [snmpversion <snmpversion>]`*
Mode	Global Config

10.1.14.1 no snmptrap

This command deletes trap receivers for a community.

Format	**`no snmptrap`** *`<name> <ipaddr>`*
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 enable 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 enable 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 `show snmptrap`

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 `show trapflags`

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 7300 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 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 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 7300 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 `clear dot1x statistics {<slot/port> | all}`

Mode Privileged EXEC

11.1.3 clear radius statistics

This command is used to clear all RADIUS statistics.

Format `clear radius statistics`

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 `dot1x defaultlogin <listname>`

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 `dot1x initialize <slot/port>`

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 `dot1x login <user> <listname>`

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	**`dot1x max-req`** <*`count`*>
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	**`no dot1x max-req`**
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	**`dot1x port-control`** *`{force-unauthorized	force-authorized	auto}`*
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	**`no dot1x port-control`**
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	**`dot1x port-control all`** *`{force-unauthorized	force-authorized	auto}`*
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	**`no dot1x port-control all`**
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	**`dot1x re-authenticate`** *`<slot/port>`*
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	**`dot1x timeout`** *`{{reauth-period <seconds>}	{quiet-period <seconds>}	{tx-period <seconds>}	{supp-timeout <seconds>}	{server-timeout <seconds>}}`*
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	**`no dot1x timeout`** *`{reauth-period	quiet-period	tx-period	supp-timeout	server-timeout}`*
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	**`dot1x user`** *`<user> {<slot/port>	all}`*
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 `no dot1x user <user> {<slot/port> | all}`

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 `users defaultlogin <listname>`

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 `users login <user> <listname>`

Mode Global Config

11.1.17 show authentication

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

Format `show authentication`

Mode Privileged EXEC

Authentication Login List This displays the authentication login listname.

Method 1 This displays the first method in the specified authentication login list, if any.

Method 2 This displays the second method in the specified authentication login list, if any.

Method 3 This displays the third method in the specified authentication login list, if any.

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 7300 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	**`no radius server host`** *`{auth	acct} <ipaddress>`*
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	**`radius server key`** *`{auth	acct} <ipaddr>`*
Mode	Global Config

11.2.4 radius server msgauth

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

Format	**`radius server msgauth`** *`<ipaddr>`*
Mode	Global Config

11.2.4.1 no radius server msgauth

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

Format	**`no radius server msgauth`** *`<ipaddr>`*
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 `radius server primary <ipaddr>`

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 `radius server retransmit <retries>`

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 `no radius server retransmit`

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 `radius server timeout <seconds>`

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 *[servers]*

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 retransmissions.

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 **`show radius statistics`** *`[ipaddr]`*

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 7300 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 4.1.8 “speed” on page 4-4.

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 4.1.8 “speed” on page 4-4.

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

12.1.4.1 no port-channel

This command deletes a port-channel (LAG).

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

12.1.7 port lacpmode

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

Default	enabled
Format	`port lacpmode`
Mode	Interface Config

12.1.7.1 no port lacpmode

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

Format	`no port lacpmode`
Mode	Interface Config

12.1.8 port lacpmode all

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

Format	`port lacpmode all`
Mode	Global Config

12.1.8.1 no port lacpmode all

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

Format	`no port lacpmode all`
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	`port-channel adminmode` *`[all]`*
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	**`no port-channel adminmode`** *`[all]`*
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	**`port-channel name`** *`{<logical slot/port>	all	<name>}`*
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	**`port-channel linktrap`** *`{<logical slot/port>	all}`*
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	**`no port-channel linktrap`** *`{<logical slot/port>	all}`*
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 brief

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

Format `show port-channel brief`

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 <*slot/port*> 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 `show port-channel {<logical slot/port> | all}`

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
Quality of Service (QoS) Commands

This section describes the Quality of Service (QoS) commands available in the 7300 Series Managed Switch CLI.

This section contains the following topics:

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.

13.1 Class of Service (CoS) Commands

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.

13.1.1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The <*userpriority*> and <*trafficlass*> 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 `classofservice dot1p-mapping <userpriority> <trafficclass>`

Modes Global Config
Interface Config

13.1.1.1 no classofservice dot1p-mapping

This command maps an 802.1p priority to a default internal traffic class value.

Format `no classofservice dot1p-mapping`

Modes Global Config
Interface Config

13.1.2 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 `classofservice ip-precedence-mapping <ip-precedence> <trafficclass>`

Modes Global Config
Interface Config

13.1.2.1 no classofservice ip-precedence-mapping

This command maps an IP precedence value to a default internal traffic class value

Format `no classofservice ip-precedence-mapping`

Modes Global Config
Interface Config

13.1.3 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 `classofservice ip-dscp-mapping` *<ipdscp> <trafficclass>*

Mode Global Config

13.1.3.1 no classofservice ip-dscp-mapping

This command maps an IP DSCP value to a default internal traffic class value.

Format `no classofservice ip-dscp-mapping`

Mode Global Config

13.1.4 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 `classofservice trust` *<dot1p | ip-dscp | ip-precedence>*

Mode Global Config
Interface Config

13.1.4.1 no classofservice trust

This command sets the interface mode to untrusted.

Format `no classofservice trust`

Modes Global Config
Interface Config

13.1.5 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

13.1.5.1 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

13.1.6 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

13.1.6.1 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

13.1.7 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

13.1.7.1 no traffic-shape

This command restores the interface shaping rate to the default value.

Format `no traffic-shape`

Modes Global Config
Interface Config

13.1.8 show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The 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` *[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.

13.1.9 show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The 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.

➡ **Note:** The IP DSCP command mapping is only supported on the Broadcom 5695 platform.

Format	**`show classofservice ip-precedence-mapping`** *`[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.

13.1.10 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.

13.1.11 show classofservice trust

This command displays the current trust mode setting for a specific interface. The 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 [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'.

13.1.12 show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The 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 `show interfaces cos-queue [slot/port]`

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 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.

13.2 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.

13.2.1 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

13.2.1.1 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

13.3 DiffServ Class Commands

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`**.

13.3.1 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`** *`<class-map-name>`*
Mode	Global Config

13.3.1.1 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** <*class-map-name*>
Mode	Global Config

13.3.2 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** <*class-map-name*> <*new-class-map-name*>
Mode	Global Config

13.3.3 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

13.3.4 match class-map

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

Format	**match class-map** <*refclassname*>
Mode	Class-Map Config

The following ruules 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.

13.3.4.1 no match class-map

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

Format	**`no match class-map`** <*refclassname*>
Mode	Class-Map Config

13.3.5 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	**`match dstip`** <*ipaddr*> <*ipmask*>
Mode	Class-Map Config

13.3.6 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	**`match dstl4port`** *`{portkey	<0-65535>}`*
Mode	Class-Map Config

13.3.7 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

13.3.8 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

13.3.9 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

13.3.10 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 is 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

13.3.11 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

13.3.12 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 {portkey	<0-65535>}`
Mode	Class-Map Config

13.4 DiffServ Policy Commands

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.

> **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.

The CLI command root is **`policy-map`**.

13.4.1 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`** `<`*`queueid`*`>`
Mode	Policy-Class-Map Config
Incompatibilities	Drop

13.4.2 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

13.4.3 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

13.4.4 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

13.4.4.1 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`** *`<classname>`*
Mode	Policy-Map Config

13.4.5 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 from 0 to 7.

Default	1
Format	`mark-cos` *`<0-7>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

13.4.6 mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

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

Format	`mark ip-dscp` *`<dscpval>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

13.4.7 mark ip-precedence

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

Format	`mark ip-precedence` *`<0-7>`*
Mode	Policy-Class-Map Config
Policy Type	In
Incompatibilities	Drop, Mark CoS, Mark IP DSCP, Police

13.4.8 police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and 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)

13.4.9 policy-map

This command establishes a new DiffServ policy. The *<policyname*> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the in parameter.

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

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

Format	**`policy-map`** *`<policyname>`* **`in`**
Mode	Global Config

13.4.9.1 no policy-map

This command eliminates an existing DiffServ policy. The *`<policyname`***`>`** 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`** *`<policyname>`*
Mode	Global Config

13.4.10 policy-map rename

This command changes the name of a DiffServ policy. The *`<policyname> i`*s the name of an existing DiffServ class. The *`<newpolicyname>`* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format	**`policy-map rename`** *`<policyname> <newpolicyname>`*
Mode	Global Config

13.5 DiffServ Service Commands

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`**.

13.5.1 service-policy

This command attaches a policy to an interface in the inbound direction. The `<policyname>` parameter is the name of an existing DiffServ policy. 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`** *`<policymapname>`*
Modes	Global Config Interface Config

Note: You can only attach a single policy to a particular interface at any time.

13.5.1.1 no service-policy

This command detaches a policy from an interface in the inbound direction. The `<policyname>` parameter is the name of an existing DiffServ policy.

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`** *`<policymapname>`*
Modes	Global Config Interface Config

13.6 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.

13.6.1 show class-map

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 <class-name>`

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.

13.6.2 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.

13.6.3 show policy-map

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

Format `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 This field denotes the style of policing, if any, used (simple).

Redirect 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.

13.6.4 show diffserv service

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

Format **`show diffserv service`** *`<slot/port>`* **`in`**

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 show policy-map `<policymapname>` command (content not repeated here for brevity).

13.6.5 show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format **`show diffserv service brief`** *`[in]`*

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.

13.6.6 show policy-map interface

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

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

Format `show policy-map interface <slot/port> [in]`

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.

13.6.7 show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format `show service-policy in`

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.

13.7 MAC Access Control List (ACL) Commands

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.

13.7.1 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

13.7.1.1 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

13.7.2 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

13.7.3 {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 13-1.

Table 13-1. 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 *{deny|permit} {<srcmac> | any} {<dstmac> | any} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [assign-queue <queue-id>]*

Mode Mac-Access-List Config

13.7.4 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	**mac access-group** *<name>* **in** *[sequence <1-4294967295>]*
Modes	Global Config Interface Config

13.7.4.1 no mac access-group

This command removes a MAC ACL identified by *<name>* from the interface in a given direction.

Format	**no mac access-list** *<name>* **in**
Modes	Global Config Interface Config

13.7.5 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	**show mac access-lists** *[name]*
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 slot/port to which packets matching this rule are forwarded.

13.8 IP Access Control List (ACL) Commands

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 7300 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.

13.8.1 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 i*cmp,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

13.8.1.1 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

13.8.2 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

13.8.2.1 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

13.8.3 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`** *<accesslistnumber>*

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).

13.8.4 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 <slot/port> 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 14
Routing Commands

This section describes the routing commands available in the 7300 Series Managed Switch CLI.

This section contains the following topics:

The commands in this section are in one of two functional 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.

14.1 Address Resolution Protocol (ARP) Commands

This section describes the commands you use to configure ARP and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

14.1.1 arp

This command creates an ARP entry. The value for <*ipaddress*> is the IP address of a device on a subnet attached to an existing routing interface. <*macaddr*> is a unicast MAC address for that device.

The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format	**`arp`** <*ipaddress*> <*macaddr*>
Mode	Global Config

14.1.1.1 no arp

This command deletes an ARP entry. The value for <*arpentry*> is the IP address of the interface. The value for <*ipaddress*> is the IP address of a device on a subnet attached to an existing routing interface. <*macaddr*> is a unicast MAC address for that device.

Format	**`no arp`** <*ipaddress*> <*macaddr*>
Mode	Global Config

14.1.2 ip proxy-arp

This command enables proxy ARP on a router interface. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default	enabled
Format	**`ip proxy-arp`**
Mode	Interface Config

14.1.2.1 no ip proxy-arp

This command disables proxy ARP on a router interface.

Format	**`no ip proxy-arp`**
Mode	Interface Config

14.1.3 arp cachesize

This command configures the ARP cache size. The value for <*cachesize*> is a platform specific integer value.

Format **arp cachesize** <*Platform specific integer value*>

Mode Global Config

14.1.3.1 no arp cachesize

This command configures the default ARP cache size.

Format **no arp cachesize**

Mode Global Config

14.1.4 arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out.

Format **arp dynamicrenew**

Mode Privileged EXEC

14.1.4.1 no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format **no arp dynamicrenew**

Mode Privileged EXEC

14.1.5 arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format **arp purge** <*ipaddr*>

Mode Privileged EXEC

14.1.6 arp resptime

This command configures the ARP request response timeout. The value for <*seconds*> is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for <*seconds*> is between 1-10 seconds.

Default	l
Format	**`arp resptime`** *`<1-10>`*
Mode	Global Config

14.1.6.1 no arp resptime

This command configures the default ARP request response timeout.

Format	**`no arp resptime`**
Mode	Global Config

14.1.7 arp retries

This command configures the ARP count of maximum request for retries. The value for <*`retries`*> is an integer, which represents the maximum number of request for retries. The range for <*`retries`*> is an integer between 0-10 retries.

Default	4
Format	**`arp retries`** <*`0-10`*>
Mode	Global Config

14.1.7.1 no arp retries

This command configures the default ARP count of maximum request for retries.

Format	**`no arp retries`**
Mode	Global Config

14.1.8 arp timeout

This command configures the ARP entry ageout time. The value for <*`seconds`*> is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for <*`seconds`*> is between 15-21600 seconds.

Default	1200
Format	**`arp timeout`** <*`15-21600`*>
Mode	Global Config

14.1.8.1 no arp timeout

This command configures the default ARP entry ageout time.

Format	**`no arp timeout`**
Mode	Global Config

14.1.9 clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the *gateway* parameter is specified, the dynamic entries of type gateway are purged as well.

Format `clear arp-cache [gateway]`

Mode Privileged EXEC

14.1.10 show arp

This command displays the ARP cache. The displayed results are not the total ARP entries. To view the total ARP entries, combine the **`show arp`** results and the **`show arp switch`** results.

Format `show arp`

Mode Privileged EXEC

Age Time (seconds) Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.

Response Time (seconds) Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.

Retries Is the maximum number of times an ARP request is retried. This value was configured into the unit.

Cache Size Is the maximum number of entries in the ARP table. This value was configured into the unit.

Dynamic Renew Mode Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.

Total Entry Count Current / Peak Field listing the total entries in the ARP table and the peak entry count in the ARP table.

Static Entry Count Current / Max Field listing the static entry count in the ARP table and maximum static entry count in the ARP table.

The following fields are displayed for each ARP entry.

IP Address Is the IP address of a device on a subnet attached to an existing routing interface.

MAC Address Is the hardware MAC address of that device.

Interface Is the routing slot/port associated with the device ARP entry.

Type Is the type that was configured into the unit. The possible values are Local, Gateway, Dynamic and Static.

Age This field displays the current age of the ARP entry since last refresh (in hh:mm:ss format

14.1.11 show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format `show arp brief`

Mode Privileged EXEC

Age Time (seconds) Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.

Response Time (seconds) Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.

Retries Is the maximum number of times an ARP request is retried. This value was configured into the unit.

Cache Size Is the maximum number of entries in the ARP table. This value was configured into the unit.

Dynamic Renew Mode Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.

Total Entry Count Current / Peak Field listing the total entries in the ARP table and the peak entry count in the ARP table.

Static Entry Count Current / Max Field listing the static entry count in the ARP table and maximum static entry count in the ARP table.

14.2 IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

14.2.1 routing

This command enables routing for an interface.

You can view the current value for this function with the **`show ip brief`** command. The value is labeled as “Routing Mode.”

Default	disabled
Format	**`routing`**
Mode	Interface Config

14.2.1.1 no routing

This command disables routing for an interface.

You can view the current value for this function with the **`show ip brief`** command. The value is labeled as “Routing Mode.”

Format	**`no routing`**
Mode	Interface Config

14.2.2 ip routing

This command enables the IP Router Admin Mode for the master switch.

Format	**`ip routing`**
Mode	Global Config

14.2.2.1 no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format	**`no ip routing`**
Mode	Global Config

14.2.3 ip address

This command configures an IP address on an interface. You can also use this command to configure one or more secondary IP addresses on the interface.

The value for <*ipaddr*> is the IP Address of the interface.

The value for <*subnetmask*> is a 4-digit dotted-decimal number which represents the subnet mask of the interface. This changes the label IP address in **show ip interface**.

Format	**ip address** <*ipaddr*> <*subnetmask*> *[secondary]*
Mode	Interface Config

14.2.3.1 no ip address

This command deletes an IP address from an interface. The value for <*ipaddr*> is the IP Address of the interface. The value for <*subnetmask*> is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface.

Format	**no ip address** <*ipaddr*> <*subnetmask*> *[secondary]*
Mode	Interface Config

14.2.4 ip route

This command configures a static route. The <*ipaddr*> is a valid ip address. The <*subnetmask*> is a valid subnet mask. The <*nextHopRtr*> is a valid IP address of the next hop router.

The <*preference*> is an integer value from 1 to 255. The user can specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, the user controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

The following must be present before the static routes are visible:

- Enable ip routing globally.
- Enable ip routing for the interface.
- The associated link must also be up.

Default	preference - 1
Format	**`ip route`** *`<ipaddr> <subnetmask> <nextHopRtr> [<preference>]`*
Mode	Global Config

14.2.4.1 no ip route

This command deletes all next hops to a destination static route. If you use the *`<nextHopRtr>`* parameter, the next hop is deleted. If you use the *`<preference>`* value, the preference value of the static route is reset to its default.

Format	**`no ip route`** *`<ipaddr> <subnetmask> [{<nextHopRtr> | <preference>}]`*
Mode	Global Config

14.2.5 ip route default

This command configures the default route. The value for *`<nextHopRtr>`* is a valid IP address of the next hop router. The *`<preference>`* is an integer value from 1 to 255

Default	preference - 1
Format	**`ip route default`** *`<nextHopRtr> [<preference>]`*
Mode	Global Config

14.2.5.1 no ip route default

This command deletes all configured default routes. If the optional *`<nextHopRtr>`* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Format	**`no ip route default`** *`[{<nextHopRtr> | <preference>}]`*
Mode	Global Config

14.2.6 ip route distance

This command sets the default distance for static routes. Lower route preference values are preferred when determining the best route. The **`ip route`** and **`ip route default`** commands allow you to optionally set the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **`ip route distance`** command.

Default	1
Format	**`ip route distance`** *<1-255>*
Mode	Global Config

14.2.6.1 no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format	**`no ip route distance`**
Mode	Global Config

14.2.7 ip forwarding

This command enables forwarding of IP frames.

Default	enabled
Format	**`ip forwarding`**
Mode	Global Config

14.2.7.1 no ip forwarding

This command disables forwarding of IP frames.

Format	**`no ip forwarding`**
Mode	Global Config

14.2.8 ip netdirbcast

This command enables the forwarding of network-directed broadcasts. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default	disabled
Format	`ip netdirbcast`
Mode	Interface Config

14.2.8.1 no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Format	`no ip netdirbcast`
Mode	Interface Config

14.2.9 ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. The 7300 Series Managed Switch software currently does not fragment IP packets.

- Packets forwarded in hardware ignore the IP MTU.
- Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the ip mtu command.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency (unless OSPF has been instructed to ignore differences in IP MTU with the ip ospf mtu-ignore command.)

Note: The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (See Section 4.1.5 “mtu” on page 4-3) must take into account the size of the Ethernet header.

The minimum IP MTU is 68 bytes.The maximum IP MTU is 1500 bytes.

Default 1500 bytes

Format `ip mtu <mtu>`

Mode Interface Config

14.2.9.1 no ip mtu

This command resets the ip mtu to the default value.

Format `no ip mtu <mtu>`

Mode Interface Config

14.2.10 encapsulation

This command configures the link layer encapsulation type for the packet. Acceptable values for `<encapstype>` are ethernet and SNAP. The default is ethernet.

Format `encapsulation {ethernet | snap}`

Mode Interface Config

Note: Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

14.2.11 show ip brief

This command displays all the summary information of the IP. This command takes no options.

Format `show ip brief`

Modes Privileged EXEC
User EXEC

Default Time to Live The computed TTL (Time to Live) of forwarding a packet from

the local router to the final destination.

Routing Mode Shows whether the routing mode is enabled or disabled.

IP Forwarding Mode Shows whether forwarding of IP frames is enabled or disabled. This is a configured value.

Maximum Next Hops Shows the maximum number of next hops the packet can travel.

14.2.12 show ip interface

This command displays all pertinent information about the IP interface.

Format `show ip interface <slot/port>`

Modes Privileged EXEC
User EXEC

Primary IP Address Displays the primary IP address and subnet masks for the interface. This value appears only if you configure it.

Secondary IP Address Displays one or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.

Routing Mode Is the administrative mode of router interface participation. The possible values are enable or disable. This value was configured into the unit.

Administrative Mode Is the administrative mode of the specified interface. The possible values of this field are enable or disable. This value was configured into the unit.

Forward Net Directed Broadcasts Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value was configured into the unit.

Proxy ARP Displays whether Proxy ARP is enabled or disabled on the system.

Active State Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.

Link Speed Data Rate Is an integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).

MAC Address Is the burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.

Encapsulation Type Is the encapsulation type for the specified interface. The types are: Ethernet or SNAP.

IP MTU Displays the maximum transmission unit (MTU) size of a frame, in bytes.

14.2.13 show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

Format `show ip interface brief`

Modes Privileged EXEC

User EXEC

Interface Valid slot and port number separated by forward slashes.

IP Address The IP address of the routing interface in 32-bit dotted decimal format.

IP Mask The IP mask of the routing interface in 32-bit dotted decimal format.

Netdir Bcast Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.

MultiCast Fwd Indicates the multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

14.2.14 show ip route

This command displays the entire route table. This commands takes no options.

Format `show ip route`

Mode Privileged EXEC

Network Address Is an IP address identifying the network on the specified interface.

Subnet Mask Is a mask of the network and host portion of the IP address for the router interface.

Protocol Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

Total Number of Routes The total number of routes.

For each Next Hop

Next Hop Intf The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

14.2.15 show ip route bestroutes

This command causes the entire route table to be displayed. This commands takes no options.

Format `show ip route bestroutes`

Mode Privileged EXEC

Network Address Is an IP route prefix for the destination.

Subnet Mask Is a mask of the network and host portion of the IP address for the specified interface.

Protocol Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

Total Number of Routes The total number of routes in the route table.

The following information displays for each Next Hop.

Next Hop Intf The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

14.2.16 show ip route entry

This command displays the entire route table.

Format `show ip route entry`

Mode Privileged EXEC

Network Address Is a valid network address identifying the network on the specified interface.

Subnet Mask Is a mask of the network and host portion of the IP address for the attached network.

Protocol Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

The following information displays for each Next Hop.

Next Hop Interface The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Metric The cost associated with this route.

Preference The administrative distance associated with this route.

14.2.17 show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

Format	`show ip route preferences`
Modes	Privileged EXEC User EXEC
Local	This field displays the local route preference value.
Static	This field displays the static route preference value.
OSPF Intra	This field displays the OSPF Intra route preference value.
OSPF Inter	This field displays the OSPF Inter route preference value.
OSPF Type-1	This field displays the OSPF Type-1 route preference value.
OSPF Type-2	This field displays the OSPF Type-2 route preference value.
RIP	This field displays the RIP route preference value.
BGP4	This field displays the BGP-4 route preference value.

14.2.18 show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format	`show ip stats`
Modes	Privileged EXEC User EXEC

14.3 Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

14.3.1 ip irdp

This command enables Router Discovery on an interface.

Default	disabled
Format	`ip irdp`
Mode	Interface Config

14.3.1.1 no ip irdp

This command disables Router Discovery on an interface.

Format	`no ip irdp`
Mode	Interface Config

14.3.2 ip irdp address

This command configures the address that the interface uses to send the router discovery advertisements. The valid values for <*ipaddr*> are 224.0.0.1, which is the all-hosts IP multicast address, and 255.255.255.255, which is the limited broadcast address.

Default	224.0.0.1
Format	**ip irdp address** <*ipaddr*>
Mode	Interface Config

14.3.2.1 no ip irdp address

This command configures the default address to be used to advertise the router for the interface.

Format	`no ip irdp address`
Mode	Interface Config

14.3.3 ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of <*maxadvertinterval*> to 9000 seconds.

Default	3 * maxinterval
Format	**`ip irdp holdtime`** <*maxadvertinterval-9000*>
Mode	Interface Config

14.3.3.1 no ip irdp holdtime

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Format	**`no ip irdp holdtime`**
Mode	Interface Config

14.3.4 ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for maxadvertinterval is 4 to 1800 seconds.

Default	600
Format	**`ip irdp maxadvertinterval <`***4-1800*>
Mode	Interface Config

14.3.4.1 no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format	**`no ip irdp maxadvertinterval`**
Mode	Interface Config

14.3.5 ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is three to the value of maxadvertinterval.

Default	0.75 * maxadvertinterval
Format	**`ip irdp minadvertinterval`** <*3-maxadvertinterval*>
Mode	Interface Config

14.3.5.1 no ip irdp minadvertinterval

This command sets the default minimum time to the default.

Format	**`no ip irdp minadvertinterval`**
Mode	Interface Config

14.3.6 ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet. The range is -2147483648 to -1 to 0 to 1 to 2147483647.

Default	0
Format	**`ip irdp preference`** *`<-2147483648-2147483647>`*
Mode	Interface Config

14.3.6.1 no ip irdp preference

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Format	**`no ip irdp preference`**
Mode	Interface Config

14.3.7 show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

Format	**`show ip irdp`** *`{<slot/port>	all}`*
Modes	Privileged EXEC User EXEC
Interface	Shows the *`<slot/port>`*.
Ad Mode	Displays the advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Advertise Address	Displays the IP address to which the interface sends the advertisement.

Max Int Displays the maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.

Min Int Displays the minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.

Hold Time Displays the amount of time, in seconds, that a system should keep the router advertisement before discarding it.

Preference Displays the preference of the address as a default router address, relative to other router addresses on the same subnet.

14.4 Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

14.4.1 vlan routing

This command creates routing on a VLAN. The <*vlanid*> value has a range from 1 to 4094.

Format `vlan routing <vlanid>`

Mode VLAN Config

14.4.1.1 no vlan routing

This command deletes routing on a VLAN. The <*vlanid*> value has a range from 1 to 4094.

Format `no vlan routing <vlanid>`

Mode VLAN Config

14.4.2 show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format `show ip vlan`

Modes Privileged EXEC
User EXEC

MAC Address used by Routing VLANs Is the MAC Address associated with the internalbridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.

VLAN ID Is the identifier of the VLAN.

Logical Interface Shows the logical slot/port associated with the VLAN routing interface.

IP Address Displays the IP Address associated with this VLAN.

Subnet Mask Indicates the subnet mask that is associated with this VLAN.

14.5 Virtual Router Redundancy Protocol (VRRP) Commands

This section describes the commands you use to view and configure VRRP and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

14.5.1 ip vrrp

This command enables the VRRP protocol on an interface and designates the configured virtual router IP address as a secondary IP address on an interface. The parameter *<vrID>* is the virtual router ID which has an integer value range from 1 to 255.

Default none

Format **ip vrrp** *<vrID> <ipaddress> [secondary]*

Mode Interface Config

14.5.1.1 no ip vrrp

This command disables the VRRP protocol on an interface. This command also removes a virtual router IP address as a secondary IP address on an interface. The parameter *<vrID>* is the virtual router ID which has an integer value ranges from 1 to 255.

Format **no ip vrrp** *<vrID> <ipaddress> [secondary]*

Mode Interface Config

14.5.2 ip vrrp

This command enables the administrative mode of VRRP in the router. This command also designates the configured virtual router IP address as a secondary IP address on an interface.

Default	enabled
Format	**`ip vrrp`** *`<vrid> <ipaddress> [secondary]`*
Mode	Global Config

14.5.2.1 no ip vrrp

This command disables the default administrative mode of VRRP in the router.

Format	**`no ip vrrp`**
Mode	Global Config

14.5.3 ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter *`<vrID>`* is the virtual router ID which has an integer value ranging from 1 to 255.

Default	disabled
Format	**`ip vrrp`** *`<vrID>`* **`mode`**
Mode	Interface Config

14.5.3.1 no ip vrrp mode

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Format	**`no ip vrrp`** *`<vrID>`* **`mode`**
Mode	Interface Config

14.5.4 ip vrrp ip

This command sets the virtual router ipaddress value for an interface. The value for *`<ipaddr>`* is the IP Address which is to be configured on that interface for VRRP. The parameter *`<vrID>`* is the virtual router ID which has an integer value range from 1 to 255.

Default	none
Format	**`ip vrrp`** *`<vrID>`* **`ip`** *`<ipaddr>`*

Mode Interface Config

14.5.5 ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface. The parameter *{none | simple}* specifies the authorization type for virtual router configured on the specified interface. The parameter *[key]* is optional, it is only required when authorization type is simple text password. The parameter *<vrID>* is the virtual router ID which has an integer value ranges from 1 to 255.

Default no authorization

Format **ip vrrp** *<vrID>* **authentication** *{none | simple <key>}*

Mode Interface Config

14.5.5.1 no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface.

Format **no ip vrrp** *<vrID>* **authentication**

Mode Interface Config

14.5.6 ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface. The parameter *<vrID>* is the virtual router ID, which is an integer from 1 to 255

Default enabled

Format **ip vrrp** *<vrID>* **preempt**

Mode Interface Config

14.5.6.1 no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface.

Format **no ip vrrp** *<vrID>* **preempt**

Mode Interface Config

14.5.7 ip vrrp priority

This command sets the priority value for the virtual router configured on a specified interface. The priority of the interface is a priority integer from 1 to 254. The parameter *<vrID>* is the virtual router ID which has an integer value ranges from 1 to 255.

Default	100
Format	**ip vrrp** *<vrID>* **priority** *<1-254>*
Mode	Interface Config

14.5.7.1 no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface.

Format	**no ip vrrp** *<vrID>* **priority**
Mode	Interface Config

14.5.8 ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.

Default	1
Format	**ip vrrp** *<vrID>* **timers advertise** *<1-255>*
Mode	Interface Config

14.5.8.1 no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface.

Format	**no ip vrrp** *<vrID>* **timers advertise**
Mode	Interface Config

14.5.9 show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the 7300 Series Managed Switch switch.

Format	**show ip vrrp interface stats** *<slot/port>* *<vrID>*
Modes	Privileged EXEC User EXEC

Uptime The time that the virtual router has been up, in days, hours, minutes and seconds.

Protocol Represents the protocol configured on the interface.

State Transitioned to Master Represents the total number of times virtual router state has changed to MASTER.

Advertisement Received Represents the total number of VRRP advertisements received by this virtual router.

Advertisement Interval Errors Represents the total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.

Authentication Failure Represents the total number of VRRP packets received that don't pass the authentication check.

IP TTL errors Represents the total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.

Zero Priority Packets Received Represents the total number of VRRP packets received by virtual router with a priority of '0'.

Zero Priority Packets Sent Represents the total number of VRRP packets sent by the virtual router with a priority of '0'.

Invalid Type Packets Received Represents the total number of VRRP packets received by the virtual router with invalid 'type' field.

Address List Errors Represents the total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.

Invalid Authentication Type Represents the total number of VRRP packets received with unknown authentication type.

Authentication Type Mismatch Represents the total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.

Packet Length Errors Represents the total number of VRRP packets received with packet length less than length of VRRP header.

14.5.10 show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the 7300 Series Managed Switch. It also displays some global parameters which are required for monitoring This command takes no options.

Format `show ip vrrp`

Modes Privileged EXEC
User EXEC

VRRP Admin Mode Displays the administrative mode for VRRP functionality on the switch.

Router Checksum Errors Represents the total number of VRRP packets received with an invalid VRRP checksum value.

Router Version Errors Represents the total number of VRRP packets received with Unknown or unsupported version number.

Router VRID Errors Represents the total number of VRRP packets received with invalid VRID for this virtual router.

14.5.11 show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

Format `show ip vrrp interface <slot/port> <vrID>`

Modes Privileged EXEC
User EXEC

IP Address This field represents the configured IP Address for the Virtual router.

VMAC address Represents the VMAC address of the specified router.

Authentication type Represents the authentication type for the specific virtual router.

Priority Represents the priority value for the specific virtual router.

Advertisement interval Represents the advertisement interval for the specific virtual router.

Pre-Empt Mode Is the preemption mode configured on the specified virtual router.

Administrative Mode Represents the status (Enable or Disable) of the specific router.

State Represents the state (Master/backup) of the virtual router.

14.5.12 show ip vrrp interface brief

This command displays information about each virtual router configured on the 7300 Series Managed Switch. This command takes no options. It displays information about each virtual router.

Format `show ip vrrp interface brief`

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

VRID Represents the router ID of the virtual router.

IP Address The virtual router IP address.

Mode	Represents whether the virtual router is enabled or disabled.
State	Represents the state (Master/backup) of the virtual router.

14.6 Open Shortest Path First (OSPF) Commands

This section describes the commands you use to view and configure OSPF, which is a link-state routing protocol that you use to route traffic within a network.

14.6.1 router ospf

Use this command to enter Router OSPF mode.

Format	`router ospf`
Mode	Global Config

14.6.2 enable (OSPF)

This command resets the default administrative mode of OSPF in the router (active).

Default	enabled
Format	`enable`
Mode	Router OSPF Config

14.6.2.1 no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

Format	`no enable`
Mode	Router OSPF Config

14.6.3 ip ospf

This command enables OSPF on a router interface.

Default	disabled
Format	`ip ospf`
Mode	Interface Config

14.6.3.1 no ip ospf

This command disables OSPF on a router interface.

Format	`no ip ospf`
Mode	Interface Config

14.6.4 1583compatibility

This command enables OSPF 1583 compatibility.

> **Note:** 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Default	enabled
Format	`1583compatibility`
Mode	Router OSPF Config

14.6.4.1 no 1583compatibility

This command disables OSPF 1583 compatibility.

Format	`no 1583compatibility`
Mode	Router OSPF Config

14.6.5 area default-cost

This command configures the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1-16777215.

Format	**area** *<areaid>* **default-cost** *<1-16777215>*
Mode	Router OSPF Config

14.6.6 area nssa

This command configures the specified areaid to function as an NSSA.

Format	**area** *<areaid>* **nssa**
Mode	Router OSPF Config

14.6.6.1 no area nssa

This command disables nssa from the specified area id.

Format	**`no area`** *`<areaid>`* **`nssa`**
Mode	Router OSPF Config

14.6.7 area nssa default-info-originate

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777215. If no metric is specified, the default value is ****. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Format	**`area`** *`<areaid>`* **`nssa default-info-originate`** *`[<metric>] [{comparable | non-comparable}]`*
Mode	Router OSPF Config

14.6.8 area nssa no-redistribute (OSPF)

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

Format	**`area`** *`<areaid>`* **`nssa no-redistribute`**
Mode	Router OSPF Config

14.6.9 area nssa no-summary (OSPF)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format	**`area`** *`<areaid>`* **`nssa no-summary`**
Mode	Router OSPF Config

14.6.10 area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. A value of **always** causes the router to assume the role of the translator the instant it becomes a border router and a value of **candidate** causes the router to participate in the translator election process when it attains border router status.

Format	**`area`** *`<areaid>`* **`nssa translator-role`** *`{always | candidate}`*

Mode Router OSPF Config

14.6.11 area nssa translator-stab-intv

This command configures the translator *<stabilityinterval>* of the NSSA. The *<stabilityinterval>* is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format `area <areaid> nssa translator-stab-intv <stabilityinterval>`

Mode Router OSPF Config

14.6.12 area range

This command creates a specified area range for a specified NSSA. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask. The LSDB type must be specified by either *summarylink* or *nssaexternallink*, and the advertising of the area range can be allowed or suppressed.

Format `area <areaid> range <ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise | not-advertise]`

Mode Router OSPF Config

14.6.12.1 no area range

This command deletes a specified area range.

Format `no area <areaid> range <ipaddr> <subnetmask>`

Mode Router OSPF Config

14.6.13 area stub

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format `area <areaid> stub`

Mode Router OSPF Config

14.6.13.1 no area stub

This command deletes a stub area for the specified area ID.

Format	**`no area`** *`<areaid>`* **`stub`**
Mode	Router OSPF Config

14.6.14 area stub summarylsa

This command configures the Summary LSA mode for the stub area identified by **<***`areaid`***>**. The Summary LSA mode is configured as enabled.

Default	disabled
Format	**`area`** *`<areaid>`* **`stub summarylsa`**
Mode	Router OSPF Config

14.6.14.1 no area stub summarylsa

This command configures the default Summary LSA mode for the stub area identified by **<***`areaid`***>**.

Format	**`no area`** *`<areaid>`* **`stub summarylsa`**
Mode	Router OSPF Config

14.6.15 area virtual-link

This command creates the OSPF virtual interface for the specified **<***`areaid`***>** and **<***`neighbor`***>**. The **<***`neighbor`***>** parameter is the Router ID of the neighbor.

Format	**`area`** *`<areaid>`* **`virtual-link`** *`<neighbor>`*
Mode	Router OSPF Config

14.6.15.1 no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by **<***`areaid`***>** and **<***`neighbor`***>**. The **<***`neighbor`***>** parameter is the Router ID of the neighbor.

Format	**`no area`** *`<areaid>`* **`virtual-link`** *`<neighbor>`*
Mode	Router OSPF Config

14.6.16 area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The value for *<type>* is either none, simple, or encrypt. The *[key]* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple.

If the type is encrypt, the key may be up to 256 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id in the range of 0 and 255 must be specified.The default value for authentication type is none. Neither the default password key nor the default key id are configured.

Default	none
Format	**area** *<areaid>* **virtual-link** *<neighbor>* **authentication** *{none | {simple <key>} | {encrypt <key> <keyid>}}*
Mode	Router OSPF Config

14.6.16.1 no area virtual-link authentication

This command configures the default authentication type for the OSPF virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

Format	**no area** *<areaid>* **virtual-link** *<neighbor>* **authentication**
Mode	Router OSPF Config

14.6.17 area virtual-link dead-interval

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The range for *<seconds>* is 1 to 65535.

Default	40
Format	**area** *<areaid>* **virtual-link** *<neighbor>* **dead-interval** *<1-65535>*
Mode	Router OSPF Config

14.6.17.1 no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by **<*areaid*>** and **<*neighbor*>**. The **<*neighbor*>** parameter is the Router ID of the neighbor.

Format	**no area** <*areaid*> **virtual-link** <*neighbor*> **dead-interval**
Mode	Router OSPF Config

14.6.18 area virtual-link hello-interval

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by **<*areaid*>** and **<*neighbor*>**. The **<*neighbor*>** parameter is the Router ID of the neighbor. The range for **<*seconds*>** is 1 to 65535.

Default	10
Format	**area** <*areaid*> **virtual-link <*neighbor*> hello-interval <*1-65535*>**
Mode	Router OSPF Config

14.6.18.1 no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by **<*areaid*>** and **<*neighbor*>**. The **<*neighbor*>** parameter is the Router ID of the neighbor.

Format	**no area <*areaid*> virtual-link <*neighbor*> hello-interval**
Mode	Router OSPF Config

14.6.19 area virtual-link retransmit-interval

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor. The range for <*seconds*> is 0 to 3600.

Default	5
Format	**area <*areaid*> virtual-link <*neighbor*> retransmit-interval <*0-3600*>**
Mode	Router OSPF Config

14.6.19.1 no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by **<*areaid*>** and **<*neighbor*>**. The **<*neighbor*>** parameter is the Router ID of the neighbor.

Format	**no area <*areaid*> virtual-link <*neighbor*> retransmit-interval**
Mode	Router OSPF Config

14.6.20 area virtual-link transmit-delay

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by **<*areaid*>** and **<*neighbor*>**. The **<*neighbor*>** parameter is the Router ID of the neighbor. The range for **<*seconds*>** is 0 to 3600 (1 hour).

Default	1
Format	**area <*areaid*> virtual-link <*neighbor*> transmit-delay <*0-3600*>**
Mode	Router OSPF Config

14.6.20.1 no area virtual-link transmit-delay

This command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by **<*areaid*>** and **<*neighbor*>**. The **<*neighbor*>** parameter is the Router ID of the neighbor.

Format	**no area <*areaid*> virtual-link <*neighbor*> transmit-delay**
Mode	Router OSPF Config

14.6.21 default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Default	metric - unspecified; type - 2
Format	**default-information originate** *[always] [metric <0-16777215>] [metric-type {1 | 2}]*
Mode	Router OSPF Config

14.6.21.1 no default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Format **`no default-information originate`** *`[metric] [metric-type]`*

Mode Router OSPF Config

14.6.22 default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format **`default-metric`** *`<1-16777215>`*

Mode Router OSPF Config

14.6.22.1 no default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format **`no default-metric`**

Mode Router OSPF Config

14.6.23 distance ospf

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF can be intra, inter, type-1, or type-2. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2. The <*`preference`*> range is 1 to 255.

Default intra - 8; inter - 10; type-1, 13; type-2, 50.

Format **`distance ospf`** *`{intra | inter | type1 | type2} <preference>`*

Mode Router OSPF Config

14.6.23.1 no distance ospf

This command sets the default route preference value of OSPF in the router.

Format **`no distance ospf`** *`{intra | inter | type1 | type2}`*

Mode Router OSPF Config

14.6.24 distribute-list out

Use this command to specify the access list to filter routes received from the source protocol.

Format `distribute-list <1-199> out {rip | bgp | static | connected}`

Mode Router OSPF Config

14.6.24.1 no distribute-list out

Use this command to specify the access list to filter routes received from the source protocol.

Format `no distribute-list <1-199> out {rip | bgp | static | connected}`

Mode Router OSPF Config

14.6.25 exit-overflow-interval

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted. The range for *<seconds>* is 0 to 2147483647 seconds.

Default 0

Format `exit-overflow-interval <0-2147483647>`

Mode Router OSPF Config

14.6.25.1 no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format `no exit-overflow-interval`

Mode Router OSPF Config

14.6.26 external-lsdb-limit

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for <*limit*> is -1 to 2147483647.

Default	-1
Format	**`external-lsdb-limit`** *<-1-2147483647>*
Mode	Router OSPF Config

14.6.26.1 no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format	**`no external-lsdb-limit`**
Mode	Router OSPF Config

14.6.27 ip ospf areaid

This command sets the OSPF area to which the specified router interface belongs. The value for <*areaid*> is an IP address, formatted as a 4-digit dotted-decimal number that uniquely identifies the area to which the interface connects. Assigning an area id, which does not exist on an interface, causes the area to be created with default values.

Format	**`ip ospf areaid <`***areaid*>
Mode	Interface Config

14.6.28 ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface. The value of <*type*> is either none, simple or encrypt. The [*key*] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 256 bytes. If the type is encrypt a <*keyid*> in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

Default	none

Format `ip ospf authentication {none | {simple <key>} | {encrypt <key> <keyid>}}`

Mode Interface Config

14.6.28.1 no ip ospf authentication

This command sets the default OSPF Authentication Type for the specified interface.

Format `no ip ospf authentication`

Mode Interface Config

14.6.29 ip ospf cost

This command configures the cost on an OSPF interface. The <*cost*> parameter has a range of 1 to 65535.

Default 10

Format `ip ospf cost <1-65535>`

Mode Interface Config

14.6.29.1 no ip ospf cost

This command configures the default cost on an OSPF interface.

Format `no ip ospf cost`

Mode Interface Config

14.6.30 ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface. The interval is the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The interval must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4).

Default 40

Format `ip ospf dead-interval <1-2147483647>`

Mode Interface Config

14.6.30.1 no ip ospf dead-interval

This command sets the default OSPF dead interval for the specified interface.

Format	**`no ip ospf dead-interval`**
Mode	Interface Config

14.6.31 ip ospf hello-interval

This command sets the OSPF hello interval for the specified interface. The interval is the length of time in seconds. The value for the length of time must be the same for all routers attached to a network. Valid values range from 1 to 65535.

Default	10
Format	**`ip ospf hello-interval`** *<1-65535>*
Mode	Interface Config

14.6.31.1 no ip ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format	**`no ip ospf hello-interval`**
Mode	Interface Config

14.6.32 ip ospf priority

This command sets the OSPF priority for the specified router interface. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default	1, which is the highest router priority.
Format	**`ip ospf priority`** *<0-255>*
Mode	Interface Config

14.6.32.1 no ip ospf priority

This command sets the default OSPF priority for the specified router interface.

Format	**`no ip ospf priority`**
Mode	Interface Config

14.6.33 ip ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface. The retransmit interval is specified in seconds. The value for <*seconds*> is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

Default	5
Format	**`ip ospf retransmit-interval`** *<0-3600>*
Mode	Interface Config

14.6.33.1 no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format	**`no ip ospf retransmit-interval`**
Mode	Interface Config

14.6.34 ip ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for <*seconds*> range from 1 to 3600 (1 hour).

Default	1
Format	**`ip ospf transmit-delay`** *<1-3600>*
Mode	Interface Config

14.6.34.1 no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format	**`no ip ospf transmit-delay`**
Mode	Interface Config

14.6.35 ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default	enabled
Format	**`ip ospf mtu-ignore`**
Mode	Interface Config

14.6.35.1 no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format	**`no ip ospf mtu-ignore`**
Mode	Interface Config

14.6.36 router-id

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The <*ipaddress*> is a configured value.

Format	**`router-id`** <*ipaddress*>
Mode	Router OSPF Config

14.6.37 redistribute

This command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

Default	metric - unspecified; type - 2; tag - 0
Format	**`redistribute`** *{rip | bgp | static | connected} [metric <0-16777215>] [metric-type {1 | 2}] [tag <0-4294967295>] [subnets]*
Mode	Router OSPF Config

14.6.37.1 no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format	**`no redistribute`** *`{rip	bgp	static	connected} [metric] [metric-type] [tag] [subnets]`*
Mode	Router OSPF Config

14.6.38 maximum-paths

This command sets the number of paths that OSPF can report for a given destination where *`maxpaths`* is platform dependent.

Default	4
Format	**`maximum-paths`** *`<maxpaths>`*
Mode	Router OSPF Config

14.6.38.1 no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format	**`no maximum-paths`**
Mode	Router OSPF Config

14.6.39 trapflags

This command enables OSPF traps.

Default	enabled
Format	**`trapflags`**
Mode	Router OSPF Config

14.6.39.1 no trapflags

This command disables OSPF traps.

Format	**`no trapflags`**
Mode	Router OSPF Config

14.6.40 show ip ospf

This command displays information relevant to the OSPF router.

Format `show ip ospf`

Mode Privileged EXEC

Note: Some of the information below displays only if you enable OSPF and configure certain features.

Router ID Is a 32 bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.

OSPF Admin Mode Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.

ASBR Mode Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learnt by other protocols) or disabled (if the router is not configured for the same).

RFC 1583 Compatibility Reflects whether 1583 compatibility is enabled or disabled. This is a configured value.

ABR Status Shows whether the router is an OSPF Area Border Router.

Exit Overflow Interval Shows the number of seconds that, after entering OverflowState, a router will attempt to leave OverflowState.

External LSA Count Shows the number of external (LS type 5) link-state advertisements in the link-state database.

External LSA Checksum Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.

New LSAs Originated Shows the number of new link-state advertisements that have been originated.

LSAs Received Shows the number of link-state advertisements received determined to be new instantiations.

External LSDB Limit Shows the maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.

Default Metric Default value for redistributed routes.

Default Route Advertise Indicates whether the default routes received from other source protocols are advertised or not

Always Shows whether default routes are always advertised.

Metric Shows the metric for the advertised default routes. If the metric is not configured, this field is blank.

Metric Type Shows whether the routes are External Type 1 or External Type 2.

Maximum Paths Shows the maximum number of paths that OSPF can report for a given destination.

Redistributing This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.

Source Shows source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.

Metric Shows the metric of the routes being redistributed.

Metric Type Shows whether the routes are External Type 1 or External Type 2.

Tag Shows the decimal value attached to each external route.

Subnets For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Distribute-List Shows the access list used to filter redistributed routes.

14.6.41 show ip ospf area

This command displays information about the area. The <*areaid*> identifies the OSPF area that is being displayed.

Format `show ip ospf area <areaid>`

Modes Privileged EXEC
User EXEC

AreaID Is the area id of the requested OSPF area.

Aging Interval Is a number representing the aging interval for this area.

External Routing Is a number representing the external routing capabilities for this area.

Authentication Type Is the configured authentication type to use for this area.

Spf Runs Is the number of times that the intra-area route table has been calculated using this area's link-state database.

Area Border Router Count The total number of area border routers reachable within this area.

Area LSA Count Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

Area LSA Checksum A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.

Stub Mode Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.

Import Summary LSAs Controls the import of summary LSAs into stub areas. The possible values are enabled or disabled.

Metric Value Is a number representing the Metric Value for the specified area.

Metric Type Is the Default Metric Type for the specified Area. If the area is a stub area, this field does not appear.

14.6.42 show ip ospf database

This command displays the link state database. The OSPF database information is grouped into sections by link-type and area. The groups are as follows:

- Router Link States
- Network Link States
- Network Summary States
- Summary ASBR States

The AS-Externals are not grouped by area.

Format	`show ip ospf database`
Modes	Privileged EXEC User EXEC

➡ **Note:** The information below is only displayed if OSPF is enabled.

Link Id Is a number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.

Adv Router The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.

Age Is a number representing the age of the link state advertisement in seconds.

Sequence Is a number that represents which LSA is more recent.

Checksum Is the total number LSA checksum.

Options This is an integer. It indicates that the LSA receives special handling during routing calculations.

Rtr Opt Router Options are valid for router links only.

14.6.43 show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

Format `show ip ospf interface <slot/port>`

Modes Privileged EXEC
User EXEC

IP Address Represents the IP address for the specified interface.

Subnet Mask A mask of the network and host portion of the IP address for the OSPF interface.

OSPF Admin Mode States whether OSPF is enabled or disabled on a router interface.

OSPF Area ID Represents the OSPF Area Id for the specified interface.

Router Priority A number representing the OSPF Priority for the specified interface.

Retransmit Interval A number representing the OSPF Retransmit Interval for the specified interface.

Hello Interval A number representing the OSPF Hello Interval for the specified interface.

Dead Interval A number representing the OSPF Dead Interval for the specified interface.

LSA Ack Interval A number representing the OSPF LSA Acknowledgement Interval for the specified interface.

Transit Delay Interval A number representing the OSPF Transit Delay for the specified interface.

Authentication Type The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.

The information below will only be displayed if OSPF is enabled.

OSPF Interface Type Broadcast LANs, such as Ethernet and IEEE 802.5, take the value **broadcast**. The OSPF Interface Type will be 'broadcast'.

State The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.

Designated Router The router ID representing the designated router.

Backup Designated Router The router ID representing the backup designated router.

Number of Link Events The number of link events.

Metric Cost The cost of the OSPF interface.

14.6.44 show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format `show ip ospf interface brief`

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

OSPF Admin Mode States whether OSPF is enabled or disabled on a router interface.

OSPF Area ID Represents the OSPF Area Id for the specified interface.

Router Priority A number representing the OSPF Priority for the specified interface.

Hello Interval A number representing the OSPF Hello Interval for the specified interface.

Dead Interval A number representing the OSPF Dead Interval for the specified interface.

Retransmit Interval A number representing the OSPF Retransmit Interval for the specified interface.

Transit Delay Interval A number representing the OSPF Transit Delay for the specified interface.

LSA Ack Interval A number representing the OSPF LSA Acknowledgement Interval for the specified interface.

14.6.45 show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

Format **`show ip ospf interface stats`** *`<slot/port>`*

Modes Privileged EXEC
User EXEC

OSPF Area ID The area id of this OSPF interface.

Spf Runs The number of times that the intra-area route table has been calculated using this area's link-state database.

Area Border Router Count The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.

AS Border Router Count The total number of Autonomous System border routers reachable within this area.

Area LSA Count The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

IP Address The IP address associated with this OSPF interface.

OSPF Interface Events The number of times the specified OSPF interface has changed its state, or an error has occurred.

Virtual Events The number of state changes or errors that occurred on this virtual link.

Neighbor Events The number of times this neighbor relationship has changed state, or an error has occurred.

External LSA Count The number of external (LS type 5) link-state advertisements in the link-state database.

LSAs Received The number of LSAs received.

Originate New LSAs The number of LSAs originated.

14.6.46 show ip ospf neighbor

This command displays the OSPF neighbor table list. When you specify a particular neighbor ID, detailed information about a neighbor is given. The information below displays only if OSPF is enabled and the interface has a neighbor. The `<ipaddr>` parameter is the IP address of the neighbor.

Format **`show ip ospf neighbor <`**`ipaddr`**`>`** `<slot/port`**`>`**

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes..

Router Id Is a 4-digit dotted-decimal number identifying neighbor router.

Options Indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.

Router Priority Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.

State Shows the state of the neighboring routers. Possible values are:

Down- initial state of the neighbor conversation - no recent information has been received from the neighbor.

Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.

Init - an Hello packet has recently been seen from the neighbor, but bi-directional communication has not yet been established.

2 way - communication between the two routers is bi-directional.

Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.

Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor.

Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.

Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

Events The number of times this neighbor relationship has changed state, or an error has occurred.

Permanence Displays the status of the entry, either dynamic or permanent. This refers to how the neighbor became known.

Hellos Suppressed Indicates whether Hellos are being suppressed to the neighbor.

Retransmission Queue Length Is an integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

14.6.47 show ip ospf neighbor brief

This command displays the OSPF neighbor table list. The information below is displayed only if OSPF is enabled.

Format **`show ip ospf neighbor brief`** *`{<slot/port> | all}`*

Modes Privileged EXEC
User EXEC

Router ID A 4 digit dotted decimal number representing the neighbor interface.

IP Address An IP address representing the neighbor interface.

Neighbor Interface Index Is a *`slot/port`* identifying the neighbor interface index.

State Displays the current state of the neighboring router. Possible values are:

Down- initial state of the neighbor conversation - no recent information has been received from the neighbor.

Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.

Init - an Hello packet has recently been seen from the neighbor, but bi-directional communication has not yet been established.

2 way - communication between the two routers is bi-directional.

Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.

Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor.

Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.

Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

14.6.48 show ip ospf range

This command displays information about the area ranges for the specified <*areaid*>. The <*areaid*> identifies the OSPF area whose ranges are being displayed.

Format `show ip ospf range <areaid>`

Modes Privileged EXEC
User EXEC

Area ID The area id of the requested OSPF area.

IP Address An IP Address which represents this area range.

Subnet Mask A valid subnet mask for this area range.

Lsdb Type The type of link advertisement associated with this area range.

Advertisement The status of the advertisement.Possible values are enabled or disabled.

14.6.49 show ip ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format `show ip ospf stub table`

Modes Privileged EXEC
User EXEC

Area ID Is a 32-bit identifier for the created stub area.

Type of Service Is the type of service associated with the stub metric. The 7300 Series Managed Switch only supports Normal TOS.

Metric Val The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.

Metric Type Is the type of metric advertised as the default route.

Import Summary LSA Controls the import of summary LSAs into stub areas.

14.6.50 show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The <*areaid*> parameter identifies the area and the <*neighbor*> parameter identifies the neighbor's Router ID.

Format `show ip ospf virtual-link <areaid> <neighbor>`

Modes Privileged EXEC
User EXEC

Area ID The area id of the requested OSPF area.

Neighbor Router ID The input neighbor Router ID.

Hello Interval The configured hello interval for the OSPF virtual interface.

Dead Interval The configured dead interval for the OSPF virtual interface.

Iftransit Delay Interval The configured transit delay for the OSPF virtual interface.

Retransmit Interval The configured retransmit interval for the OSPF virtual interface.

Authentication Type The configured authentication type of the OSPF virtual interface.

State The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.

Neighbor State The neighbor state.

14.6.51 show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

Format `show ip ospf virtual-link brief`

Modes Privileged EXEC
User EXEC

Area Id The area id of the requested OSPF area.

Neighbor The neighbor interface of the OSPF virtual interface.

Hello Interval The configured hello interval for the OSPF virtual interface.

Dead Interval The configured dead interval for the OSPF virtual interface.

Retransmit Interval The configured retransmit interval for the OSPF virtual interface.

Transit Delay The configured transit delay for the OSPF virtual interface.

14.7 Routing Information Protocol (RIP) Commands

This section describes the commands you use to view and configure RIP, which is a distance-vector routing protocol that you use to route traffic within a small network.

14.7.1 router rip

Use this command to enter Router RIP mode.

Format	`router rip`
Mode	Global Config

14.7.2 enable (RIP)

This command resets the default administrative mode of RIP in the router (active).

Default	enabled
Format	`enable`
Mode	Router RIP Config

14.7.2.1 no enable (RIP)

This command sets the administrative mode of RIP in the router to inactive.

Format	`no enable`
Mode	Router RIP Config

14.7.3 ip rip

This command enables RIP on a router interface.

Default	disabled
Format	`ip rip`
Mode	Interface Config

14.7.3.1 no ip rip

This command disables RIP on a router interface.

Format	`no ip rip`
Mode	Interface Config

14.7.4 auto-summary

This command enables the RIP auto-summarization mode.

Default	disabled
Format	`auto-summary`
Mode	Router RIP Config

14.7.4.1 no auto-summary

This command disables the RIP auto-summarization mode.

Format	`no auto-summary`
Mode	Router RIP Config

14.7.5 default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format	`default-information originate`
Mode	Router RIP Config

14.7.5.1 no default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format	`no default-information originate`
Mode	Router RIP Config

14.7.6 default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

Format	**default-metric <*0-15*>**
Mode	Router RIP Config

14.7.6.1 no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format	`no default-metric`
Mode	Router RIP Config

14.7.7 distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route.

Default	15
Format	**`distance rip <`***`1-255`***`>`**
Mode	Router RIP Config

14.7.7.1 no distance rip

This command sets the default route preference value of RIP in the router.

Format	**`no distance rip`**
Mode	Router RIP Config

14.7.8 distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Default	0
Format	**`distribute-list`** *`<1-199>`* **`out`** *`{ospf	bgp	static	connected}`*
Mode	Router RIP Config

14.7.8.1 no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format	**`no distribute-list`** *`<1-199>`* **`out`** *`{ospf	bgp	static	connected}`*
Mode	Router RIP Config

14.7.8.2 no default-information originate

This command is used to control the advertisement of default routes.

Format	**`no default-information originate`**
Mode	Router RIP Config

14.7.9 ip rip authentication

This command sets the RIP Version 2 Authentication Type and Key for the specified interface. The value of <*type*> is either **none**, **simple**, or **encrypt**. The value for authentication key [*key*] must be 16 bytes or less. The [*key*] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the value of <*type*> is **encrypt**, a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

Default	none
Format	`ip rip authentication {none | {simple <key>} | {encrypt <key> <keyid>}}`
Mode	Interface Config

14.7.9.1 no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

Format	`no ip rip authentication`
Mode	Interface Config

14.7.10 ip rip receive version

This command configures the interface to allow RIP control packets of the specified version(s) to be received.

The value for <*mode*> is one of: **rip1** to receive only RIP version 1 formatted packets, **rip2** for RIP version 2, **both** to receive packets from either format, or **none** to not allow any RIP control packets to be received.

Default	both
Format	`ip rip receive version {rip1 | rip2 | both | none}`
Mode	Interface Config

14.7.10.1 no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format	`no ip rip receive version`
Mode	Interface Config

14.7.11 ip rip send version

This command configures the interface to allow RIP control packets of the specified version to be sent.

The value for <*mode*> is one of: **rip1** to broadcast RIP version 1 formatted packets, **rip1c** (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, **rip2** for sending RIP version 2 using multicast, or **none** to not allow any RIP control packets to be sent.

Default	rip2
Format	**ip rip send version** *{rip1 | rip1c | rip2 | none}*
Mode	Interface Config

14.7.11.1 no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

Format	**no ip rip send version**
Mode	Interface Config

14.7.12 hostroutesaccept

This command enables the RIP hostroutesaccept mode.

Default	enabled
Format	**hostroutesaccept**
Mode	Router RIP Config

14.7.12.1 no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format	**no hostroutesaccept**
Mode	Router RIP Config

14.7.13 split-horizon

This command sets the RIP split horizon mode.

Default	simple
Format	**split-horizon** *{none | simple | poison}*

Mode Router RIP Config

14.7.13.1 no split-horizon

This command sets the default RIP split horizon mode.

Format

```
no split-horizon
```

Mode Router RIP Config

14.7.14 redistribute

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match <match-type> the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

Default metric - not-configured; match - internal

Format for OSPF as source protocol

```
redistribute ospf [metric <0-15>] [match [inter-
nal] [external 1] [external 2] [nssa-external 1]
[nssa-external-2]]
```

Format for other source protocol

```
redistribute {bgp | static | connected} [metric
<0-15>]
```

Mode Router RIP Config

14.7.14.1 no redistribute

This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Format

```
no redistribute {ospf | bgp | static | connected}
[metric] [match [internal] [external 1] [external
2] [nssa-external 1] [nssa-external-2]]
```

Mode Router RIP Config

14.7.15 show ip rip

This command displays information relevant to the RIP router.

Format show ip rip

Modes Privileged EXEC
User EXEC

RIP Admin Mode Enable or disable.

Split Horizon Mode None, simple or poison reverse. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None - no special processing for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity. The default is simple

Auto Summary Mode Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries The default is enable.

Host Routes Accept Mode Enable or disable. If enabled the router accepts host routes. The default is enable.

Global Route Changes The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.

Global queries - The number of responses sent to RIP queries from other systems.

Default Metric Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are (1 to 15)

Default Route Advertise The default route.

14.7.16 show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e. ip rip).

Format `show ip rip interface brief`

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

IP Address The IP source address used by the specified RIP interface.

Send Version The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2.

Receive Version The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both

RIP Mode RIP administrative mode of router RIP operation; enable activates, disable de-activates it.

Link State The mode of the interface (up or down).

14.7.17 show ip rip interface

This command displays information related to a particular RIP interface.

Format `show ip rip interface <slot/port>`

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes. This is a configured value.

IP Address The IP source address used by the specified RIP interface. This is a configured value.

Send version The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.

Receive version The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.

Both RIP Admin Mode RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.

Link State Indicates whether the RIP interface is up or down. This is a configured value.

Authentication Type The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.

Default Metric A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value.

The following information will be invalid if the link state is down.

Bad Packets Received The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.

Bad Routes Received The number of routes contained in valid RIP packets that were ignored for any reason.

Updates Sent The number of triggered RIP updates actually sent on this interface.

14.8 Border Gateway Protocol (BGP) Commands

This section describes the commands you use to view and configure BGP, which is an exterior gateway routing protocol that you use to route traffic between autonomous systems. The BGP CLI commands are available in the 7300 Series Managed Switch software BGP Package.

14.8.1 router bgp

Use this command to enter Router BGP mode. The <*asnumber*> variable is the autonomous system (AS) number, which is a number from 1 to 65535. Each AS typically encapsulates a single IGP routing domain.

Format `router bgp <asnumber>`

Mode Global Config

14.8.2 aggregate-address

This command creates an address aggregation entry. The <*prefix*> is a valid IP address entry. The <*mask*> is the netmask for the ip address. A maximum of ten entries can be added.

Default	none
Format	**aggregate-address** <*prefix*> <*mask*>
Mode	Router BGP Config

14.8.2.1 no aggregate-address

This command deletes an address aggregation entry. The <*prefix*> is a valid IP address entry.

Format	**no aggregate-address** <*prefix*> <*mask*>
Mode	Router BGP Config

14.8.3 bgp addrfamily create

This command assigns the an Address Family with a Subsequent Address Family Identifier (SAFI). The AFI identifies a supported protocol, and is defined as having the value of IP version 4. The SAFI describes a sub-AFI value that is supported for the AFI. The possible values for <*safi*> are **unicast**, **multicast**, **both-unicast-multicast** and **labeldist**.

Default	none
Format	**bgp addrfamily create <*safi*>**
Mode	Router BGP Config

14.8.3.1 no bgp addrfamily create

This command deletes the Address Family with the assigned Subsequent Address Family Identifier (SAFI).TheAFI identifies a supported protocol, and is defined as having the value of IP version 4. The SAFI describes a sub-AFI value that is supported for the AFI. The possible values for <*safi*> are unicast, multicast, both-unicast-multicast and labeldist.

Default	none
Format	**no bgp addrfamily create <*safi*>**
Mode	Router BGP Config

14.8.4 bgp autorestart

This command informs the BGP4 module to enable automatic message sending in the case of connection failure.

Default	disabled
Format	**`bgp autorestart`**
Mode	Router BGP Config

14.8.4.1 no bgp autorestart

This command informs the BGP4 module to disable automatic message sending in the case of connection failure.

Format	**`no bgp autorestart`**
Mode	Router BGP Config

14.8.5 bgp calcmedmode

This command informs the BGP4 module to enable or disable the use of the Calculated MED attribute. The MED attribute is used to describe the degree of preference of a particular link.

Default	disabled
Format	**`bgp calcmedmode`**
Mode	Router BGP Config

14.8.5.1 no bgp calcmedmode

This command informs the BGP4 module to disable (set to default) the use of the Calculated MED attribute.

Format	**`no bgp calcmedmode`**
Mode	Router BGP Config

14.8.6 bgp cluster-id

This command assigns the cluster ID to which the router belongs. The Cluster value is a valid IP address.

Default	0.0.0.0
Format	**`bgp cluster-id <`***`clusterid`***`>`**
Mode	Router BGP Config

14.8.6.1 no bgp cluster-id

This command assigns the default cluster ID to which the router belongs.

Format	**`no bgp cluster-id`**
Mode	Router BGP Config

14.8.7 bgp community

This command specifies the associated community value for the route exchanges. The community attribute values range from 0x00000000 through 0x0000FFFF and 0xFFFF0000 through 0xFFFFFFFF are reserved. The rest of the community attribute values are encoded using an autonomous system number in the first two octets. The range is 1 to 65535.

Default	none
Format	**`bgp community`** *`<1-65535>`*
Mode	Router BGP Config

14.8.7.1 no bgp community

This command specifies the default associated community value for the route exchanges.

Default	none
Format	**`no bgp community`**
Mode	Router BGP Config

14.8.8 bgp confederation identifier

This command assigns the external AS number that identifies the AS confederation. The range for this field is 1 to 65535.

Default	0
Format	**`bgp confederation identifier <`***`confedid`***`>`**
Mode	Router BGP Config

14.8.8.1 no bgp confederation identifier

This command resets the bgp confederation identifier value to its default.

Default	0
Format	**`no bgp confederation identifier`**
Mode	Router BGP Config

14.8.9 bgp default local-preference

This command sets the local preference of the BGP4 router. The range for this field is -1 to 2147483647. A value of -1 indicates the absence of this attribute.

Default	none
Format	**`bgp default local-preference`** *`<-1-2147483647>`*
Mode	Router BGP Config

14.8.9.1 no bgp default local-preference

This command sets the default value of local preference of the BGP4 router.

Format	**`no bgp default local-preference`**
Mode	Router BGP Config

14.8.10 bgp flapdamping dampfactor

This command configures the flap damping factor. The range for this field is 1 to 65535.

Default	2
Format	**`bgp flapdamping dampfactor <`***`dampfactor`***`>`**
Mode	Router BGP Config

14.8.10.1 no bgp flapdamping dampfactor

This command configures the default flap damping factor.

Format	**`no bgp flapdamping dampfactor`**
Mode	Router BGP Config

14.8.11 bgp flapdamping flapmaxtime

This command configures the flap entry lifetime in seconds. The range for this field is 1 to 65535.

Default	900
Format	**`bgp flapdamping flapmaxtime <`***`seconds`***`>`**
Mode	Router BGP Config

14.8.11.1 no bgp flapdamping flapmaxtime

This command configures the default flap entry lifetime.

Format	**`no bgp flapdamping flapmaxtime`**
Mode	Router BGP Config

14.8.12 bgp flapdamping mode

This command enables the damping of the route flaps. Damping suppresses the advertisement of the route close to the route source until the route becomes stable. The possible values for this field are *`enable`* and *`disable.`*

Default	disabled
Format	**`bgp flapdamping mode`**
Mode	Router BGP Config

14.8.12.1 no bgp flapdamping mode

This command disables the damping of the route flaps. Damping suppresses the advertisement of the route close to the route source until the route becomes stable.

Format	**`no bgp flapdamping mode`**
Mode	Router BGP Config

14.8.13 bgp flapdamping penaltyinc

This command configures the route damping penalty increment. The range for this field is 1 to 65535*.*

Default	100
Format	**`bgp flapdamping penaltyinc <`***`penalty`***`>`**
Mode	Router BGP Config

14.8.13.1 no bgp flapdamping penaltyinc

This command configures the default route damping penalty increment.

Format	**`no bgp flapdamping penaltyinc`**
Mode	Router BGP Config

14.8.14 bgp flapdamping reuselimit

This command configures the reuse limit of the flapped route. The range for this field is 1 to 65535.

Default	2
Format	**`bgp flapdamping reuselimit <`*`limit`*`>`**
Mode	Router BGP Config

14.8.14.1 no bgp flapdamping reuselimit

This command configures the default reuse limit of the flapped route.

Format	**`no bgp flapdamping reuselimit`**
Mode	Router BGP Config

14.8.15 bgp flapdamping reusemaxsize

This command configures the maximum reuse array size. The range for this field is 1 to 65535.

Default	1024
Format	**`bgp flapdamping reusemaxsize <`*`size`*`>`**
Mode	Router BGP Config

14.8.15.1 no bgp flapdamping reusemaxsize

This command configures the default reuse array size.

Format	**`no bgp flapdamping reusemaxsize`**
Mode	Router BGP Config

14.8.16 bgp flapdamping suppresslimit

This command configures the damping suppress limit of the route flaps. The range for this field is 1 to 65535.

Default	600
Format	**`bgp flapdamping suppresslimit <`*`limit`*`>`**
Mode	Router BGP Config

14.8.16.1 no bgp flapdamping suppresslimit

This command configures the default suppress limit of the route flaps.

Format	**`no bgp flapdamping suppresslimit`**
Mode	Router BGP Config

14.8.17 bgp flapdamping timerresolution

This command configures the delta time used in flap damping. The range for this field is 1 to 65535*.*

Default	2
Format	**`bgp flapdamping timerresolution <`***`resolution`***`>`**
Mode	Router BGP Config

14.8.17.1 no bgp flapdamping timerresolution

This command configures the default delta time used in flap damping.

Format	**`no bgp flapdamping timerresolution`**
Mode	Router BGP Config

14.8.18 bgp interval minasorigin

This command sets the time interval in seconds for the Minimum AS origination interval*.* The range for this field is 1 to 32767 seconds*.*

Default	15
Format	**`bgp interval minasorigin <`***`1-32767`***`>`**
Mode	Router BGP Config

14.8.18.1 no bgp interval minasorigin

This command sets the time interval to the default value for the Minimum AS origination interval*.*

Format	**`no bgp interval minasorigin`**
Mode	Router BGP Config

14.8.19 bgp interval minrouteadvint

This command sets the time interval in seconds for the minimum route advertisement interval. This controls the frequency of route advertisements. The range for this field is 1 to 32767 seconds.

Default	30
Format	**`bgp interval minrouteadvint <`***`1-32767`***`>`**
Mode	Router BGP Config

14.8.19.1 no bgp interval minrouteadvint

This command sets the time interval to the default value for the minimum route advertisement interval.

Format	**`no bgp interval minrouteadvint`**
Mode	Router BGP Config

14.8.20 bgp localmed

This command sets the local Multi-Exit-Discriminator (MED) value for the BGP4 router. This metric is used to discriminate between multiple exit points to an adjacent autonomous system. The range for this field is -1 to 2147483647. A value of -1 indicates the absence of this attribute.

Default	none
Format	**`bgp localmed <`***`localmed`***`>`**
Mode	Router BGP Config

14.8.20.1 no bgp localmed

This command sets the local Multi-Exit-Discriminator (MED) value to the default value for the BGP4 router. This metric is used to discriminate between multiple exit points to an adjacent autonomous system.

Format	**`no bgp localmed`**
Mode	Router BGP Config

14.8.21 bgp optionalcap

This command enables the specified capability. Optional capabilities allow a BGP4 speaker to be aware of the protocol extension capabilities of a BGP4 neighbor. By default, all capabilities are disabled. The possible optional capabilities are **`multiproto`**, **`routereflect`**, **`community`**, **`confed`**, and **`all`**. Each capability may be enabled or disabled.

Default	disabled
Format	**`bgp optionalcap <`***`option`***`>`**
Mode	Router BGP Config

14.8.21.1 no bgp optionalcap

This command disables the specified capability. The possible optional capabilities are **multiproto**, **routereflect**, **community**, **confed,** and **all**.

Format	**`no bgp optionalcap <`***`option`***`>`**
Mode	Router BGP Config

14.8.22 bgp origin

This command sets a value for the Origin attribute of the locally originated routes. The possible values for <*`origin`*> are **`igp`**, **`egp`**, and **`incomplete`**.

Format	**`bgp origin <`***`origin`***`>`**
Mode	Router BGP Config

14.8.23 bgp policy

This command creates a policy with an access mode of permit or deny and with the specified index. The possible value for the <*`protocol`*> are **`bgpinternalin`**, and **`bgpinternalout`**. The possible values for the <*`matchtype`*> are **`aspath`**, **`origin`**, **`localpreference`**, **`multiexitdisc`**, **`community`**, **`confederationid`**, **`clusternumber`**, **`nexthop`**, **`lenaspath`**, **`peer`**, **`atomicaggregate`**, **`aggregatoras`**, and **`aggregatorid`**. You can add a maximum of 20 policies.

Default	none
Format	**`bgp policy`** *`<index> <access> <protocol> <matchtype`***`>`**
Mode	Router BGP Config

14.8.23.1 no bgp policy

This command deletes a policy entry.

Format	no bgp policy <*index*>
Mode	Router BGP Config

14.8.24 bgp policy action addint

This command configures an **add** action on the policy identified with the specified index. This command is used with matchtypes that use an integer as a modifier. The possible values for the <*matchtype*> are **aspath**, **origin**, **localpreference**, **multiexitdisc**, **community, confederationid**, **lenaspath**, **atomicaggregate**, and **aggregatoras**. The <*value*> parameter is an integer.

If the matchtype is community, the integer value is specified as a 32-bit number. The first 16 bits represent the AS number and the second 16 bits represent any arbitrary number. The combination of the 2 16-bit fields comprise the 32-bit community number. For example, a system with AS number 1 and using arbitrary number 256 might specify community as 65792 which is equivalent to 0x00010100.

The ranges for the matchtypes are as follows:

Table 14-1. BGP Policy Matchtypes

matchtype	range
aspath	1 to 65535
origin	1 to 3
localpreference	1 to 65535
multiexitdisc	1 to 65535
community	1 to 4294967295
confederationid	1 to 65535
lenaspath	1 to 65535
atomicaggregate	1 to 2
aggregatoras	0 to 65535

Format	**bgp policy action addint** <*index*> <*matchtype*> <*value*>
Mode	Router BGP Config

14.8.24.1 no bgp policy action addint

This command configures an **add** action on the policy identified with the specified index. This command is used with matchtypes that use an integer as a modifier. The possible values for the <*matchtype*> are **aspath**, **origin**, **localpreference**, **multiexitdisc**, **community**, **confederationid**, **lenaspath**, **atomicaggregate**, and **aggregatoras**. The [*value*] parameter is an integer and is used only for match types of **aspath** and **community**.

Format	**no bgp policy action addint** <*index*> <*matchtype*> [*value*]
Mode	Router BGP Config

14.8.25 bgp policy action addint modify

This command configures a ‘modify’ action on the policy identified with the specified index. This command is used with matchtypes that use an integer as a modifier. The possible values for the <*matchtype*> are **aspath**, **origin**, **localpreference**, **multiexitdisc**, **community**, **confederationid**, **lenaspath**, **atomicaggregate**, and **aggregatoras**. The [*value*] parameter is an integer and is used only for match types of **aspath** and **community**.

If the matchtype is community, the integer value is specified as a 32-bit number. The first 16 bits represent the AS number and the second 16 bits represent any arbitrary number. The combination of the 2 16-bit fields comprise the 32-bit community number. For example, a system with AS number 1 and using arbitrary number 256 might specify community as 65792 which is equivalent to 0x00010100.

Format	**bgp policy action addint modify** <*index*> <*matchtype*> <*value*> [*value*]
Mode	Router BGP Config

14.8.26 bgp policy action addip

This command configures an ‘add’ action on the policy identified with the specified index. This command is used with matchtypes that use an IP Address as a modifier. The possible values for the <*matchtype*> are **clusternumber**, **nexthop**, and **aggregatorid**. The <*ipaddr*> parameter is a valid IP Address.

Format	**bgp policy action addip** <*index*> <*matchtype*> <*ipaddr*>
Mode	Router BGP Config

14.8.26.1 no bgp policy action addip

This command configures an 'delete' action on the policy identified with the specified index. This command is used with matchtypes that use an IP Address as a modifier. The possible values for the <*matchtype*> are `clusternumber`, *nexthop*, and *aggregatorid*.

Format **no bgp policy action addip** *<index> <matchtype> [ipaddr]*

Mode Router BGP Config

14.8.27 bgp policy action addip modify

This command configures an 'modify' action on the policy identified with the specified index. This command is used with matchtypes that use an IP Address as a modifier. The possible values for the <*matchtype*> are `clusternumber`, *nexthop*, and *aggregatorid*. The <*ipaddr*> and *[ipaddr]* parameters are IP Addresses. The [*ipaddr]* parameter is only used if the <*matchtype*> is `clusternumber`.

Format **bgp policy action addip modify** *<index> <matchtype> <ipaddr> [ipaddr]*

Mode Router BGP Config

14.8.28 bgp policy action remove

This command removes an action identified by the <*matchtype*> from the policy identified with the specified index. The possible values for the <*matchtype*> are *aspath, origin, localpreference, multiexitdisc, community, confederationid, clusternumber, nexthop, lenaspath, peer, atomicaggregate, aggregatoras,* and *aggregatorid.*

If the matchtype is community, the integer value a 32-bit number. The first 16 bits represent the AS number and the second 16 bits represent any arbitrary number. The combination of the two 16-bit fields comprise the 32-bit community number. For example, a system with AS number 1 and using arbitrary number 256 might specify community as 65792 which is equivalent to 0x00010100.

Format **bgp policy action remove** *<index> <matchtype>*

Mode Router BGP Config

14.8.29 bgp policy range address

This command adds a network IP address to a policy*.* The value for <*peerlocalid*> is an IP address, and <*mask*> is a network mask. Use a mask of 255.255.255.255 for an exact peer match.

Format	**`bgp policy range address`** *<index> <peerlocalid> <mask>*
Mode	Router BGP Config

14.8.30 bgp policy range between

This command adds a range to a policy identified by <*index*>*.* The range is specified by its outer bounds <*minvalue*> and <*maxvalue*>, which are from 1 to 4294967295.

Format	**`bgp policy range between`** *<index> <minvalue> <max-value>*
Mode	Router BGP Config

14.8.31 bgp policy range equal

This command adds a value equal-to specification to a policy identified by <*index*>*.* The <*value*> parameter is an integer from 0 to 4294967295.

Default	none
Format	**`bgp policy range equal`** *<index> <value>*
Mode	Router BGP Config

14.8.32 bgp policy range greaterthan

This command adds a greater than range specification to a policy identified by <*index*>*.* The <*value*> parameter is an integer from 0 to 4294967295.

Default	none
Format	**`bgp policy range greaterthan`** *<index> <value>*
Mode	Router BGP Config

14.8.33 bgp policy range lessthan

This command adds a less than range specification to a policy identified by <*index*>. The <*value*> parameter is an integer from 0 to 4294967295.

Default	none
Format	`bgp policy range lessthan <index> <value>`
Mode	Router BGP Config

14.8.34 bgp propmedmode

This command informs the BGP4 module to enable propagation of the MULTI_EXIT_DISC (MED) metric. The possible values for this field are enable and disable.

Default	disabled
Format	`bgp propmedmode`
Mode	Router BGP Config

14.8.34.1 no bgp propmedmode

This command informs the BGP4 module to disable propagation of the MED metric.

Format	`no bgp propmedmode`
Mode	Router BGP Config

14.8.35 bgp router-id

This command sets the system identification of the BGP Router. Generally, this is the Router IP Address. The Router IP Address will be taken as the default value unless this is explicitly configured.

Default	0.0.0.0
Format	`bgp router-id <ipaddress>`
Mode	Router BGP Config

14.8.35.1 no bgp router-id

This command sets the system identification of the BGP Router. Generally, this is the Router IP Address. The Router IP Address will be taken as the default value unless this is explicitly configured.

Format	**`no bgp router-id <`***`ipaddress`***`>`**
Mode	Router BGP Config

14.8.36 bgp snpa

This command builds the list of SNPAs (Subnet Point of Attachment) by adding each entered SNPA address and its length to the SNPA list. The SNPA address is a valid IP address. The SNPA length is a valid length of an SNPA address with a range of 1 to 128. A maximum of 10 SNPAs can be added.

Default	none
Format	**`bgp snpa`** *`<snpaaddr> <snpalen>`*
Mode	Router BGP Config

14.8.36.1 no bgp snpa

This command removes the specified SNPA (Subnet Point of Attachment) entry from the list of SNPAs. The SNPA address is a valid IP address. The SNPA length is a valid length of an SNPA address with a range of 1 to 128.

Format	**`no bgp snpa`** *`<snpaaddr> <snpalen>`*
Mode	Router BGP Config

14.8.37 bgp suppressmode

This command informs the BGP4 module to enable the selection of less-specific routes. If this mode is enabled, more specific routes will be suppressed. The possible values for this field are *`enable`* and *`disable.`*

Default	disabled
Format	**`bgp suppressmode`**
Mode	Router BGP Config

14.8.37.1 no bgp suppressmode

This command informs the BGP4 module to disable the selection of less-specific routes.

Format	**`no bgp suppressmode`**
Mode	Router BGP Config

14.8.38 clear bgp

This command resets the peer connection. This command should be used carefully as it could cause route flapping and overhead. The <*neighboraddress*> parameter specifies the neighboring BGP4 speaker's IP address.

Default	none
Format	**`clear bgp <`***`neighboraddress`***`>`**
Mode	Privileged EXEC

14.8.39 default-information originate (BGP)

This command is used to enable the advertisement of default routes.

Format	**`default-information originate`**
Mode	Router BGP Config

14.8.39.1 no default-information originate (BGP)

This command is used to disable the advertisement of default routes.

Format	**`no default-information originate`**
Mode	Router BGP Config

14.8.40 default-metric (BGP)

This command is used to set a default for the metric of distributed routes.

Format	**`default-metric`** *`<0-4294967295>`*
Mode	Router BGP Config

14.8.40.1 no default-metric (BGP)

This command is used to delete the default for the metric of distributed routes.

Format	**`no default-metric`**
Mode	Router BGP Config

14.8.41 distance bgp

This command sets the route preference value of BGP-4 routes in the router. Lower route preference values are preferred when determining the best route.

Default	170
Format	**`distance bgp`** *`<1-255>`*
Mode	Router BGP Config

14.8.41.1 no distance bgp

This command sets the default route preference value of BGP-4 routes in the router.

Format	**`no distance bgp`**
Mode	Router BGP Config

14.8.42 distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format	**`distribute-list`** *`<1-199>`* **`out`** *`{rip	ospf	static	connected}`*
Mode	Router BGP Config

14.8.42.1 no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format	**`no distribute-list`** *`<1-199>`* **`out`** *`{ospf	rip	static	connected}`*
Mode	Router BGP Config

14.8.43 enable (BGP)

This command enables the administrative mode of BGP4 on the system.

Format	**`enable`**
Mode	Router BGP Config

14.8.43.1 no enable (BGP)

This command disables the administrative mode of BGP4 on the system.

Format	**`no enable`**
Mode	Router BGP Config

14.8.44 neighbor addrfamily

This command assigns an Address Family with a Subsequent Address Family Identifier (SAFI) to the peer. The AFI identifies a supported protocol, and the defined value is IP version 4. The SAFI describes a sub-AFI value that is supported for the AFI. The possible values for *<`safi`>* are *`unicast, multicast, both-unicast-multicast`* and *`labeldist.`* After executing this command, the BGP peer must be reset before the changes will take effect.

Default	none
Format	**`neighbor`** *`<peeripaddr>`* **`addrfamily`** *`<safi>`*
Mode	Router BGP Config

14.8.44.1 no neighbor addrfamily

This command removes the Address Family with the assigned Subsequent Address Family Identifier (SAFI). The AFI identifies a supported protocol, and is defined as IP version 4. The SAFI describes a sub-AFI value that is supported for the AFI. The possible values for *<`safi`>* are *`unicast, multicast, both-unicast-multicast`* and *`labeldist.`* After executing this command, the BGP peer must be reset before the changes will take effect.

Default	none
Format	**`no neighbor`** *`<peeripaddr>`* **`addrfamily`** *`<safi>`*
Mode	Router BGP Config

14.8.45 neighbor <peeripaddr> authentication none

This command configures the authentication type as none for a particular peer address, which is the default setting.

Format	**`neighbor`** *`<peeripaddr>`* **`authentication`** *`<none>`*
Mode	Router BGP Config

14.8.46 neighbor <peeripaddr> authentication simple

This command configures the authentication as simple password and the key for a particular peer address. This is used in OPEN messages to authenticate the peer connection. The key parameter must be less than16 characters long. After you execute this command, reset the BGP peer for the changes to take effect.

Default	none
Format	**neighbor** *<peeripaddr>* **authentication** *<simple>* *[key]*
Mode	Router BGP Config

14.8.47 neighbor confedmember

This command enables the peer as a member of the confederation. The possible values for this field are **enable** and **disable**. After you execute this command, reset the BGP peer for the changes to take effect.

Default	disabled
Format	**neighbor** *<peeripaddr>* **confedmember**
Mode	Router BGP Config

14.8.47.1 no neighbor confedmember

This command disables the peer as a member of the confederation. The possible values for this field are *enable* and *disable*. After executing this command, the BGP peer must be reset before the changes will take effect.

Format	**no neighbor <***peeripaddr***> confedmember**
Mode	Router BGP Config

14.8.48 neighbor connretry

This command specifies the connection retry interval in seconds for a peer. The range is 1 to 65535 seconds.

Default	120
Format	**neighbor <***peeripaddr***> connretry <***1-65535***>**
Mode	Router BGP Config

14.8.48.1 no neighbor connretry

This command specifies the default connection retry interval for a peer.

Format	**no neighbor <*peeripaddr*> connretry**
Mode	Router BGP Config

14.8.49 neighbor msgsendlimit

This command configures the maximum number of messages in a peer transmission queue. The range for <*sendlimit*> is 1 to 100. The <*peeripaddr*> parameter specifies the neighboring BGP4 speaker's IP address.

Default	100
Format	**neighbor <*peeripaddr*> msgsendlimit <*sendlimit*>**
Mode	Router BGP Config

14.8.49.1 no neighbor msgsendlimit

This command configures the default number of messages in the peer transmission queue

Format	**no neighbor <*peeripaddr*> msgsendlimit <*sendlimit*>**
Mode	Router BGP Config

14.8.50 neighbor next-hop-self

This command enables the peer as the next hop for the locally originated paths. The possible values for this field are enable and disable. After executing this command, the BGP peer must be reset before the changes take effect.

Default	disabled
Format	**neighbor <*peeripaddr*> next-hop-self**
Mode	Router BGP Config

14.8.50.1 no neighbor next-hop-self

This command disables the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

Format	**no neighbor** *<peeripaddr>* **next-hop-self**
Mode	Router BGP Config

14.8.51 neighbor optionalcap

This command enables the specified capability for the peer connection. Optional capabilities allow a BGP4 speaker to be aware of the protocol extensions capabilities of a BGP4 neighbor. The possible optional capabilities are multiproto, routereflect, community, confed, and all. Each capability may be enabled or disabled. After executing this command, the BGP peer must be reset before the changes take effect.

Default	all capabilities are disabled
Format	**`neighbor <`*`peeripaddr`*`> optionalcap`**
Mode	Router BGP Config

14.8.51.1 no neighbor optionalcap

This command disables the specified capability for the peer connection

Format	**`no neighbor <`*`peeripaddr`*`> optionalcap`**
Mode	Router BGP Config

14.8.52 neighbor remote-as

This command assigns the remote Autonomous System (AS) Number for the peer. The range for this field is 1 to 65535*.* After executing this command, the BGP peer must be reset before the changes take effect.

Format	**`neighbor <`*`peeripaddr`*`> remote-as <`*`peerasnumber`*`>`**
Mode	Router BGP Config

14.8.52.1 no neighbor

This command removes the remote Autonomous System (AS) number assignment for the peer. After executing this command, the BGP peer must be reset before the changes will take effect.

Format	**`no neighbor`** *`<peeripaddr>`* **`[remote-as]`**
Mode	Router BGP Config

14.8.53 neighbor route-reflector-client

This command enables the route reflector client. A route reflector client relies on a route reflector to re-advertise its routes to the entire AS. The possible values for this field are *`enable`* and *`disable.`* After executing this command, the BGP peer must be reset before the changes will take effect.

Default disabled

Format **neighbor <***peeripaddr***> route-reflector-client**

Mode Router BGP Config

14.8.53.1 no neighbor route-reflector-client

This command disables the route reflector client. After executing this command, the BGP peer must be reset before the changes will take effect.

Format **no neighbor <***peeripaddr***> route-reflector-client**

Mode Router BGP Config

14.8.54 neighbor shutdown

This command disables the state of the BGP4 peer connection by stopping the connection mode. The <*peeripaddr*> parameter specifies the neighboring BGP4 speaker's IP address.

Default disabled

Format **neighbor <***peeripaddr***> shutdown**

Mode Router BGP Config

14.8.54.1 no neighbor shutdown

This command enables the state of the BGP4 peer connection by opening the connection mode. The <*peeripaddr*> parameter specifies the neighboring BGP4 speaker's IP address.

Format **no neighbor <***peeripaddr***> shutdown**

Mode Router BGP Config

14.8.55 neighbor timers

This command specifies the keep alive and hold time for a peer. This value is placed in an OPEN message sent to this peer by this BGP speaker. The possible values for keep alive field are 0 to 21845 seconds and for hold time field are 0 and 3 to 65535 seconds. After executing this command, the BGP peer must be reset before the changes will take effect

Default holdtime - 180 seconds; keepalive - 90 seconds

Format **neighbor <***peeripaddr***> timers** <*keepalive*> <*holdtime*>

Mode Router BGP Config

14.8.55.1 no neighbor timers

This command specifies the default keep alive and hold time for a peer. After executing this command, the BGP peer must be reset before the changes will take effect

Format `no neighbor <peeripaddr> timers`

Mode Router BGP Config

14.8.56 neighbor txdelayint

This command configures the delay interval between two transmission sessions of MsgSendLimit packets. The range for this field is 1 to 5.

Format `neighbor <peeripaddr> txdelayint <1-5>`

Mode Router BGP Config

14.8.56.1 no neighbor txdelayint

This command configures the default delay interval between two transmission sessions of MsgSendLimit packets.

Format `no neighbor <peeripaddr> txdelayint`

Mode Router BGP Config

14.8.57 network

This command adds network layer reachability information (NLRI) to the BGP4 Router. The NLRI field contains a list of network numbers being advertised. The network number is a valid IP address entry. The `[send | donotsend]` field indicates whether or not this prefix should be sent. The <*vpncos*> field allows assignment of the VPN/CoS identifier. You can add a maximum of ten NLRIs.

Default none

Format `network <networknumber> [mask <networkmask> [<vpn-cos> [<nexthop> [send | donotsend]]]]`

Mode Router BGP Config

14.8.57.1 no network

This command removes NLRI (Network Layer Reachability Information) from the BGP4 Router. The Network number is a valid IP address entry.

Format `no network <networknumber> [mask <networkmask>]`

Mode Router BGP Config

14.8.58 redistribute

This command configures BGP protocol to redistribute routes from the specified source protocol/routers. RFC 1745 requires that the BGP/IDRP identifier must be equal to the OSPF router identifier at all times that the router is up. But in the current 7300 Series Managed Switch implementation, these two can be different.

Default	metric - none; match - internal
Format for OSPF as source protocol	**`redistribute ospf`** *`[metric <0-4294967295>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`*
Format for other source protocol	**`redistribute`** *`{rip | static | connected} [metric <0-4294967295>]`*
Mode	Router BGP Config

14.8.58.1 no redistribute

This command removes the configuration for the redistribution for BGP protocol from the specified source protocol/routers.

Format	**`no redistribute`** *`{ospf | bgp | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`*
Mode	Router BGP Config

14.8.59 route-aggregation

This command enables the usage of path address aggregation. The possible values for this field are *`enable`* and *`disable.`*

Default	disabled
Format	**`route-aggregation`**
Mode	Router BGP Config

14.8.59.1 no route-aggregation

This command disables the usage of path address aggregation.

Format	`no route-aggregation`
Mode	Router BGP Config

14.8.60 route-reflect

This command enables route reflection mode. If this is enabled, the BGP4 speaker will re-advertise to other BGP4 neighbor's routes*.*

Default	disabled
Format	`route-reflect`
Mode	Router BGP Config

14.8.60.1 no route-reflect

This command disables route reflection mode. If this is enabled, the BGP4 speaker will re-advertise to other BGP4 neighbor's routes*.*

Format	`no route-reflect`
Mode	Router BGP Config

14.8.61 trapflags

This command enables BGP4 trap flags.

Default	disabled
Format	`trapflags`
Mode	Router BGP Config

14.8.61.1 no trapflags

This command disables BGP4 trap flags.

Format	`no trapflags`
Mode	Router BGP Config

14.8.62 show ip bgp

This command displays all the entries in the BGP4 route table.

Format	`show ip bgp`
Mode	Privileged EXEC
PeerId	This displays the Peer ID for this entry in the BGP4 route table.
Prefix/Len	This displays the prefix and the prefix length of this entry in the BGP4 route table.
NextHop	This displays the Next Hop for this entry in the BGP4 route table.
VpncosId	This displays the VPN/CoS ID for this entry in the BGP4 route table.

14.8.63 show ip bgp addrfamilyinfo

This command displays the Address Family Identifier Info.

Format	`show ip bgp addrfamilyinfo`
Mode	Privileged EXEC
AFI	This displays the Address Family Identifier (AFI).
SAFI	This displays the Subsequent Address Family Identifier (SAFI).

14.8.64 show ip bgp aggregate-address

This command displays all the aggregation entries that are present in the aggregation list.

Format	`show ip bgp aggregate-address`
Mode	Privileged EXEC
Address Aggregation Mode	This field displays whether Path Attribute Aggregation is enabled or disabled.
Prefix/Len	This field displays the IP address which identifies the network and the prefix length.

14.8.65 show ip bgp brief

This command displays Border Gateway Protocol (BGP4) information and Route Redistribution information.

Format `show ip bgp brief`

Mode User EXEC

Admin Mode This displays the administrative mode of Border Gateway Protocol (BGP4) for the system.

Version This displays the version of BGP4 running on the router.

Local Identifier The router ID of the BGP4 router.

Local Autonomous System This represents the Autonomous number of the BGP4 router.

Propagate MED Mode This indicates whether the MULTI_EXIT_DISC (MED) propagation to internal links is enabled or disabled.

Calculate MED Mode This indicates whether or not to take the MULTI_EXIT_DISC (MED) metric into account when breaking a Phase 2 tie.

Minimum AS Origination Interval This represents the time interval in seconds for the Minimum AS Origination Interval timer.

Minimum Route Advertisement Interval This represents the time interval in seconds for the Minimum Route Advertisement Interval timer.

Optional Capabilities Supported This lists the optional capabilities supported by the BGP4 router. Route Reflector Mode

Route Reflector Mode Shows whether or not this router is configured as a route reflector.

Cluster ID This represents the cluster ID of the BGP4 router.

Confederation ID This represents the AS confederation ID to which the BGP4 router belongs.

Auto Restart Mode This states whether to automatically start message sending in the case of connection failure or not.

Default-Metric Default value for redistributed routes.

Default Route Advertise Indicates whether the default routes received from other source protocols are advertised or not.

Static Redistribution

Source Source protocol/routes that are being redistributed.

Metric-value Metric of the routes being redistributed.

Distribute-list The Access list used to filter redistributed routes

RIP Redistribution

Source Source protocol/routes that are being redistributed.

Metric-value Metric of the routes being redistributed.

Distribute-list The Access list used to filter redistributed routes

Connected Redistribution

Source Source protocol/routes that are being redistributed.

Metric-value Metric of the routes being redistributed.

Distribute-list The Access list used to filter redistributed routes.

OSPF Redistribution

Source Source protocol/routes that are being redistributed.

Metric-value Metric of the routes being redistributed.

Match-value The criteria by which OSPF routes are redistributed into other routing domains.

Distribute-list The Access list used to filter redistributed routes.

14.8.66 show ip bgp damping

This command displays all the information configured for BGP4 that relates to flap parameters. You can configure all of the parameters in the output.

Format `show ip bgp damping` *`{dampened-paths | flap-statistics}`*

Mode Privileged EXEC

Route Flap Mode This field indicates whether or not damping of the route flaps is enabled.

Suppress Limit This field displays the damping suppress limit for the route flaps.

Reuse Limit This field displays the reuse limit for the dampened routes.

Penalty Increment This field displays the penalty increment for the route flaps.

Delta Time This field is the delta time used for the dampened routes.

Flap Max Time This field displays the maximum flap entry time for the route.

Damping Factor This field is the exponential decay factor for the flapped routes.

Reuse Size This field displays the maximum reuse array size.

Prefix/Len This field displays the prefix and the prefix length for the entry in the route flap dampened table.

State This field indicates whether the route is suppressed, not suppressed, or reused.

Penalty Value This field indicates the accumulated penalty for the route.

Decay Decrement This field indicates the decay decrement for the entry in the route flag dampened table.

Time Created This field indicates the time that this entry was created.

Time Suppressed This field indicates the suppressing time for this route

Event State This field indicates the event state for this entry in the route flap dampened table.

14.8.67 show ip bgp local

This command displays the local parameter information for the BGP4 object in the system. You can configure all of the parameters in the output.

Format `show ip bgp local`

Mode Privileged EXEC

Route Local Origin This displays the value of the Local Origin attribute for the locally originated routes.

Route Local MED This displays the local multi-exit-discriminator value for the BGP4 router.

Route Local Preference This displays the Local Preference value used for the local originating routes.

Suppress Mode This indicates whether or not the selection of less-specific routes is suppressed. If this is set to <*enable*> then more specific routes will be suppressed.

Route Community This field displays the local associated community used for the locally originating routes.

Address Aggregation Mode This field states whether or not Address Aggregation is being used.

14.8.68 show ip bgp mplslabels

This command displays the multi protocol label switching (MPLS) information.

Format **`show ip bgp mplslabels`** *`<prefix> <prefixlen> <peerid> <vpncos>`*

Mode Privileged EXEC

Prefix This is the prefix of this entry in the BGP4 route table.

Prefix Length This is the prefix length of this entry in the BGP4 route table.

Peer ID This is the Peer ID for this entry in the BGP4 route table.

VPNCOS Id This is the VPN/CoS ID for this entry in the BGP4 route table.

Labels This shows the labels for this entry in the BGP4 route table

14.8.69 show ip bgp neighbors

This command displays information about state and current activity of connections with the BGP4 peers.

Format `show ip bgp neighbors <`*`peeripaddr`*`>`

Modes Privileged EXEC
User EXEC

Remote Address The remote IP address of the BGP4 peer.

Peer ID This is the unique identification number of the peer.

Peer Admin Status This states whether or not the peer is enabled.

Peer State This represents the state of the peer connection.

Local Port This is the local port of the BGP4 router.

Remote AS This is the remote AS number of the BGP4 peer.

Remote Port This is the remote port of the BGP4 peer.

Connect Retry Interval This is the time interval in seconds for the connection retry.

Confederation Member This field indicates whether or not the peer is enabled as a confederation member.

Optional Capabilities This lists the optional capabilities supported by the BGP4 router.

Route Reflector Mode This states whether or not the peer is a route reflection client.

Next Hop Self Mode This states whether or not the BGP4 router will configure itself as the next hop for the locally originated paths.

Authentication Code This is the authentication mechanism being used between the peers.

Local Interface Address This is the local interface address of the BGP4 router used as Next Hop to this peer when new local path is originated.

Message Send Limit This states the maximum number of messages in the peer transmission queue for the BGP4 peer.

Transmission Delay Interval This states the delay interval between two transmission sessions for the BGP4 peer.

Negotiated Version This states the negotiated version between the peers.

Configured Hold Time This states the configured hold time between the peers.

Configured Keep Alive Time This states the configured keep alive time between the peers.

Configured Prefix Limit Shows the configured prefix limit, if any.

Configured Prefix Warning Threshold Shows the configured prefix warning threshold.

Warning Only On Prefix Limit Shows whether a warning will be sent before the prefix limit is reached.

14.8.70 show ip bgp neighbors addrfamilyinfo

This command displays the BGP4 Peer Address Family Information.

Format `show ip bgp neighbors addrfamilyinfo <peeripaddr>`

Modes Privileged EXEC
User EXEC

AFI This displays the Address Family Identifier (AFI).

SAFI This displays the Subsequent Address Family Identifier (SAFI)

14.8.71 show ip bgp neighbors stats

This command displays the peer statistics for the specified peer. The <*peeripaddr*> parameter specifies the neighboring BGP4 speaker's IP address.

Format **`show ip bgp neighbors stats <`*`peeripaddr`*`>`**

Modes Privileged EXEC
User EXEC

Peer Admin Status This represents the state of the peer connection.

Remote Address This represents the IP address of the remote peer.

Updates Received This represents the total number of Update Packets received from the peer.

Updates Sent This represents the total number of Update Messages sent to the peer.

Total Messages Received This represents the total number of messages received from the peer.

Total Messages Sent This represents the total number of messages sent to the peer.

Last Error This states the last error seen on this connection.

Established Transitions This represents the total number of times the BGP4 FSM transitioned into the established state.

Established Time This represents the time the BGP peer has been in the established state.

Time Elapsed since Last Update This represents the time since the last update message was received from the specified BGP peer.

14.8.72 show ip bgp nlrilist

This command displays all the NLRI (Network Layer Reachability Information) entries in the BGP4 route table.

Format	`show ip bgp nlrilist`
Mode	Privileged EXEC
Prefix/len	This displays the prefix and the prefix length of this entry in the NLRI list.
NextHop	This displays the Next Hop for this entry in the NLRI List.
VpnCosId	This displays the VPN/CoS ID for this entry in the NLRI List.
Send Now	This field indicates whether or not this prefix is being sent

14.8.73 show ip bgp pathattrtable

This command displays the BGP4 received path attribute table. This table contains one entry per path to a network, with path attributes received from all peers running BGP4.

Format	`show ip bgp pathattrtable`
Mode	Privileged EXEC
Peer	The IP address of the peer for this path attribute.
Prefix/Length	The network/prefix-length (i.e. route) for this path attribute.
Origin	The origin of the information. This can have three values: IGP - learned from an internal peer EGP - learned from an external peer Incomplete - origin of information not known
ASPath	Displays the segments of the ASPath (the path taken by the update through the different autonomous systems -- this path is used to prevent loops). If the path attribute has no value, it will show “empty”.
NextHop	The address of the router that will be the destination for traffic to the network of this path attribute.
MultiExitDisc	This field displays the value of the multi-exit-discriminator (MED) metric which discriminates between multiple exit points to an adjacent autonomous system.

LocalPref This field indicates the preference for an advertised route, with higher values being preferred.

AtomicAggr This field indicates whether the BGP4 router has selected the less specific route or not.

AggrAS This field indicates the AS number of the most recent BGP4 router which preformed route aggregation.

Aggregator This field indicates the IP address of the most recent BGP4 router which performed route aggregation.

CalcLocalPref This field indicates the degree of preference calculated by the receiving BGP4 router for an advertised route.

Communities This field shows the associated community value for the route exchanges.

Best This field indicates whether this route is considered the best route from any routes that are available to choose from. If only one route is available, it will be considered best. It will show True / False.

Unknown Attributes This field indicates if there are any attributes in the received update that are of an unknown type to this version of BGP. Usually this field will contain “NONE”. If there is a unknown attribute, it will show the content of that field.

14.8.74 show ip bgp peer-list

This command displays all the entries in the BGP4 Peer list.

Format `show ip bgp peer-list`

Modes Privileged EXEC
User EXEC

Peer Address This is the IP Address of the Peer.

14.8.75 show ip bgp policy brief

This command displays the policy table for the BGP4 router.

Format `show ip bgp policy brief`

Mode Privileged EXEC

Index This displays the index of this entry in the policy table.

Protocol This displays the protocol that was assigned to this policy in the policy table.

MatchType This displays the match type associated with this policy.

permit/deny This indicates whether this policy entry has permit or deny access.

14.8.76 show ip bgp policy detailed

This command displays the details of a specified policy for the BGP4 router.

Format **`show ip bgp policy detailed <`*`index`*`>`**

Mode Privileged EXEC

Policy Index This displays the index of this entry in the policy table.

Protocol ID This displays the protocol that was assigned to this policy in the policy table.

Access Mode This indicates whether this policy entry has permit or deny access.

Match Type This displays the match type associated with this policy.

For each action configured for this policy, the following is displayed:

Action Type This indicates the type of action. Possible values are add, modify or delete.

Match Type The match type associated with this action.

Values The values associated with this match.

14.8.77 show ip bgp snpalist

This command displays the list of SNPAs (Subnet Point of Attachment) that have been added to the BGP4 router.

Format **`show ip bgp snpalist`**

Mode Privileged EXEC

SNPA Address This displays the SNPA IP Address of this entry in the table.

SNPA Length This displays the length of this SNPA address in the table.

14.8.78 show ip bgp trapflags

This command displays the status of the BGP4 trapflags.

Format	**`show ip bgp trapflags`**
Mode	Privileged EXEC
BGP4 Traps	This is the status of the BGP4 trapflags.

Chapter 15
IP Multicast Commands

This section describes the IP Multicast commands available in the 7300 Series Managed Switch CLI.

This section contains the following topics:

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.

15.1 Multicast Commands

This section describes the commands you use to configure IP Multicast and to view IP Multicast settings and statistics.

15.1.1 ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message appears if you enable multicast routing while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Default	disabled
Format	**`ip multicast`**
Mode	Global Config

15.1.1.1 no ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to inactive. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Format	**`no ip multicast`**
Mode	Global Config

15.1.2 ip mcast boundary

This command adds an administrative scope multicast boundary specified by <*`groupipaddr`*> and <*`mask`*> for which this multicast administrative boundary is applicable. <*`groupipaddr`*> is a group IP address and <*`mask`*> is a group IP mask.

Format	**`ip mcast boundary <`***`groupipaddr`***`> <mask>`**
Mode	Interface Config

15.1.2.1 no ip mcast boundary

This command deletes an administrative scope multicast boundary specified by <*groupipaddr*> and <*mask*> for which this multicast administrative boundary is applicable. <*groupipaddr*> is a group IP address and <*mask*> is a group IP mask.

Format	**no ip mcast boundary <*groupipaddr*> <*mask*>**
Mode	Interface Config

15.1.3 ip multicast staticroute

This command creates a static route which is used to perform RPF checking in multicast packet forwarding. The combination of the <*sourceipaddr*> and the <*mask*> fields specify the network IP address of the multicast packet source. The <*groupipaddr*> is the IP address of the next hop toward the source. The <*metric*> is the cost of the route entry for comparison with other routes to the source network and is a value in the range of 0 and 255. The *current* incoming interface is used for RPF checking for multicast packets matching this multicast static route entry.

Default	none
Format	**ip multicast staticroute** *<sourceipaddr> <mask> <rpfipaddr> <metric> <slot/port>*
Mode	Global Config

15.1.3.1 no ip multicast staticroute

This command add deletes a static route in the static mcast table. The <*sourceipaddr*> is the IP address of the multicast packet source.

Format	**no ip multicast staticroute <*sourceipaddr*>**
Mode	Global Config

15.1.4 ip multicast ttl-threshold

This command applies the given <*ttlthreshold*> to a routing interface. The <*ttlthreshold*> is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface*.* The value for <*ttlthreshold*> has range from 0 to 255.

Default	1
Format	**ip multicast ttl-threshold <*ttlvalue*>**
Mode	Interface Config

15.1.4.1 no ip multicast ttl-threshold

This command applies the default <*`ttlthreshold`*> to a routing interface. The <*`ttlthreshold`*> is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Format	**`no ip multicast ttl-threshold`**
Mode	Interface Config

15.1.5 disable ip multicast mdebug mtrace

This command is used to disable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Default	none
Format	**`disable ip multicast mdebug mtrace`**
Mode	Global Config

15.1.5.1 no disable ip multicast mdebug mtrace

This command is used to enable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Format	**`no disable ip multicast mdebug mtrace`**
Mode	Global Config

15.1.6 mrinfo

This command is used to query the neighbor information of a multicast-capable router specified by *`[ipaddr]`*. The default value is the IP address of the system at which the command is issued. The mrinfo command can take up to 2 minutes to complete. Only one mrinfo command may be in process at a time. The results of this command will be available in the results bufferpool which can be displayed by using **`show mrinfo`**.

Default	none
Format	**`mrinfo`** *`[<ipaddr>]`*
Mode	Privileged EXEC

15.1.7 mstat

This command is used to find the IP Multicast packet rate and loss information path from a source to a receiver (unicast router id of the host running mstat). The results of this command will be available in the results bufferpool which can be displayed by using the command Section 15.1.18 "show mstat" on page 15-11. If a debug command is already in progress, a message is displayed and the new request fails.

The <*source*> is the IP address of the remote multicast-capable source. The [*receiver*] is the IP address of the receiver. The default value is the IP address of the system at which the command is issued. The [*group*] is a multicast address of the group to be displayed. The default value is 224.2.0.1(the group used for the multicast backbone).

Note: The group and receiver IP addresses can be entered in any order.

Default	none
Format	`mstat <source> [<group/receiver>] [<group/receiver>]`
Mode	Privileged EXEC

15.1.8 mtrace

This command is used to find the IP Multicast path from a source to a receiver (unicast router ID of the host running mtrace). A trace query is passed hop-by-hop along the reverse path from the receiver to the source, collecting hop addresses, packet counts, and routing error conditions along the path, and then the response is returned to the requestor. The results of this command are available in the results buffer pool which can be displayed by using the command Section 15.1.19 "show mtrace" on page 15-11.

The <*source*> is the IP address of the remote multicast-capable source. The *[receiver]* is the IP address of the receiver. The default value is the IP address of system at which the command is issued. The *[group]* is the multicast address of the group to be displayed. The default value is 224.2.0.1(the group used for the multicast backbone).

If a debug command is already in execution, a message is displayed and the new request fails.

Note: The group and destination IP addresses can be entered in any order.

Default	none
Format	`mtrace` *<sourceipaddr> [<group/destination>] [<group/destination >]*
Mode	Privileged EXEC

15.1.9 no ip mcast mroute

This command is used to clear entries in the mroute table. The all parameters is used to clear all entries.

The source parameter is used to clear the routes in the mroute table entries containing the specified *<sourceipaddr>* or *<sourceipaddr> [groupipaddr]* pair. The source address is the source IP address of the multicast packet. The group address is the Group Destination IP address of the multicast packet.

The group parameter is used to clear the routes in the mroute table entries containing the specified *<groupipaddr>*. The group address is the Group Destination IP address of the multicast packet.

Default	none
Format	`no ip mcast mroute` *{group <groupipaddr> | source <sourceipaddr> [<groupipaddr>] | all}*
Mode	Global Config

15.1.10 show ip mcast

This command displays the system-wide multicast information.

Format	`show ip mcast`
Modes	Privileged EXEC User EXEC
Admin Mode	The administrative status of multicast.
Protocol State	The current state of the multicast protocol. Possible values are Operational or Non-Operational.

Table Max Size	The maximum number of entries allowed in the multicast table.
Number Of Packets For Which Source Not Found	The number of packets for which the source is not found.
Number Of Packets For Which Group Not Found	The number of packets for which the group is not found.
Protocol	The multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.
Entry Count	The number of entries in the multicast table.
Highest Entry Count	The highest entry count in the multicast table.

15.1.11 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Format	**`show ip mcast boundary`** *`{<slot/port>	all}`*
Modes	Privileged EXEC User EXEC
Interface	Valid slot and port number separated by forward slashes.
Group Ip	The group IP address
Mask	The group IP mask

15.1.12 show ip mcast interface

This command displays the multicast information for the specified interface.

Format	**`show ip mcast interface`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC
Interface	Valid slot and port number separated by forward slashes.
TTL	The time-to-live value for this interface.

15.1.13 show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Format `show ip mcast mroute {detail | summary}`

Modes Privileged EXEC
User EXEC

If you use the *detail* parameter, the following fields are displayed:

Source IP Addr The IP address of the multicast data source.

Group IP Addr The IP address of the destination of the multicast packet.

Expiry Time The time of expiry of this entry in seconds.

Up Time The time elapsed since the entry was created in seconds.

RPF Neighbor The IP address of the RPF neighbor.

Flags The flags associated with this entry.

If you use the *summary* parameter, the following fields are displayed:

Source IP Addr The IP address of the multicast data source.

Group IP Addr The IP address of the destination of the multicast packet.

Protocol The multicast routing protocol by which the entry was created.

Incoming Interface The interface on which the packet for the source/group arrives.

Outgoing Interface List The list of outgoing interfaces on which the packet is forwarded.

15.1.14 show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given <*groupipaddr*>.

Format `show ip mcast mroute group <groupipaddr> {detail |summary}`

Modes Privileged EXEC
User EXEC

Source IP Addr The IP address of the multicast data source.

Group IP Addr The IP address of the destination of the multicast packet.

Protocol The multicast routing protocol by which this entry was created.

Incoming Interface The interface on which the packet for this group arrives.

Outgoing Interface List The list of outgoing interfaces on which this packet is forwarded.

15.1.15 show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given *<sourceipaddr>* or *<sourceipaddr> [<groupipaddr>]* pair.

Format **`show ip mcast mroute source`** *`<sourceipaddr> {summary | <groupipaddr>}`*

Modes Privileged EXEC
User EXEC

If the detail parameter is specified the follow fields are displayed:

Source IP Addr The IP address of the multicast data source.

Group IP Addr The IP address of the destination of the multicast packet.

Expiry Time The time of expiry of this entry in seconds.

Up Time The time elapsed since the entry was created in seconds.

RPF Neighbor The IP address of the RPF neighbor.

Flags The flags associated with this entry.

If the summary parameter is specified the follow fields are displayed:

Source IP Addr The IP address of the multicast data source.

Group IP Addr The IP address of the destination of the multicast packet.

Protocol The multicast routing protocol by which this entry was created.

Incoming Interface The interface on which the packet for this source arrives.

Outgoing Interface List The list of outgoing interfaces on which this packet is forwarded.

15.1.16 show ip mcast mroute static

This command displays all the static routes configured in the static mcast table if is specified or displays the static route associated with the particular <*`sourceipaddr`*>.

Format	**`show ip mcast mroute static`** *`[<sourceipaddr>]`*
Modes	Privileged EXEC User EXEC
Source Address	The IP address of the multicast packet source.
Source Mask	The mask applied to the IP address of the multicast packet source.
RPF Address	The IP address to be used as RPF for the given source and mask.
Metric	The metric value corresponding to the source address.
Interface	Valid slot and port number separated by forward slashes.

15.1.17 show mrinfo

This command is used to display the neighbor information of a multicast-capable router from the results buffer pool of the router subsequent to the execution/completion of a **`mrinfo`** *`[ipaddr]`* command.

The results subsequent to the completion of the latest **`mrinfo`** will be available in the buffer pool after a maximum duration of two minutes after the completion of the **`show mrinfo`** command. A subsequent issue **`mrinfo`** overwrites the contents of the buffer pool with fresh results.

Default	none
Format	**`show mrinfo`**
Mode	Privileged EXEC
Router Interface	The IP address of this neighbor
Neighbor	The neighbor associated with the router interface
Metric	The metric value associated with this neighbor
TTL	The TTL threshold associated with this neighbor

Flags Status of the neighbor

15.1.18 show mstat

This command is used to display the results of packet rate and loss information from the results buffer pool of the router, subsequent to the execution/completion of a **`mstat`** *`<source> [group] [receiver]`* command. Within two minutes of the completion of the **`mstat`** command, the results will be available in the buffer pool. The next issuing of **`mstat`** overwrites the buffer pool with fresh results.

Default none

Format show mstat

Mode Privileged EXEC

15.1.19 show mtrace

This command is used to display results of multicast trace path from the results buffer pool of the router, subsequent to the execution/completion of a **`mtrace`** *`<source> [group] [receiver]`* command. The results subsequent to the completion of the **`mtrace`** will be available in the buffer pool within two minutes and thereafter. A subsequent **`mtrace`** command overwrites the results in the buffer pool.

Default none

Format **`show mtrace`**

Modes Privileged EXEC
User EXEC

Hops Away From Destination The ordering of intermediate routers between the source and the destination

Intermediate Router Address The address of the intermediate router at the specified hop distance

Mcast Protocol In Use The multicast routing protocol used for the out interface of the specified intermediate router.

TTL Threshold The Time-To-Live threshold of the out interface on the specified intermediate router.

Time Elapsed Between Hops (msecs)	The time between arrival at one intermediate router to the arrival at the next.

15.2 DVMRP Commands

This section provides a detailed explanation of the Distance Vector Multicast Routing Protocol (DVMRP) commands.

15.2.1 ip dvmrp

This command sets administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Default	disabled
Format	`ip dvmrp`
Mode	Global Config

15.2.1.1 no ip dvmrp

This command sets administrative mode of DVMRP in the router to inactive.

Format	`no ip dvmrp`
Mode	Global Config

15.2.2 ip dvmrp metric

This command configures the metric for an interface. This value is used in the DVMRP messages as the cost to reach this network. This field has a range of 1 to 31.

Default	1
Format	ip dvmrp metric <*`metric`*>
Mode	Interface Config

15.2.2.1 no ip dvmrp metric

This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

Format	no ip dvmrp metric
Mode	Interface Config

15.2.3 ip dvmrp trapflags

This command enables the DVMRP trap mode.

Default	disabled
Format	`ip dvmrp trapflags`
Mode	Global Config

15.2.3.1 no ip dvmrp trapflags

This command disables the DVMRP trap mode.

Format	`no ip dvmrp trapflags`
Mode	Global Config

15.2.4 ip dvmrp

This command sets the administrative mode of DVMRP on an interface to active.

Default	disabled
Format	**`ip dvmrp`**
Mode	Interface Config

15.2.4.1 no ip dvmrp

This command sets the administrative mode of DVMRP on an interface to inactive.

Format	**`no ip dvmrp`**
Mode	Interface Config

15.2.5 show ip dvmrp

This command displays the system-wide information for DVMRP.

Format	**`show ip dvmrp`**
Modes	Privileged EXEC User EXEC
Admin Mode	This field indicates whether DVMRP is enabled or disabled.
Version String	The version of DVMRP being used.
Number of Routes	The number of routes in the DVMRP routing table.

Reachable Routes The number of entries in the routing table with non-infinite metrics.

The following fields are displayed for each interface.

Interface Valid slot and port number separated by forward slashes.

Interface Mode The mode of this interface. Possible values are Enabled and Disabled.

State The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.

15.2.6 show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

Format `show ip dvmrp interface <slot/port>`

Modes Privileged EXEC
User EXEC

Interface Mode This field indicates whether DVMRP is enabled or disabled on the specified interface.

Metric The metric of this interface. This is a configured value.

Local Address The IP Address of the interface.

This Field is displayed only when DVMRP is operational on the interface.

Generation ID The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

The following fields are displayed only if DVMRP is enabled on this interface.

Received Bad Packets The number of invalid packets received.

Received Bad Routes The number of invalid routes received.

Sent Routes The number of routes that have been sent on this interface.

15.2.7 show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

Format	`show ip dvmrp neighbor`
Modes	Privileged EXEC User EXEC
IfIndex	The value of the interface used to reach the neighbor.
Nbr IP Addr	The IP Address of the DVMRP neighbor for which this entry contains information.
State	The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.
Up Time	The time since this neighboring router was learned.
Expiry Time	The time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.
Generation ID	The Generation ID value for the neighbor.
Major Version	The major version of DVMRP protocol of neighbor.
Minor Version	The minor version of DVMRP protocol of neighbor.
Capabilities	The capabilities of neighbor.
Received Routes	The number of routes received from the neighbor.
Rcvd Bad Pkts	The number of invalid packets received from this neighbor.
Rcvd Bad Routes	The number of correct packets received with invalid routes.

15.2.8 show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Format	`show ip dvmrp nexthop`
Modes	Privileged EXEC User EXEC
Source IP	The sources for which this entry specifies a next hop on an outgoing interface.
Source Mask	The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.

Next Hop Interface The interface in slot/port format for the outgoing interface for this next hop.

Type The network is a LEAF or a BRANCH.

15.2.9 show ip dvmrp prune

This command displays the table listing the router's upstream prune information.

Format `show ip dvmrp prune`

Modes Privileged EXEC
User EXEC

Group IP This field identifies the multicast Address that is pruned.

Source IP This field displays the IP Address of the source that has pruned.

Source Mask This field displays the network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.

Expiry Time (secs) This field indicates the expiry time in seconds. This is the time remaining for this prune to age out.

15.2.10 show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Format `show ip dvmrp route`

Modes Privileged EXEC
User EXEC

Source Address This field displays the multicast address of the source group.

Source Mask This field displays the IP Mask for the source group.

Upstream Neighbor This field indicates the IP Address of the neighbor which is the source for the packets for a specified multicast address.

Interface This field displays the interface used to receive the packets sent by the sources.

Metric	This field displays the distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.
Expiry Time (secs)	This field indicates the expiry time in seconds. This is the time remaining for this route to age out.
Up Time (secs)	This field indicates the time when a specified route was learnt, in seconds.

15.3 PIM-DM Commands

This section describes the commands you use to configure Protocol Independent Multicast - Dense Mode (PIM-DM). PIM-DM is a multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. PIM-DM is typically used in LAN applications, while PIM-SM is for WAN applications.

15.3.1 ip pimdm

This command enables the administrative mode of PIM-DM in the router.

Default	disabled
Format	`ip pimdm`
Mode	Global Config

15.3.1.1 no ip pimdm

This command disables the administrative mode of PIM-DM in the router. IGMP must be enabled before PIM-DM can be enabled.

Format	`no ip pimdm`
Mode	Global Config

15.3.2 ip pimdm mode

This command sets administrative mode of PIM-DM on an interface to enabled.

Default	disabled
Format	**ip pimdm mode** *<slot/port>*
Mode	Interface Config

15.3.2.1 no ip pimdm mode

This command sets administrative mode of PIM-DM on an interface to disabled.

Format	`no ip pimdm mode <slot/port>`
Mode	Interface Config

15.3.3 ip pimdm query-interval

This command configures the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

Default	30
Format	`ip pimdm query-interval <seconds>`
Mode	Interface Config

15.3.3.1 no ip pimdm query-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format	`no ip pimdm query-interval`
Mode	Interface Config

15.3.4 show ip pimdm

This command displays the system-wide information for PIM-DM.

Format	`show ip pimdm`
Modes	Privileged EXEC User EXEC
PIM-DM Admin Mode	This field indicates whether PIM-DM is enabled or disabled.
Interface	Valid slot and port number separated by forward slashes.
Interface Mode	This field indicates whether PIM-DM is enabled or disabled on this interface.
State	The current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

15.3.5 show ip pimdm interface

This command displays the interface information for PIM-DM on the specified interface.

Format `show ip pimdm interface <slot/port>`

Modes Privileged EXEC
User EXEC

Interface Mode This field indicates whether PIM-DM is enabled or disabled on the specified interface.

PIM-DM Interface Hello Interval The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

15.3.6 show ip pimdm interface stats

This command displays the statistical information for PIM-DM on the specified interface.

Format `show ip pimdm interface stats {<slot/port> | all}`

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

IP Address The IP Address that represents the PIM-DM interface.

Nbr Count The neighbor count for the PIM-DM interface.

Hello Interval The time interval between two hello messages sent from the router on the given interface.

Designated Router The IP Address of the Designated Router for this interface.

15.3.7 show ip pimdm neighbor

This command displays the neighbor information for PIM-DM on the specified interface.

Format `show ip pimdm neighbor {<slot/port> | all}`

Modes Privileged EXEC
User EXEC

Neighbor Address The IP Address of the neighbor on an interface.

Interface Valid slot and port number separated by forward slashes.

Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.

15.4 PIM-SM Commands

This section describes the commands you use to configure Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-SM is a multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. PIM-DM is typically used in LAN applications, while PIM-SM is for WAN applications.

15.4.1 ip pimsm cbsrpreference

This command is used to configure the CBSR preference for a particular PIM-SM interface. The range of CBSR preference is –1 to 255.

Default	0
Format	**`ip pimsm cbsrpreference`** *<-1-255>*
Mode	Interface Config

15.4.1.1 no ip pimsm cbsrpreference

Use this command to reset the CBSR preference for a particular PIM-SM interface to zero.

Format	no ip pimsm cbsrpreference
Mode	Interface Config

15.4.2 ip pimsm cbsrhashmasklength

This command is used to configure the CBSR hash mask length to be advertised in bootstrap messages for a particular PIM-SM interface. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid range is 0 - 32.

Default	30
Format	**`ip pimsm cbsrhashmasklength`** *<0-32>*
Mode	Interface Config

15.4.2.1 no ip pimsm cbsrhashmasklength

Use this command to reset the CBSR hash mask length for a particular PIM-SM interface to the default.

Format	no ip pimsm `cbsrhashmasklength`
Mode	Interface Config

15.4.3 ip pimsm crppreference

This command is used to configure the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface. The valid values are from (-1 to 255), and the value of -1 is used to indicate that the local interface is not a Candidate RP interface.

The active router interface, with the highest IP Address and crppreference greater than -1, is chosen as the CRP for the router. The default value is 0.

In the CRP advertisements sent to the bootstrap router (BSR), the router interface advertises itself as the CRP for the group range 224.0.0.0 mask 240.0.0.0.

Default	0
Format	`ip pimsm crppreference <-1-255>`
Mode	Interface Config

15.4.3.1 no ip pimsm crppreference

This command is used to reset the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface to the default value.

Format	no ip pimsm `crppreference`
Mode	Interface Config

15.4.4 ip pimsm message-interval

This command is used to configure the global join/prune interval for PIM-SM router. The join/prune interval is specified in seconds. This parameter can be configured to a value from 10 to 3600.

Default	60
Format	`ip pimsm message-interval <10-3600>`
Mode	Global Config

15.4.4.1 no ip pimsm message-interval

This command is used to reset the global join/prune interval for PIM-SM router to the default value.

Format	`no ip pimsm message-interval`
Mode	Global Config

15.4.5 ip pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to enabled. IGMP must be enabled before PIM-SM can be enabled.

Default	disabled
Format	`ip pimsm`
Mode	Global Config

15.4.5.1 no ip pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to the default value. IGMP must be enabled before PIM-SM can be enabled.

Format	`no ip pimsm`
Mode	Global Config

15.4.6 ip pimsm mode

This command sets administrative mode of PIM-SM multicast routing on a routing interface to enabled.

Default	disabled
Format	`ip pimsm mode`
Mode	Interface Config

15.4.6.1 no ip pimsm mode

This command sets administrative mode of PIM-SM multicast routing on a routing interface to the default value.

Format	`no ip pimsm mode`
Mode	Interface Config

15.4.7 ip pimsm query-interval

This command configures the transmission frequency of hello messages in seconds between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

Default	30
Format	**`ip pimsm query-interval`** *`<10-3600>`*
Mode	Interface Config

15.4.7.1 no ip pimsm query-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format	**`no ip pimsm query-interval`**
Mode	Interface Config

15.4.8 ip pimsm spt-threshold

This command is used to configure the Threshold rate for the RP router to switch to the shortest path. The rate is specified in Kilobytes per second. The possible values are 0 to 2000.

Default	50
Format	**`ip pimsm spt-threshold`** *`<0-2000>`*
Mode	Global Config

15.4.8.1 no ip pimsm spt-threshold

This command is used to reset the Threshold rate for the RP router to switch to the shortest path to the default value.

Format	**`no ip pimsm spt-threshold`**
Mode	Global Config

15.4.9 ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Default	disabled
Format	`ip pim-trapflags`
Mode	Global Config

15.4.9.1 no ip pim-trapflags

This command sets the PIM trap mode to the default.

Format	`no ip pim-trapflags`
Mode	Global Config

15.4.10 ip pimsm staticrp

This command is used to create RP IP address for the PIM-SM router. The parameter <*ipaddress*> is the IP address of the RP. The parameter <*groupaddress*> is the group address supported by the RP. The parameter <*groupmask*> is the group mask for the group address.

Default	disabled
Format	**ip pimsm staticrp** <*ipaddress*> <*groupaddress*> <*groupmask*>
Mode	Global Config

15.4.10.1 no ip pimsm staticrp

This command is used to delete RP IP address for the PIM-SM router. The parameter <*ipaddress*> is the IP address of the RP. The parameter <*groupaddress*> is the group address supported by the RP. The parameter <*groupmask*> is the group mask for the group address.

Format	**no ip pimsm staticrp** <*ipaddress*> <*groupaddress*> <*groupmask*>
Mode	Global Config

15.4.11 show ip pimsm rphash

This command displays the RP router that will be selected from the set of active RP routers. The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.

Format	**show ip pimsm rphash** <*groupaddress*>
Modes	Privileged EXEC User EXEC
RP IP Address	The IP address of the RP.
Group Mask	The group mask for the group address.

15.4.12 show ip pimsm staticrp

This command displays the static RP information for the PIM-SM router.

Format `show ip pimsm staticrp`

Modes Privileged EXEC
User EXEC

RP IP Address The IP address of the RP.

Group Address The group address supported by the RP.

Group Mask The group mask for the group address.

15.4.13 show ip pimsm

This command displays the system-wide information for PIM-SM.

Format `show ip pimsm`

Modes Privileged EXEC
User EXEC

PIM-SM Admin Mode This field indicates whether PIM-SM is enabled or disabled.

Join/Prune Interval (secs) The interval at which periodic PIM-SM Join/Prune messages are to be sent.

Data Threshold Rate (K bits/sec) The data threshold rate for the PIM-SM router.

Register Threshold Rate (K bits/sec) The threshold rate for the RP router to switch to the shortest path.

Interface Valid slot and port number separated by forward slashes.

Interface Mode This field indicates whether PIM-SM is enabled or disabled on the interface.

Protocol State The current state of the PIM-SM protocol on the interface. Possible values are Operational or Non-Operational.

15.4.14 show ip pimsm candrptable

This command displays the IP multicast groups for which the local router is to advertise itself as a Candidate-RP when the value of hold time is non-zero.

Format `show ip pimsm candrptable`

Modes Privileged EXEC
User EXEC

Group Address The IP multicast group address.

Group Mask The multicast group address subnet mask.

Address The unicast address of the interface that will be advertised as a Candidate-RP.

15.4.15 show ip pimsm componenttable

This command displays the table containing objects specific to a PIM domain. One row exists for each domain to which the router is connected.

Format `show ip pimsm componenttable`

Modes Privileged EXEC
User EXEC

Component Index A number which uniquely identifies the component.

Component BSR Address The IP address of the bootstrap router (BSR) for the local PIM region.

Component BSR Expiry Time The minimum time remaining before the BSR in the local domain will be declared down.

Component CRP Hold Time The hold time of the component when it is a candidate.

15.4.16 show ip pimsm interface

This command displays the interface information for PIM-SM on the specified interface.

Format `show ip pimsm interface <slot/port>`

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

IP Address The IP address of the specified interface.

Subnet Mask The Subnet Mask for the IP address of the PIM interface.

Mode This field indicates whether PIM-SM is enabled or disabled on the specified interface. By default it is disabled.

Hello Interval The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

CBSR Preference The preference value for the local interface as a candidate bootstrap router.

CRP Preference The preference value as a candidate rendezvous point on this interface.

CBSR Hash Mask Length The hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. The value is used in the hash algorithm for selecting the RP for a particular group.

15.4.17 show ip pimsm interface stats

This command displays the statistical information for PIM-SM on the specified interface.

Format **`show ip pimsm interface stats`** *`{<slot/port> | all}`*

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

IP Address The IP Address that represents the PIM-SM interface.

Subnet Mask The Subnet Mask of this PIM-SM interface.

Designated Router The IP Address of the Designated Router for this interface.

Neighbor Count The number of neighbors on the PIM-SM interface.

15.4.18 show ip pimsm neighbor

This command displays the neighbor information for PIM-SM on the specified interface.

Format **`show ip pimsm neighbor`** *`{<slot/port> | all}`*

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

IP Address The IP Address of the neighbor on an interface.

Up Time The time since this neighbor has become active on this interface.

Expiry Time The expiry time of the neighbor on this interface.

15.4.19 show ip pimsm rp

This command displays the PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups or for the specific <*groupaddress*> <*groupmask*> provided in the command. The information in the table is displayed for each IP multicast group.

Format `show ip pimsm rp {<groupaddress> <groupmask> | candidate | all}`

Modes Privileged EXEC
User EXEC

Group Address The IP multicast group address.

Group Mask The multicast group address subnet mask.

Address The IP address of the Candidate-RP.

Hold Time The hold time of a Candidate-RP.

Expiry Time The minimum time remaining before the Candidate-RP is declared down.

Component A number which uniquely identifies the component. Each protocol instance connected to a separate domain should have a different index value.

15.4.20 show ip pimsm rphash

This command displays the RP router that will be selected from the set of active RP routers. The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.

Format `show ip pimsm rphash <groupaddress>`

Modes Privileged EXEC
User EXEC

RP IP Address The IP address of the RP.

Group Mask The group mask for the group address.

15.5 Internet Group Message Protocol (IGMP) Commands

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

15.5.1 ip igmp

This command sets the administrative mode of IGMP in the system to active.

Default	disabled
Format	**`ip igmp`**
Mode	Global Config

15.5.1.1 no ip igmp

This command sets the administrative mode of IGMP in the system to inactive.

Format	**`no ip igmp`**
Mode	Global Config

15.5.2 ip igmp version

This command configures the version of IGMP for an interface. The value for <version> is either 1, 2 or 3.

Default	3
Format	**`ip igmp version <`***`version`***`>`**
Mode	Interface Config

15.5.2.1 no ip igmp version

This command resets the version of IGMP to the default value.

Format	**`no ip igmp version`**
Mode	Interface Config

15.5.3 ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface. The range for <*`count`*> is 1 to 20.

Format	**`ip igmp last-member-query-count`** <*`count`*>
Mode	Interface Config

15.5.3.1 no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

Format	**`no ip igmp last-member-query-count`**
Mode	Interface Config

15.5.4 ip igmp last-member-query-interval

This command configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages. The range for <*seconds*> is 0 to 255 tenths of a second.

Default	10 tenths of a second (1 second)
Format	**`ip igmp last-member-query-interval <`*`seconds`*`>`**
Mode	Interface Config

15.5.4.1 no ip igmp last-member-query-interval

This command resets the Maximum Response Time to the default value.

Format	**`no ip igmp last-member-query-interval`**
Mode	Interface Config

15.5.5 ip igmp query-interval

This command configures the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for <*queryinterval*> is 1 to 3600 seconds.

Default	125 seconds
Format	**`ip igmp query-interval <`*`seconds`*`>`**
Mode	Interface Config

15.5.5.1 no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format	**`no ip igmp query-interval`**
Mode	Interface Config

15.5.6 ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface.The time interval is specified in tenths of a second. The range for <*maxresptime*> is 0 to 255 tenths of a second.

Default	100
Format	**`ip igmp query-max-response-time <seconds>`**
Mode	Interface Config

15.5.6.1 no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format	**`no ip igmp query-max-response-time`**
Mode	Interface Config

15.5.7 ip igmp robustness

This command configures the robustness that allows tuning of the interface. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface. The range for <*robustness*> is 1 to 255.

Default	2
Format	**`ip igmp robustness <robustness>`**
Mode	Interface Config

15.5.7.1 no ip igmp robustness

This command sets the robustness value to default.

Format	**`no ip igmp robustness`**
Mode	Interface Config

15.5.8 ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface. The range for <*count*> is 1 to 20.

Default	2
Format	**`ip igmp startup-query-count <`*`count`*`>`**
Mode	Interface Config

15.5.8.1 no ip igmp startup-query-count

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format	**`no ip igmp startup-query-count`**
Mode	Interface Config

15.5.9 ip igmp startup-query-interval

This command sets the interval between General Queries sent on startup on the interface. The time interval value is in seconds. The range for <*interval*> is 1 to 300 seconds.

Default	31
Format	**`ip igmp startup-query-interval <`*`interval`*`>`**
Mode	Interface Config

15.5.9.1 no ip igmp startup-query-interval

This command resets the interval between General Queries sent on startup on the interface to the default value.

Format	**`no ip igmp startup-query-interval`**
Mode	Interface Config

15.5.10 show ip igmp

This command displays the system-wide IGMP information.

Format	**`show ip igmp`**
Modes	Privileged EXEC User EXEC

IGMP Admin Mode This field displays the administrative status of IGMP. This is a configured value.

Interface Valid slot and port number separated by forward slashes.

Interface Mode This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.

Protocol State This field indicates the current state of IGMP on this interface. Possible values are Operational or Non-Operational.

15.5.11 show ip igmp groups

This command displays the registered multicast groups on the interface. If *`[detail]`* is specified this command displays the registered multicast groups on the interface in detail.

Format **`show ip igmp groups <`*`slot/port`*`>`** *`[detail]`*

Mode Privileged EXEC

If you do not use the **`detail`** keyword, the following fields appear:

IP Address This displays the IP address of the interface participating in the multicast group.

Subnet Mask This displays the subnet mask of the interface participating in the multicast group.

Interface Mode This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled:

Querier Status This displays whether the interface has IGMP in Querier mode or Non-Querier mode.

Groups This displays the list of multicast groups that are registered on this interface.

If you use the **`detail`** keyword, the following fields appear:

Multicast IP Address This displays the IP Address of the registered multicast group on this interface.

Last Reporter This displays the IP Address of the source of the last membership report received for the specified multicast group address on this interface.

Up Time This displays the time elapsed since the entry was created for the specified multicast group address on this interface.

Expiry Time This displays the amount of time remaining to remove this entry before it is aged out.

Version1 Host Timer This displays the time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or “-----” if there is no Version 1 host present.

Version2 Host Timer This displays the time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or “-----” if there is no Version 2 host present.

Group Compatibility Mode The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

15.5.12 show ip igmp interface

This command displays the IGMP information for the interface.

Format `show ip igmp interface <slot/port>`

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

IGMP Admin Mode The administrative status of IGMP.

Interface Mode This field indicates whether IGMP is enabled or disabled on the interface.

IGMP Version The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.

Query Interval The frequency at which IGMP Host-Query packets are transmitted on this interface.

Query Max Response Time The maximum query response time advertised in IGMPv2 queries on this interface.

Robustness The tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface.

Startup Query Interval The interval between General Queries sent by a Querier on startup.

Startup Query Count The number of Queries sent out on startup, separated by the Startup Query Interval.

Last Member Query Interval The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.

Last Member Query Count The number of Group-Specific Queries sent before the router assumes that there are no local members.

15.5.13 show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

Format `show ip igmp interface membership` *<multiipaddr> [detail]*

Mode Privileged EXEC

Interface Valid unit, slot and port number separated by forward slashes.

Interface IP The IP address of the interface participating in the multicast group.

State The interface that has IGMP in Querier mode or Non-Querier mode.

Group Compatibility Mode The group compatibility mode (v1, v2 or v3) for the specified group on this interface.

Source Filter Mode The source filter mode (Include/Exclude) for the specified group on this interface. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.

If you use the **`detail`** keyword, the following fields appear:

Interface Valid unit, slot and port number separated by forward slashes.

Group Compatibility Mode The group compatibility mode (v1, v2 or v3) for the specified group on this interface.

Source Filter Mode The source filter mode (Include/Exclude) for the specified group on this interface. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.

Source Hosts The list of unicast source IP Addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP Address. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.

Expiry Time The amount of time remaining to remove this entry before it is aged out. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.

15.5.14 show ip igmp interface stats

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

Format **`show ip igmp interface stats`** *`<slot/port>`*

Modes Privileged EXEC
User EXEC

Querier Status The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.

Querier IP Address The IP Address of the IGMP Querier on the IP subnet to which this interface is attached.

Querier Up Time The time since the interface Querier was last changed.

Querier Expiry Time The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.

Wrong Version Queries The number of queries received whose IGMP version does not match the IGMP version of the interface.

Number of Joins The number of times a group membership has been added on this interface.

Number of Groups The current number of membership entries for this interface

Chapter 16
IGMP Snooping Commands

This section describes the Internet Group Management Protocol (IGMP) snooping commands available in the 7300 Series Managed Switch CLI.

The 7300 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 16.1 “IGMP Snooping Configuration Commands” on page 16-1
- Section 16.2 “IGMP Snooping Show Commands” on page 16-6

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.

16.1 IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping.

16.1.1 set igmp

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	**`set igmp`** *<vlanId>*
Modes	Global Config Interface Config VLAN Mode

16.1.1.1 no set igmp

This command disables IGMP Snooping on the system.

Format	**`no set igmp`** *<vlanId>*
Modes	Global Config Interface Config VLAN Mode

16.1.2 set igmp 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	**`set igmp interfacemode`**
Mode	Global Config

16.1.2.1 no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

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

16.1.3 set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default	disabled
Format	**`set igmp fast-leave`** <*`vlanId`*>
Modes	Interface Config VLAN Mode

16.1.3.1 no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format	**`no set igmp fast-leave`** <*`vlanId`*>
Modes	Interface Config VLAN Mode

16.1.4 set igmp 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	**`set igmp groupmembership-interval`** *`<vlanId> <2-3600>`*
Modes	Interface Config Global Config VLAN Mode

16.1.4.1 no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format	**`no set igmp groupmembership-interval`**
Modes	Interface Config Global Config VLAN Mode

16.1.5 set igmp 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	**`set igmp maxresponse`** *`<1-3599>`*
Modes	Global Config Interface Config VLAN Mode

16.1.5.1 no set igmp maxresponse

This command sets the IGMP Maximum Response time (on the interface or VLAN) to the default value.

Format	**`no set igmp maxresponse`**
Modes	Global Config Interface Config VLAN Mode

16.1.6 set igmp mcrtexpiretime

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	**`set igmp mcrtexpiretime`** *`<vlanId> <0-3600>`*
Modes	Global Config Interface Config

16.1.6.1 no set igmp 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	**`no set igmp mcrtexpiretime`** *`<vlanId>`*
Modes	Global Config Interface Config

16.1.7 set igmp mrouter

This command configures the VLAN ID (<*vlanId*>) that has the multicast router mode enabled.

Format	**`set igmp mrouter <`***`vlanId`***`>`**
Mode	Interface Config

16.1.7.1 no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (<*vlanId*>).

Format **no set igmp mrouter <***vlanId***>**

Mode Interface Config

16.1.8 set igmp mrouter interface

This command configures the interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default disabled

Format **set igmp mrouter interface**

Mode Interface Config

16.1.8.1 no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format **no set igmp mrouter interface**

Mode Interface Config

16.2 IGMP Snooping Show Commands

This section describes the commands you use to view IGMP snooping status and information.

16.2.1 show igmpsnooping

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

Format **show igmpsnooping** *[<slot/port> | <vlanId>]*

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.

16.2.2 show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format	**`show igmpsnooping mrouter interface`** <*slot/port*>
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.

16.2.3 show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format	**`show igmpsnooping mrouter vlan`** <*slot/port*>
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.

16.2.4 show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format `show mac-address-table igmpsnooping`

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:).

Chapter 17
Power Over Ethernet Commands

This chapter provides information on the Power Over Ethernet Commands available in the FSM7326P Switch software.

The IEEE 802.3 Ethernet standard body has a task force called the 802.3af, which specifies the method to deliver power over the LAN. 802.3af, also known as Power over Ethernet, defines a way to build Ethernet power-sourcing equipment and powered terminals. The specification involves delivering 48 volts of AC power over unshielded twisted-pair (UTP/FTP) wiring.

Power over Ethernet (PoE) is a technology that can integrate data, voice and power on a LAN. PoE supplies reliable, uninterrupted power to Internet Protocol (IP) telephones, wireless LAN access points, and other Ethernet devices that use existing Cat5 cables.

Power over Ethernet, when used in conjunction with an uninterrupted power supply (UPS), ensures continuous operation during power failures. PoE saves time and eliminates the cost of installing separate power cabling and AC outlets.

The power delivered over the Ethernet cabling is automatically activated when a compatible device is identified. The power is injected by either new generation Ethernet switches (end-Span) or by a dedicated patch-panel like device, residing between an ordinary Ethernet switch or hub and the terminals (mid-span). Mid-span devices are available with 1,6,12 or 24 ports. PoE technology does not degrade the network data communication performance or decrease the network reach.

Wireless Access points often need to be located in high places, like the ceiling, where the necessary power lines and data access are not readily available. An integrated power-data network solves that problem and allows greater flexibility and range in wireless networking.

In order for the network to carry power, you need to add power sourcing equipment (PSE). This is the source of power and the means to integrate that power onto the network. The PSE also provides a detection method for determining whether the Ethernet device on the other end of the cable, the Powered Device (PD), is 802.3af compliant or not.

Most vendors today implement the PSE technology outside of the existing switch, a technique called a midspan solution. AVAYA and Cisco also implement this technology inside the switch, called an end-span solution.

Attached to the PSE is the UPS. A UPS is connected to each device that requires alternative power. With Power over Ethernet, this function is centralized in a UPS connected to the PSE. Note that this may require further changes in the environmental conditions of the room needing to support this UPS with all of its electrical and cooling requirements.

The current delivered to each node is limited to 350 milliamps. The total amount of continuous power that can be delivered to each node, taking into account some power loss over the cable run, is 12.95 watts. IP phones and wireless LAN access points typically consume 3.5 to 10 watts. Power is carried on two wire pairs, to comply with safety standards and existing cable limitations.

Management may also be added to monitor and control the PSE. This management function may be integrated into a standard network management platform using the simple network management protocol (SNMP) or through a custom platform. Beyond the basic control of the PSE, the management stations provides additional power management functions, like power quality of service (QoS) where key users are given higher priority to power in the event of a outage.

Voice-over IP (VoIP), is the transmission of telephone calls over a data network like one of the many networks that make up the Internet.

Other NETGEAR products that work with 7300 Series L3 Switch:

- WG302
- WG602
- WAG302

17.1 Power Over Ethernet (POE) Commands

This section shows the additional CLI commands required to provide the management interface to the Power-over-Ethernet (PoE) function. The commands only applies to FSM7326P model.

⇨	**Note:** Note: For the FSM7326P, only ports 0.1-0.24 are eligible to participate in the PoE function.

17.1.1 poe

This command enables or disables the Power over Ethernet function on the specified port(s).

Default	enable
Format	`poe`
Mode	Global Config

17.1.2 poe priority

This command sets the priority level for the delivery of power to an attached device. The switch may not be able to supply power to all connected devices, so the port priority is used to determine which ports will supply power if adequate power capacity is not available for all enabled ports. For ports that have the same priority level, the lower numbered port will have higher priority.

Default	low
Format	`poe priority <high/medium/low>`
Mode	Global Config

17.1.3 poe limit

This command sets the power limit (in watts) for the port. The port will not supply more power than the value specified as the limit.

For the FSM7326P, the valid range is 3 - 18.

Default	18
Format	`poe limit`
Mode	Global Config

17.1.4 poe usagethreshold

This command sets the power threshold level at which a trap will be generated. If the total power consumed is greater than or equal to the specified percentage of the total power available, a trap will be sent. The switch will continue to provide power even if the threshold is exceeded. The threshold value is for providing a warning. It does not interrupt the power. Valid values are 0 - 100.

Default	80
Format	**`poe usagethreshold <0-100>`**
Mode	Global Config

17.1.5 show poe port info

This command displays a summary for the ports that support the PoE function.

Format	**`show poe port <slot/port, All>`**
Mode	Privilege

The following fields are displayed for each port. If a port does not have link, or is not enabled for PoE, the following fields display a value of “N/A”.

17.1.5.1 Class

The Class field reports the class of the powered device according to IEEE802.3af definition.

Table 17-1. Class of the Powered Device

Class	Usage	Max Power
0	Default	0.44-12.95
1	Optional	0.44-3.84
2	Optional	3.84-6.49
3	Optional	6.49-12.95
4	Not Allowed	Reserved

17.1.5.2 Output

The Output field reports the power supplied to the powered device (in watts).

17.1.5.3 Limit

The LIMIT field is the preset limit defined by the “config poe port limit” command. This value is stated in watts.

17.1.5.4 Status

The Status field reports the state of power supplied to the associated port. Possible values are:

- **Disabled**—the POE function is disabled on this port
- **Searching**—the port is detecting POE device
- **Delivering Power**—the port is providing power to POE device
- **Fault**—the POE device is not IEEE compliance, no power is provided
- **Test**—the port is in testing state
- **Other Fault**—the port has experience problems other than compliance issue

When a port begins to deliver power, there will be a trap indicating so. When a port stops delivering power, there will be a trap indicating so.

17.1.6 show poe

This command displays the total power available and the total power consumed in the system.

Format	`show poe`
Mode	Privilege

Chapter 18
System Maintenance Commands

This section describes the system maintenance commands available in the 7300 Series Managed Switch CLI.

The System Maintenance Commands section includes the following subsections:

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.

18.1 System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

18.1.1 show arp switch

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

Format **`show arp switch`**

Mode Privileged EXEC

MAC Address A unicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB

IP Address The IP address assigned to each interface.

Interface Valid slot and port number separated by forward slashes.

18.1.2 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 **`show eventlog`** *`[unit]`*

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.

18.1.3 show hardware

This command displays inventory information for the switch.

Format `show hardware`

Mode Privileged EXEC

Switch Description Text used to identify the product name of this switch.

Machine Type Specifies the machine model as defined by the Vital Product Data.

Machine Model Specifies the machine model as defined by the Vital Product Data.

Serial Number The unique box serial number for this switch.

FRU Number The field replaceable unit number.

Part Number Manufacturing part number.

Maintenance Level Indicates hardware changes that are significant to software.

Manufacturer Manufacturer descriptor field.

Burned in MAC Address Universally assigned network address.

Software Version The release.version.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.

18.1.4 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 18.1.5 “show interface ethernet” on page 18-6.

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.

18.1.5 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).

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

Packets Transmitted Successfully

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

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

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

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

Transmit Errors

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

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

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

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

Transmit Discards

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

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

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

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

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

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

Protocol Statistics

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Dot1x Statistics

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

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

Time Since Counters Last Cleared

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

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 subnetwork-unicast address, including those that were discarded or not sent.

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

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

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

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

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

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

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

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

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

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

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

18.1.6 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 `show logging`

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.

18.1.7 show mac-addr-table

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

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

Mode Privileged EXEC

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

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.

18.1.8 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.

Format **show running-config** *[all | <scriptname>]*

Mode Privileged EXEC

18.1.9 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.

18.2 System Utility Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

18.2.1 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`** *`<ipaddr> [port]`*
Mode	Privileged EXEC

18.2.2 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

18.2.3 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`** *`{<slot/port>	all}`*
Mode	Privileged EXEC

18.2.4 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

18.2.5 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

18.2.6 enable passwd

This command prompts you to change the Privileged EXEC password.

Format	`enable passwd`
Mode	User EXEC

18.2.7 clear port-channel

This command clears all port-channels (LAGs).

Format	`clear port-channel`
Mode	Privileged EXEC

18.2.8 clear traplog

This command clears the trap log.

Format	`clear traplog`
Mode	Privileged EXEC

18.2.9 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format	`clear vlan`
Mode	Privileged EXEC

18.2.10 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 18-1. 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 18-1. Copy Parameters

Source	Destination	Description
nvram:clibanner	*<url>*	Copies the CLI banner to a server.
nvram:errorlog	*<url>*	Copies the error log file to a server.
nvram:log	*<url>*	Copies the log file to a server.
nvram:script *<scriptname>*	*<url>*	Copies a specified configuration script file to a server.
nvram:startup-config	*<url>*	Copies the startup configuration to a server.
nvram:traplog	*<url>*	Copies the trap log file to a server.
system:running-config	**nvram:startup-config**	Saves the running configuration to nvram.
<url>	**nvram:clibanner**	Downloads the CLI banner to the system.
<url>	**nvram:script** *<destfilename>*	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.
<url>	**nvram:sshkeydsa**	Downloads an SSH key file. For more information, see Section 3.4 “Secure Shell (SSH) Command” on page 3-13.

Table 18-1. Copy Parameters (continued)

Source	Destination	Description
<url>	**`nvram:sshkeyrsa1`**	Downloads an SSH key file.
<url>	**`nvram:sshkeyrsa1`**	Downloads an SSH key file.
<url>	**`nvram:sslpemroot`**	Downloads an HTTP secure-server certificate. For more information, see Section 3.5 "Hypertext Transfer Protocol (HTTP) Commands" on page 3-15.
<url>	**`nvram:sslpemserver`**	Downloads an HTTP secure-server certificate.
<url>	**`nvram:sslpemdhweak`**	Downloads an HTTP secure-server certificate.
<url>	**`nvram:sslpemdhstrong`**	Downloads an HTTP secure-server certificate.
<url>	**`nvram:startup-config`**	Downloads the startup configuration file to the system.
<url>	**`system:image`**	Downloads a code image to the system.

18.2.11 logout

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

Note: Save configuration changes before logging out.

Format	**`logout`**
Mode	Privileged EXEC

18.2.12 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	`ping <ipaddr>`
Modes	Privileged EXEC, User EXEC

18.2.13 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	`reload`
Mode	Privileged EXEC

18.3 Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

18.3.1 logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

Default	disabled; critical
Format	`logging buffered`
Mode	Global Config

18.3.1.1 no logging buffered

This command disables logging to in-memory log.

Format	`no logging buffered`
Mode	Global Config

18.3.2 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	`logging buffered wrap`
Mode	Privileged EXEC

18.3.2.1 no logging wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format	**`no logging buffered wrap`**
Mode	Privileged EXEC

18.3.3 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`** *`[severitylevel]`*
Mode	Global Config

18.3.3.1 no logging console

This command disables logging to the console.

Format	**`no logging console`**
Mode	Global Config

18.3.4 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`** *`<ipaddr> [<port>][<severitylevel>]`*
Mode	Global Config

18.3.5 logging host remove

This command disables logging to host. See Section 18.3.10 “show logging hosts” on page 18-25 for a list of host indexes.

Format	**`logging host remove`** *`<hostindex>`*
Mode	Global Config

18.3.6 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	**`logging port`** *`<portid>`*
Mode	Global Config

18.3.6.1 no logging port

This command resets the local logging port to the default.

Format	**`no logging port`**
Mode	Global Config

18.3.7 logging syslog

This command enables syslog logging.

Default	disabled; local0
Format	**`logging syslog`**
Mode	Global Config

18.3.7.1 no logging syslog

This command disables syslog logging.

Format	**`no logging syslog`**
Mode	Global Config

18.3.8 show logging

This command displays logging.

Format `show logging`

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.

18.3.9 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.

18.3.10 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.

18.3.11 show logging traplogs

This command displays SNMP trap events and statistics.

Format `show logging traplogs`

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.

18.4 CLI Command Logging Command

This section describes the commands you use to configure CLI Command Logging.

18.4.1 logging cli-command

This command enables the CLI command logging feature, which enables the 7300 Series Managed Switch software to log all CLI commands issued on the system.

Default	enabled
Format	`logging cli-command`
Mode	Global Config

18.4.1.1 no logging cli-command

This command disables the CLI command Logging feature.

Format	`no logging cli-command`
Mode	Global Config

18.5 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 18.1.8 “show running-config” on page 18-16) to capture the running configuration into a script. Use the **`copy`** command (see Section 18.2.10 “copy” on page 18-19) 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
```

18.5.1 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`** <*`scriptname`*>
Mode	Global Config

18.5.2 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`** *`{<scriptname>	all}`*
Mode	Global Config

18.5.3 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.

18.5.4 script show

This command displays the contents of a script file, which is named <*scriptname*>.

Format	**`script show`** *`<scriptname>`*
Mode	Global Config
Output Format	**`line`** *`<number>`*`:` *`<line contents>`*

18.5.5 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	**`script validate`** *`<scriptname>`*
Mode	Global Config