

# NetApp® CN1601 Network Switch

## **CLI Command Reference**

NetApp, Inc.  
495 East Java Drive  
Sunnyvale, CA 94089 U.S.A.  
Telephone: +1 (408) 822-6000  
Fax: +1 (408) 822-4501  
Support telephone: +1 (888) 4-NETAPP  
Documentation comments: [doccomments@netapp.com](mailto:doccomments@netapp.com)  
Information Web: [www.netapp.com](http://www.netapp.com)

Part number: 215-06283\_B0  
July 2013

# Copyright and trademark information

---

## Copyright information

Copyright © 1994-2013 NetApp, Inc. All rights reserved. Printed in the U.S.A.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, FAServer, FilerView, FlexCache, FlexClone, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), ONTAPI, OpenKey, RAID-DP, ReplicatorX, SANscreen, SecureAdmin, SecureShare, Select, Shadow Tape, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, and Web Filer are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

Broadcom®, the pulse logo, Connecting everything®, the Connecting everything logo, and FASTPATH® are among the trademarks of Broadcom Corporation and/or its affiliates in the United States, certain other countries and/or the EU.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks. NetApp, Inc. NetCache is certified RealSystem compatible.



# Table of Contents

---

<b>Chapter 1</b>	<b>About This Document . . . . .</b>	<b>5</b>
<b>Chapter 2</b>	<b>Using the Command-Line Interface . . . . .</b>	<b>7</b>
	Command Syntax . . . . .	8
	Command Conventions . . . . .	9
	Common Parameter Values . . . . .	10
	Slot/Port Naming Convention . . . . .	12
	Using the no Form of a Command . . . . .	14
	CN1601 Software Modules . . . . .	15
	Command Modes . . . . .	16
	Command Completion and Abbreviation . . . . .	22
	CLI Error Messages . . . . .	23
	CLI Line-Editing Conventions . . . . .	24
	Using CLI Help . . . . .	26
	Accessing the CLI . . . . .	28
<b>Chapter 3</b>	<b>Management Commands . . . . .</b>	<b>29</b>
	Access Commands . . . . .	30
	Configuration Scripting Commands . . . . .	32
	Console Port Access Commands . . . . .	35
	Management Security Commands . . . . .	38
	Network Interface Commands . . . . .	39
	Pre-login Banner, System Prompt, and Host Name Commands . . . . .	45
	RADIUS Commands . . . . .	47
	Secure Shell Commands . . . . .	64
	SNMP Commands . . . . .	67
	TACACS+ Commands . . . . .	79
	Telnet Commands . . . . .	83

User Account Commands. . . . .	86
--------------------------------	----

## Chapter 4

<b>Utility Commands . . . . .</b>	<b>.113</b>
AutoInstall Commands . . . . .	.114
Cable Test Command. . . . .	.118
DHCP Server Commands. . . . .	.120
DNS Client Commands. . . . .	.134
Dual Image Commands. . . . .	.140
Email Alerting and Mail Server Commands . . . . .	.142
IP Address Conflict Commands . . . . .	.150
Logging Commands . . . . .	.151
Serviceability Packet Tracing Commands . . . . .	.157
Simple Network Time Protocol Commands . . . . .	.167
System Information and Statistics Commands . . . . .	.174
System Utility and Clear Commands. . . . .	.198

## Chapter 5

<b>Switching Commands . . . . .</b>	<b>.213</b>
Denial of Service Commands. . . . .	.215
802.1X Supplicant Commands . . . . .	.226
GARP Commands . . . . .	.231
GMRP Commands . . . . .	.234
GVRP Commands . . . . .	.238
IGMP Snooping Configuration Commands . . . . .	.241
IGMP Snooping Querier Commands. . . . .	.251
ISDP Commands . . . . .	.256
LLDP (802.1AB) Commands . . . . .	.262
LLDP-MED Commands . . . . .	.273
MAC Database Commands. . . . .	.281
Port-Based Network Access Control Commands . . . . .	.284
Port Channel/LAG (802.3ad) Commands . . . . .	.304

	Port Configuration Commands . . . . .	.324
	Port Mirroring Commands . . . . .	.330
	Port Security Commands . . . . .	.333
	Protected Ports Commands . . . . .	.337
	Provisioning (IEEE 802.1p) Commands . . . . .	.340
	Spanning Tree Protocol Commands . . . . .	.341
	Static MAC Filtering Commands. . . . .	.361
	Storm-Control Commands . . . . .	.366
	VLAN Commands . . . . .	.379
	Voice VLAN Commands. . . . .	.391
<b>Chapter 6</b>	<b>IPv6 Management Commands.</b> . . . .	.395
	IPv6 Management Commands . . . . .	.396
<b>Chapter 7</b>	<b>Quality of Service Commands</b> . . . . .	.403
	Auto-Voice over IP Commands . . . . .	.404
	IP Access Control List Commands . . . . .	.406
	MAC Access Control List Commands . . . . .	.416
	Time Range Commands for Time-Based ACLs . . . . .	.422
	<b>Command Index.</b> . . . .	.427





## Introduction

This document describes command-line interface (CLI) commands you use to view and configure the CN1601 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.

---

### Note

This document contains standalone commands. Stacking commands are not supported on the CN1601 switch.

---

---

### Note

Some commands in this document may not be available with your version of the FASTPATH software. Enter a question mark (?) after typing one or more characters of a word to list the available commands or parameters that begin with the letters. See “[Using CLI Help](#)” on page 26 for more information.

---

## Audience

This document is for system administrators who configure and operate systems using FASTPATH® software. It provides an understanding of the configuration options of the FASTPATH software.

Software engineers who integrate FASTPATH software into their hardware platform can also benefit from a description of the configuration options.

This document assumes that you have an understanding of the FASTPATH software base and have read the appropriate specification for the relevant networking device platform. It also assumes that you have a basic knowledge of Ethernet and networking concepts.

Refer to the release notes for the FASTPATH application-level code. The release notes detail the platform-specific functionality of the Switching, SNMP, Configuration, Management, and other packages. The suite of features the FASTPATH packages support is not available on all the platforms to which FASTPATH software has been ported.

## About FASTPATH Software

FASTPATH 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.

## Scope

FASTPATH software encompasses both hardware and software support. The 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.

## Product Concept

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

The exact functionality provided by each networking device on which the FASTPATH software base runs varies depending upon the platform and requirements of the FASTPATH software.

FASTPATH software includes a set of comprehensive management functions for managing both FASTPATH software and the network. You can manage the FASTPATH software by using one of the following two methods:

- ◆ Command-Line Interface (CLI)
- ◆ Simple Network Management Protocol (SNMP)

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

## About this chapter

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.

## Topics in this chapter

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

- ◆ [“Command Syntax”](#) on page 8
- ◆ [“Command Conventions”](#) on page 9
- ◆ [“Common Parameter Values”](#) on page 10
- ◆ [“Slot/Port Naming Convention”](#) on page 12
- ◆ [“Using the no Form of a Command”](#) on page 14
- ◆ [“CN1601 Software Modules”](#) on page 15
- ◆ [“Command Modes”](#) on page 16
- ◆ [“Command Completion and Abbreviation”](#) on page 22
- ◆ [“CLI Error Messages”](#) on page 23
- ◆ [“CLI Line-Editing Conventions”](#) on page 24
- ◆ [“Using CLI Help”](#) on page 26
- ◆ [“Accessing the CLI”](#) on page 28

# 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:

```
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 *NetApp CN1601 Network Switch 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 shows.

# Command Conventions

---

The parameters for a command might include mandatory values, optional values, or keyword choices. Parameters are order-dependent. The following Parameter Conventions table describes the conventions this document uses to distinguish between value types:

Symbol	Example	Description
[ ] square brackets	[value]	Indicates an optional parameter.
<i>italic font in a parameter.</i>	value or [value]	Indicates a variable value. You must replace the italicized text and brackets with an appropriate value, which might be a name or number.
{ } 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}]	Indicates a choice within an optional element.

## 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. The following Parameter Descriptions table describes common parameter values and value formatting:

Parameter	Description
ipaddr	<p>This parameter is a valid IP address. You can enter the IP address in the following formats:</p> <ul style="list-style-type: none"><li>a (32 bits)</li><li>a.b (8.24 bits)</li><li>a.b.c (8.8.16 bits)</li><li>a.b.c.d (8.8.8.8)</li></ul> <p>In addition to these formats, the CLI accepts decimal, hexadecimal, and octal formats through the following input formats (where <i>n</i> is any valid hexadecimal, octal or decimal number):</p> <ul style="list-style-type: none"><li>0xn (CLI assumes hexadecimal format.)</li><li>0n (CLI assumes octal format with leading zeros.)</li><li>n (CLI assumes decimal format.)</li></ul>
ipv6-address	<p>FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or FE80:0:0:0:20F:24FF:FEBF:DBCB, or FE80::20F24FF:FEBF:DBCB, or FE80:0:0:0:20F:24FF:128:141:49:32</p> <p>For additional information, refer to RFC 3513.</p>
Interface or slot/port	<p>Valid slot and port number separated by a forward slash. For example, 0/1 represents slot number 0 and port number 1.</p>
Logical Interface	<p>Represents a 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.</p>

Parameter	Description
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

## Slot/Port Naming Convention

---

FASTPATH software references physical entities such as cards and ports by using a slot/port naming convention. The FASTPATH 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.

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.

Port Type	Description
Physical ports	The physical ports for each slot are numbered sequentially starting from zero.
Logical interfaces	<p>There are four types of logical interfaces:</p> <ul style="list-style-type: none"><li>◆ Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions.</li><li>◆ VLAN routing interfaces are only used for routing functions.</li><li>◆ Loopback interfaces are logical interfaces that are always up.</li><li>◆ Tunnel interfaces are logical point-to-point links that carry encapsulated packets.</li></ul>



Port Type	Description
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

---

**Note**

In the CLI, loopback and tunnel interfaces do not use the slot/port format. To specify a loopback interface, use the loopback ID. To specify a tunnel interface, use the tunnel ID.

---

## 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.

## CN1601 Software Modules

---

The CN1601 software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The commands and command modes available on your switch depend on the installed modules. Additionally, for some `show` commands, the output fields might change based on the modules included in the CN1601 software.

The CN1601 software suite includes the following modules:

- ◆ Switching (Layer 2)
- ◆ Quality of Service
- ◆ Management (CLI and SNMP)
- ◆ IPv6 Management—Allows management of the CN1601 switch through an IPv6 address without requiring the IPv6 Routing package in the system. The management address can be associated with the network port (front-panel switch ports), a routine interface (port or VLAN), and the Service port.
- ◆ Security

## Command Modes

---

The CLI groups commands into modes according to the command function. Each of the command modes supports specific CN1601 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 changes in each command mode to help you identify the current mode. The following CLI Command Modes table describes the command modes and the prompts visible in that mode:

Command Mode	Prompt	Mode Description
User EXEC	(CN1601) >	Contains a limited set of commands to view basic system information.
Privileged EXEC	(CN1601) #	Allows you to enter any EXEC command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	(CN1601) (Config) #	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	(CN1601) (Vlan) #	Groups all the VLAN commands.

Command Mode	Prompt	Mode Description
Interface Config	(CN1601) (Interface slot/port)#  (CN1601) (Interface Loopback id)#  (CN1601) (Interface Tunnel id)#  (CN1601) (Interface slot/port (startrange) - slot/port (endrange) #	<p>Manages the operation of an interface and provides access to the router interface configuration commands.</p> <p>Use this mode to set up a physical port for a specific logical connection operation.</p> <p>You can also use this mode to manage the operation of a range of interfaces. For example, the prompt may display as follows:</p> <p>(CN1601) (Interface 1/0/1-1/0/4) #</p>
Line Console	(CN1601) (config-line)#	Contains commands to configure outbound Telnet settings and console interface settings, as well as to configure console login/enable authentication.
Line SSH	(CN1601) (config-ssh)#	Contains commands to configure SSH login/enable authentication.

Command Mode	Prompt	Mode Description
Line Telnet	(CN1601) (config-telnet)#	Contains commands to configure Telnet login/enable authentication.
AAA IAS User Config	(CN1601) (Config-IAS-User)#	Allows password configuration for a user in the IAS database.
Mail Server Config	(CN1601) (Mail-Server)#	Allows configuration of the email server.
Policy Map Config	(CN1601) (Config-policy-map)#	Contains the QoS Policy-Map configuration commands.
Policy Class Config	(CN1601) (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	(CN1601) (Config-class-map)#	Contains the QoS class map configuration commands.
MAC Access-list Config	(CN1601) (Config-mac-access-list)#	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.
TACACS Config	(CN1601) (Tacacs)#	Contains commands to configure properties for the TACACS servers.

Command Mode	Prompt	Mode Description
DHCP Pool Config	(CN1601) (Config dhcp-pool)#	Contains the DHCP server IP address pool configuration commands.

The following CLI Mode Access and Exit table explains how to enter or exit each mode:

Command Mode	Prompt	Mode Description
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 or interface loopback id or interface tunnel id or interface slot/port (startrange) - slot/port (endrange)	To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.

<b>Command Mode</b>	<b>Prompt</b>	<b>Mode Description</b>
Line Console	From the Global Config mode, enter <code>line console</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
AAA IAS User Config	From the Global Config mode, enter <code>aaa ias-user username name</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Mail Server Config	From the Global Config mode, enter <code>mail-server address</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Policy-Map Config	From the Global Config mode, enter <code>policy-map</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Policy-Class-Map Config	From the Policy Map mode, enter <code>class</code> .	To exit to the Policy Map mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Class-Map Config	From the Global Config mode, enter <code>class-map</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .



Command Mode	Prompt	Mode Description
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.
TACACS Config	From the Global Config mode, enter tacacs-server host ip-addr, where ip-addr is the IP address of the TACACS server on your network.	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 pool-name.	To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.

## 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 have entered enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

# CLI Error Messages

---

If you enter a command and the system is unable to execute it, an error message appears. The following table describes the most common 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.

## CLI Line-Editing Conventions

---

The following CLI editing conventions table 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.

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.
Ctrl-S	Disables serial flow.
Ctrl-Z	Return to root command prompt.
Tab, <SPACE>	Command-line completion.
Exit	Go to next lower command prompt.

Key Sequence	Description
?	List available commands, keywords, or parameters.

## Using CLI Help

---

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

```
(CN1601)>?
```

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.
quit	Exit this session. Any unsaved changes are lost.
show	Display Switch Options and Settings.
telnet	Telnet to a remote host.

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

```
(CN1601)#network ?
```

mgmt_vlan	Configure the Management VLAN ID of the switch.
parms	Configure Network Parameters of the router.
protocol	Select DHCP, BootP, or None as the network config protocol.

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

```
(CN1601)#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:

```
(CN1601) #show m?
```

```
mac-addr-table
```

```
mac-address-table
```

```
monitor
```

## 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, subnet mask, and default gateway. 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 “[Console Port Access Commands](#)” on page 35.



## About this chapter

This chapter describes the management commands available with the CN1601 CLI.

## Topics in this chapter

This chapter includes the following sections:

- ◆ “[Access Commands](#)” on page 30
- ◆ “[Configuration Scripting Commands](#)” on page 32
- ◆ “[Console Port Access Commands](#)” on page 35
- ◆ “[Management Security Commands](#)” on page 38
- ◆ “[Network Interface Commands](#)” on page 39
- ◆ “[Pre-login Banner, System Prompt, and Host Name Commands](#)” on page 45
- ◆ “[RADIUS Commands](#)” on page 47
- ◆ “[Secure Shell Commands](#)” on page 64
- ◆ “[SNMP Commands](#)” on page 67
- ◆ “[TACACS+ Commands](#)” on page 79
- ◆ “[Telnet Commands](#)” on page 83
- ◆ “[User Account Commands](#)” on page 86

---

### CAUTION

The commands in this chapter 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.
-

## Access Commands

---

### Introduction

Use the commands in this section to close remote connections or to view information about connections to the system.

### disconnect

This command closes HTTP, HTTPS, Telnet, or SSH sessions. Use `all` to close all active sessions, or use `session-id` to specify the session ID to close. To view the possible values for `session-id`, use the `show login session` command.

Format	<code>disconnect {session-id   all}</code>
Mode	Privileged EXEC

### show login session

This command displays current Telnet, SSH, and serial port connections to the switch. This command displays truncated user names. Use the `show login session long` command to display the complete usernames.

Format	<code>show login session</code>
Mode	Privileged EXEC

Output	Description
ID	Login session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote 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.
Session Type	Shows the type of session, which can be HTTP, HTTPS, Telnet, serial, or SSH.

## **show login session long**

This command displays the complete user names of the users currently logged in to the switch.

Format	show login session long
Mode	Privileged EXEC

**Example:** The following shows an example of the command:

```
(CN1601) #show login session long
User Name
-----
admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

# Configuration Scripting Commands

---

## Introduction

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 “[show running-config](#)” on page 194) to capture the running configuration into a script. Use the `copy` command (see “[copy](#)” on page 204) 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 nondefault configurations.

Scripts must conform to the following rules:

- ◆ 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 cannot 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 management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

---

**Note**

To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user jane from a blank password to hello, the script entry is as follows:

```
users passwd jane  
" "  
hello  
hello
```

---

**script apply**

This command executes the commands in the script, applying them to the running configuration.

Format	<code>script apply <i>scriptname</i></code>
Mode	Privileged EXEC

**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	<code>script delete {<i>scriptname</i>   all}</code>
Mode	Privileged EXEC

**script list**

This command lists all of the scripts present on the switch as well as the remaining available space.

Format	<code>script list</code>
Mode	Privileged EXEC

Output	Description
Configuration Script Name	The name of the script.

Output	Description
Size	The size of the script, in bytes.

**Example:** The following shows sample output from this command:

```
(CN1601) #script list
Configuration Script Name      Size(Bytes)
-----
runconfig-17Jan.scr           2586
1 configuration script(s) found.
2045 Kbytes free.
```

## script show

This command displays the contents of a script file, which is called a *scriptname*.

Format	script show <i>scriptname</i>
Mode	Privileged EXEC

Output	Description
Output Format	<i>line number: line contents</i>

## 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 <i>scriptname</i>
Mode	Privileged EXEC

# Console Port Access Commands

**Introduction** 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.

**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

**line** This command gives you access to the Line Console mode, which allows you to configure various Telnet settings and the console port, as well as to configure console login/enable authentication.

Format	line {console   telnet   ssh}
Mode	Global Config

Parameter	Description
console	Console terminal line.
telnet	Virtual terminal for remote console access (Telnet).
ssh	Virtual terminal for secured remote console access (SSH).

**Example:** The following example shows a CLI display:  
(CN1601) (config)#line telnet  
(CN1601) (config-telnet)#

## serial baudrate

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

Default	9600
Format	serial baudrate {1200   2400   4800   9600   19200   38400   57600   115200}
Mode	Line Config

## no serial baudrate

This command sets the communication rate of the terminal interface.

Format	no serial baudrate
Mode	Line Config

## serial timeout

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

Default	5
Format	serial timeout 0-160
Mode	Line Config

## no serial timeout

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

Format	no serial timeout
Mode	Line Config



**show serial**

This command displays serial communication settings for the switch.

Format	show serial
Mode	◆ Privileged EXEC ◆ User EXEC

Output	Description
Serial Port Login Timeout (minutes)	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 Type used on the Serial Port. The Parity Type is always None.

**Example:** The following shows sample output from this command:

```
(CN1601) >show serial
Serial Port Login Timeout (minutes)..... 5
Baud Rate (bps)..... 9600
Character Size (bits)..... 8
Flow Control..... Disable
Stop Bits..... 1
Parity..... none
```

# Management Security Commands

---

## Introduction

This section describes commands you use to generate keys and certificates, which you can do in addition to loading them as before.

### **crypto key generate dsa**

This command generates a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format	crypto key generate dsa
Mode	Global Config

### **no crypto key generate dsa**

This command deletes the DSA key files from the device.

Format	no crypto key generate dsa
Mode	Global Config

### **crypto key generate rsa**

This command generates an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format	crypto key generate rsa
Mode	Global Config

### **no crypto key generate rsa**

This command deletes the RSA key files from the device.

Format	no crypto key generate rsa
Mode	Global Config

# Network Interface Commands

---

Introduction

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see “[network mgmt\\_vlan](#)” on page 379.

enable (Privileged EXEC access)

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

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. You can specify the none option to clear the IPv4 address and mask and the default gateway (that is, to reset each of these values to 0.0.0.0).

Format	network parms {ipaddr netmask [gateway]   none}
Mode	Privileged EXEC

network protocol

This command specifies the network configuration protocol to be used. 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

**network mac-address**

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

- ◆ Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- ◆ Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- ◆ The second character of the twelve-character *macaddr* must be 2, 6, A, or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

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

## 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

## no network mac-type

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

Format	no network mac-type
Mode	Privileged EXEC

## renew dhcp network-port

This command renews an IP address on a network port.

Format	renew dhcp network-port
Modes	Privileged EXEC

## renew dhcp service-port

This command renews an IP address on a service port.

Format	renew dhcp service-port
Modes	Privileged EXEC

## 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. The network interface is always considered to be up, whether or not any member ports are up; therefore, the `show network` command will always show Interface Status as Up.

Format	show network
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
Interface Status	The network interface status; it is always considered to be up.
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.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Prefix	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.

Output	Description
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, for example, byte 0 should have the 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 Bridge Identifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which 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.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp   dhcp   none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp   none.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.

**Example:** The following shows example CLI display output for the network port:

```
(CN1601) #show network
```

```
Interface Status..... Always Up
IP Address..... 10.250.3.1
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.250.3.3
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is .....
fe80::210:18ff:fe82:64c/64
IPv6 Prefix is ..... 2003::1/128
IPv6 Default Router is .....
fe80::204:76ff:fe73:423a
Burned In MAC Address..... 00:10:18:82:06:4C
Locally Administered MAC address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Configured IPv4 Protocol ..... None
Configured IPv6 Protocol ..... DHCP
DHCPv6 Client DUID .....
00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode..... Disabled
Management VLAN ID..... 1
```



# Pre-login Banner, System Prompt, and Host Name Commands

Introduction

This section describes the commands you use to 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`.

copy (pre-login banner)

This command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using TFTP, SFTP, SCP, or Xmodem.

**Note**  
The parameter `ip6address` is also a valid parameter for routing packages that support IPv6.

Default	none
Format	<code>copy &lt;tftp://&lt;ipaddr&gt;/&lt;filepath&gt;/&lt;filename&gt;&gt; nvram:clibanner</code>  <code>copy nvram:clibanner &lt;tftp://&lt;ipaddr&gt;/&lt;filepath&gt;/&lt;filename&gt;&gt;</code>
Mode	Privileged EXEC

set prompt

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

Format	<code>set prompt <i>prompt_string</i></code>
Mode	Privileged EXEC

## hostname

This command sets the system hostname. It also changes the prompt. The length of *hostname* may be up to 64 alphanumeric, case-sensitive characters.

Format	hostname <i>hostname</i>
Mode	Privileged EXEC

# RADIUS Commands

---

**Introduction**

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

**radius accounting mode**

This command enables the RADIUS accounting function.

Default	disabled
Format	radius accounting mode
Mode	Global Config

**no radius accounting mode**

This command sets the RADIUS accounting function to the default value, that is, the RADIUS accounting function is disabled.

Format	no radius accounting mode
Mode	Global Config

**radius server attribute 4**

This command specifies the RADIUS client to use the NAS-IP Address attribute (4) in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending the NAS-IP-Address attribute in RADIUS communication.

Format	radius server attribute 4 [ <i>ipaddr</i> ]
Mode	Global Config

Parameter	Description
4	The NAS-IP-Address attribute to be used in RADIUS requests.

Parameter	Description
<i>ipaddr</i>	The IP address of the server.

### no radius server attribute 4

The **no** version of this command disables the NAS-IP-Address attribute global parameter for the RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format	<code>no radius server attribute 4 [ipaddr]</code>
Mode	Global Config

**Example:** The following shows an example of the command:

```
(CN1601) (Config) #radius server attribute 4 192.168.37.60
(CN1601) (Config) #radius server attribute 4
```

### radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses

Default\_RADIUS\_Auth\_Server and Default\_RADIUS\_Acct\_Server as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the *auth* parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to three servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by entering 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 to 65535, with 1812 being the default value.

---

#### Note

To reconfigure a RADIUS authentication server to use the default UDP port, set the *port* parameter to 1812.

---

If you use the `acct` token, the command configures the IP address or hostname 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 or hostname 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 0 to 65535, with 1813 being the default.

**Note**  
To reconfigure a RADIUS accounting server to use the default UDP port, set the `port` parameter to 1813.

Format	<code>radius server host {auth   acct} {ipaddr/dnsname} [name servername] [port 0-65535]</code>
Mode	Global Config

Parameter	Description
<code>ipaddr</code>	The IP address of the server.
<code>dnsname</code>	The DNS name of the server.
<code>0-65535</code>	The port number to use to connect to the specified RADIUS server.
<code>servername</code>	The alias name to identify the server.

**no radius server  
host**

The `no` version of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. 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|dnsname` parameter must match the IP address or DNS name of the previously configured RADIUS authentication / accounting server.

Format	<code>no radius server host {auth   acct} {ipaddr dnsname}</code>
Mode	Global Config

**Example:** The following shows an example of the command:

```
(CN1601)(Config) #radius server host acct 192.168.37.60
(CN1601)(Config) #radius server host acct 192.168.37.60 port 1813
(CN1601)(Config) #radius server host auth 192.168.37.60 name
Network1_RS port 1813
(CN1601)(Config) #radius server host acct 192.168.37.60 name
Network2_RS
(CN1601)(Config) #no radius server host acct 192.168.37.60
```

## radius server key

This command configures the key to use in RADIUS client communication with the specified 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 or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports the RADIUS server's secrets in encrypted and nonencrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the `show running config` command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

### Note

The secret must be an alphanumeric value not exceeding 16 characters.

Format	<code>radius server key {auth   acct} {ipaddr dnsname}</code> <i>encrypted password</i>
Mode	Global Config

Parameter	Description
<i>ipaddr</i>	The IP address of the server.
<i>dnsname</i>	The DNS name of the server.
<i>password</i>	The password in encrypted format.

**Example:** The following shows an example of the command:

```
radius server key acct 10.240.4.10 encrypted encrypt-string
```

### radius server msgauth

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	<code>radius server msgauth <i>ipaddr/dnsname</i></code>
Mode	Global Config

Parameter	Description
<i>ipaddr</i>	The IP address of the server.
<i>dnsname</i>	The DNS name of the server.

### no radius server msgauth

The no version of this command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	<code>no radius server msgauth <i>ipaddr/dnsname</i></code>
Mode	Global Config

### radius server primary

This command specifies a configured server that should be the primary server in the group of servers that have the same server name. Multiple primary servers can be configured for each number of servers that have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of specified name, the client uses the primary server that has the specified server name by default. If the RADIUS client fails to communicate with the primary server for any reason, the client uses the backup servers configured with the same server name. These backup servers are identified as the Secondary type.

Format	<code>radius server primary {<i>ipaddr dnsname</i>}</code>
Mode	Global Config

Parameter	Description
<i>ipaddr</i>	The IP address of the RADIUS Authenticating server.
<i>dnsname</i>	The DNS name of the server.

### radius server retransmit

This command configures the global parameter for the RADIUS client that specifies the number of transmissions of the messages to be made before attempting the fall back server upon unsuccessful communication with the current RADIUS authenticating server. When the maximum number of retries are exhausted for the RADIUS accounting server and no response is received, the client does not communicate with any other server. The number of retries allowed ranges from 1 to 15. The default number of retries is 4.

Default	4
Format	radius server retransmit <i>retries</i>
Mode	Global Config

Parameter	Description
<i>retries</i>	The maximum number of transmission attempts in the range of 1 to 15.

### no radius server retransmit

The no version of this command sets the value of this global parameter to the default value.

Format	no radius server retransmit
Mode	Global Config



**radius server  
timeout**

This command configures the global parameter for the RADIUS client that specifies 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. The default is 5 seconds.

Default	5
Format	radius server timeout <i>seconds</i>
Mode	Global Config

Parameter	Description
<i>seconds</i>	The timeout value, in seconds, after which a request must be retransmitted. Range is 1 to 30.

**no radius server  
timeout**

The no version of this command sets the timeout global parameter to the default value.

Format	no radius server timeout
Mode	Global Config

**show radius**

This command displays the values configured for the global parameters of the RADIUS client.

Format	show radius
Mode	Privileged EXEC

Output	Description
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.

Output	Description
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether or not the accounting mode for all the servers is enabled.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled for use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute of RADIUS requests.

**Example:** The following shows example CLI display output for the command:  
(CN1601) #show radius

```

Number of Configured Authentication Servers..... 32
Number of Configured Accounting Servers..... 32
Number of Named Authentication Server Groups..... 15
Number of Named Accounting Server Groups..... 3
Number of Retransmits..... 4
Time Duration..... 10
RADIUS Accounting Mode..... Disable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value .....192.168.37.60

```

**show radius servers** This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

Format	<code>show radius servers [{<i>ipaddr/dnsname</i>   name [<i>servername</i>}]}</code>
Mode	Privileged EXEC

Output	Description
<i>ipaddr</i>	The IP address of the authenticating server.
<i>dnsname</i>	The DNS name of the authenticating server.
<i>servername</i>	The alias name to identify the server.
Current	The * symbol preceding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.

Output	Description
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled for use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute of RADIUS requests.

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#show radius servers
```

```
Current Host Address  Server Name          Port  Type
-----
*   192.168.37.200    Network1_RADIUS_Server 1813  Primary
    192.168.37.201    Network2_RADIUS_Server 1813  Secondary
    192.168.37.202    Network3_RADIUS_Server 1813  Primary
    192.168.37.203    Network4_RADIUS_Server 1813  Secondary
```

```
(CN1601)#show radius servers name
```

```
Current Host Address  Server Name          Type
-----
192.168.37.200        Network1_RADIUS_Server  Secondary
192.168.37.201        Network2_RADIUS_Server  Primary
192.168.37.202        Network3_RADIUS_Server  Secondary
192.168.37.203        Network4_RADIUS_Server  Primary
```

```
(CN1601)#show radius servers name Default_RADIUS_Server
```

```
Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.58
Secret Configured..... No
```

```
Message Authenticator ..... Enable
Number of Retransmits..... 4
Time Duration..... 10
RADIUS Accounting Mode..... Disable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value ..... 192.168.37.60

(CN1601)#show radius servers 192.168.37.58

Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.58
Secret Configured..... No
Message Authenticator ..... Enable
Number of Retransmits..... 4
Time Duration..... 10
RADIUS Accounting Mode..... Disable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value ..... 192.168.37.60
```

**show radius accounting**

This command displays a summary of configured RADIUS accounting servers.

Format	show radius accounting name [servername]
Mode	Privileged EXEC

Output	Description
<i>servername</i>	An alias name to identify the server.
RADIUS Accounting Mode	A global parameter to indicate whether or not the accounting mode for all the servers is enabled.

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Output	Description
Host Address	The IP address of the host.
Server Name	The name of the accounting server.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

**Example:** The following shows example CLI display output for the command:  
(CN1601)#show radius accounting name

Host Address	Server Name	Port	Secret Configured
-----	-----	-----	-----
192.168.37.200	Network1_RADIUS_Server	1813	Yes
192.168.37.201	Network2_RADIUS_Server	1813	No
192.168.37.202	Network3_RADIUS_Server	1813	Yes
192.168.37.203	Network4_RADIUS_Server	1813	No

```
(CN1601)#show radius accounting name Default_RADIUS_Server
```

```
Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.200
RADIUS Accounting Mode..... Disable
Port ..... 1813
Secret Configured ..... Yes
```

## show radius accounting statistics

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format	show radius accounting statistics {ipaddr/dnsname   name servername}
Mode	Privileged EXEC

Output	Description
<i>ipaddr</i>	The IP address of the server.
<i>dnsname</i>	The DNS name of the server.
<i>servername</i>	The alias name to identify the server.
RADIUS Accounting Server Name	The name of the accounting server.
Host Address	The IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Retransmissions	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 or signature attributes or 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.

Output	Description
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.

**Example:** The following shows example CLI display output for the command:  
(CN1601)#show radius accounting statistics 192.168.37.200

```

RADIUS Accounting Server Name.....
Default_RADIUS_Server
Host Address..... 192.168.37.200
Round Trip Time..... 0.00
Requests..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0

```

```

(CN1601)#show radius accounting statistics name
Default_RADIUS_Server

RADIUS Accounting Server Name.....
Default_RADIUS_Server
Host Address..... 192.168.37.200
Round Trip Time..... 0.00
Requests..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0

```



**show radius statistics**

This command displays the summary statistics of configured RADIUS Authenticating servers.

Format	<code>show radius statistics {ipaddr/dnsname   name servername}</code>
Mode	Privileged EXEC

Output	Description
<i>ipaddr</i>	The IP address of the server.
<i>dnsname</i>	The DNS name of the server.
<i>servername</i>	The alias name to identify the server.
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.

Output	Description
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 packets of unknown type that 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.

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#show radius statistics 192.168.37.200
```

```
RADIUS Server Name.....
Default_RADIUS_Server
Server Host Address..... 192.168.37.200
Access Requests..... 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

```
(CN1601)#show radius statistics name Default_RADIUS_Server
```

```
RADIUS Server Name.....
Default_RADIUS_Server
Server Host Address..... 192.168.37.200
Access Requests..... 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

# Secure Shell Commands

---

Introduction

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

Note

The system allows a maximum of five SSH sessions.

---

ip ssh

This command enables SSH access to the system. (This command is the short form of the `ip ssh server enable` command.)

Default	disabled
Format	ip ssh
Mode	Privileged EXEC

ip ssh protocol

This command sets or removes protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 [1] and [2] can be set. The default is 1 and 2.

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

ip ssh server enable

This command enables the IP secure shell server. No new SSH connections are allowed, but the existing SSH connections continue to work until timed out or logged out.

Default	disabled
Format	ip ssh server enable

Mode	Privileged EXEC
------	-----------------

### **no ip ssh server enable**

This command disables the IP secure shell server.

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

### **sshcon maxsessions**

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

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

### **no sshcon maxsessions**

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

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

### **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. The default is 5 minutes.

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

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

## 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 reaccessed. Also, any keystroke activates the new timeout duration.

Format	no sshcon timeout
Mode	Privileged EXEC

## show ip ssh

This command displays the SSH settings.

Format	show ip ssh
Mode	Privileged EXEC

Output	Description
Administra- tive 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 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH timeout value, in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

# SNMP Commands

---

Introduction

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The parameters *name*, *loc*, and *con* can be up to 255 characters in length.

Format	<code>snmp-server {sysname <i>name</i>   location <i>loc</i>   contact <i>con</i>}</code>
Mode	Global Config

snmp-server community

This command adds (and names) a new SNMP community. A community *name* is a name associated with the switch and 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 simple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default	<ul style="list-style-type: none"><li>◆ Public and private, which you can rename.</li><li>◆ Default values for the remaining four community names are blank.</li></ul>
Format	<code>snmp-server community <i>name</i></code>
Mode	Global Config

### **no snmp-server community**

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

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

### **snmp-server community ipaddr**

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address. It 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 <i>ipaddr name</i>
Mode	Global Config

### **no snmp-server community ipaddr**

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

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

### **snmp-server community ipmask**

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

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



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

### **no snmp-server community ipmask**

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

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

### **snmp-server community mode**

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right.

Default	<ul style="list-style-type: none"> <li>◆ private and public communities - Enabled</li> <li>◆ other four communities - Disabled</li> </ul> <p><b>Note:</b> A maximum of six communities can be assigned for this switch, which leaves four since two (public and private) are assigned by default. See the command “<a href="#">show snmpcommunity</a>” on page 75.</p>
Format	<code>snmp-server community mode <i>name</i></code>
Mode	Global Config

### **no snmp-server community mode**

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

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

**snmp-server  
community ro**

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

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

**snmp-server  
community rw**

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

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

**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. You can use this command to configure a single interface or a range of interfaces.

**Note**

For other port security commands, see [“Port Security Commands”](#) on page 333.

Default	disabled
Format	<code>snmp-server enable traps violation</code>
Mode	Interface Config

**no snmp-server  
enable traps  
violation**

This command disables the sending of new violation traps.

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

**snmp-server enable  
traps**

This command enables the Authentication Flag.

Default	enabled
---------	---------

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

### **no snmp-server enable traps**

This command disables the Authentication Flag.

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

### **snmp-server enable traps linkmode**

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See “[snmp trap link-status](#)” on page 74.

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

### **no snmp-server enable traps linkmode**

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

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

### **snmp-server enable traps multiusers**

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

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

**no snmp-server  
enable traps  
multiusers**

This command disables Multiple User traps.

Format	no snmp-server enable traps multiusers
Mode	Global Config

**snmp-server enable  
traps stpmode**

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

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

**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

**snmptrap**

This command adds an SNMP trap receiver. The maximum length of *name* is 16 case-sensitive alphanumeric characters. The value for *ipaddr* or *ip6addr* can be an IPv4 address, IPv6 address, or hostname. The *snmpversion* is the version of SNMP. The *snmpversion* parameter options are *snmpv1* or *snmpv2*. The default is *snmpv2*. The SNMP trap address can be set using both an IPv4 address format as well as an IPv6 global address format.

---

**Note**

The *name* parameter does not need to be unique; however, the *name* and receiver pair must be unique. Multiple entries can exist with the same *name*, as long as they are associated with a different receiver IP address or hostname. 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. See “[snmp-server community](#)” on page 67.

---

Default	snmpv2
Format	snmptrap <i>name</i> { <i>ipaddr</i>   <i>ip6addr</i> } { <i>ipaddr</i>   <i>ip6addr</i>   <i>hostname</i> } [ <i>snmpversion snmpversion</i> ]
Mode	Global Config

**Example:** The following shows an example of the CLI command:  
(CN1601) # snmptrap mytrap ip6addr 3099::2

## no snmptrap

This command deletes trap receivers for a community.

Format	no snmptrap <i>name</i> { <i>ipaddr</i>   <i>ip6addr</i> } { <i>ipaddr</i>   <i>ip6addr</i>   <i>hostname</i> }
Mode	Global Config

## snmptrap snmpversion

This command modifies the SNMP version of a trap. The maximum length of *name* is 16 case-sensitive alphanumeric characters. The *snmpversion* parameter options are *snmpv1* or *snmpv2*. The default is *snmpv2*.

### Note

This command does not support a no form.

Default	snmpv2
Format	snmptrap <i>snmpversion name</i> { <i>ipaddr</i>   <i>ip6addr</i>   <i>hostname</i> } <i>snmpversion</i>
Mode	Global Config

**snmptrap ipaddr**

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

**Note**\_\_\_\_\_

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

\_\_\_\_\_

Format	<code>snmptrap ipaddr name ipaddrold {ipaddrnew   hostnamenew}</code>
Mode	Global Config

**snmptrap mode**

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

Format	<code>snmptrap mode name {ipaddr   ip6addr   hostname}</code>
Mode	Global Config

**no snmptrap mode**

This command deactivates an SNMP trap. Disabled trap receivers are unable to receive traps.

Format	<code>no snmptrap mode name {ipaddr   ip6addr   hostname}</code>
Mode	Global Config

**snmp trap link-status**

This command enables link status traps on an interface or range of interfaces.

**Note**\_\_\_\_\_

This command is valid only when the Link Up/Down Flag is enabled. See [“snmp-server enable traps linkmode”](#) on page 71.

\_\_\_\_\_

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

**no snmp trap link-status**

This command disables link status traps by interface.

**Note**\_\_\_\_\_

This command is valid only when the Link Up/Down Flag is enabled.

Format	no snmp trap link-status
Mode	Interface Config

**snmp trap link-status all**

This command enables link status traps for all interfaces.

**Note**\_\_\_\_\_

This command is valid only when the Link Up/Down Flag is enabled. See [“snmp-server enable traps linkmode”](#) on page 71.

Format	snmp trap link-status all
Mode	Global Config

**no snmp trap link-status all**

This command disables link status traps for all interfaces.

**Note**\_\_\_\_\_

This command is valid only when the Link Up/Down Flag is enabled. See [“snmp-server enable traps linkmode”](#) on page 71.

Format	no snmp trap link-status all
Mode	Global Config

**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

Output	Description
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.  <b>Note:</b> 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 the IP address. If the result matches with the 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, for example, 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.



**Example:** The following shows sample output from this command:

```
(CN1601) #show snmpcommunity
```

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
private	0.0.0.0	0.0.0.0	Read/Write	Enable
netapp	0.0.0.0	0.0.0.0	Read Only	Enable

## 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

Output	Description
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 in length.
IP Address	The IPv4 address to receive SNMP traps from this device.
IPv6 Address	The IPv6 address to receive SNMP traps from this device.
SNMP Version	SNMPv2
Status	The receiver's status (enabled or disabled).

**Example:** The following shows an example of the CLI command:

```
(CN1601) #show snmptrap
```

SNMP Trap Name	IP Address	IPv6 Address	SNMP Version	Status
Mytrap	2.2.2.2		snmpv2	Enable

**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

Output	Description
Authentication Flag	Status can be Enable or Disable. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Status can be Enable or Disable. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Status can be Enable or Disable. 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 through Telnet or the serial port).
Spanning Tree Flag	Status can be Enable or Disable. The factory default is enabled. Indicates whether spanning tree traps are sent.

**Example:** The following shows an example of this command:

```
(CN1601) #show trapflags

Authentication Flag..... Enable
Link Up/Down Flag..... Enable
Multiple Users Flag..... Enable
Spanning Tree Flag..... Enable
ACL Traps..... Disable
```

# TACACS+ Commands

---

## Introduction

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

## **tacacs-server host**

Use this `tacacs-server host` command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The *ip-address/hostname* parameter is the IP address or hostname of the TACACS+ server. To specify multiple hosts, you can use multiple `tacacs-server host` commands.

Format	<code>tacacs-server host ip-address/hostname</code>
Mode	Global Config

## **no tacacs-server host**

This command deletes the specified hostname or IP address. The *ip-address/hostname* parameter is the IP address of the TACACS+ server.

Format	<code>no tacacs-server host ip-address/hostname</code>
Mode	Global Config

## **tacacs-server key**

This command sets the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *key-string* parameter has a range of 0 to 128 characters and specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon.

Text-based configuration supports TACACS server's secrets in encrypted and nonencrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the “[show running-config](#)” command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	<code>tacacs-server key [key-string   encrypted key-string]</code>
Mode	Global Config

### **no tacacs-server key**

This command disables the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *key-string* parameter has a range of 0 to 128 characters. This key must match the key used on the TACACS+ daemon.

Format	<code>no tacacs-server key key-string</code>
Mode	Global Config

### **tacacs-server timeout**

This command sets the timeout value for communication with the TACACS+ servers. The *timeout* parameter has a range of 1 to 30 and is the timeout value in seconds. The default is 5 seconds.

Default	5
Format	<code>tacacs-server timeout timeout</code>
Mode	Global Config

### **no tacacs-server timeout**

This command restores the default timeout value for all TACACS+ servers.

Format	<code>no tacacs-server timeout</code>
Mode	Global Config

**key** Use this command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the key used on the TACACS+ daemon. The *key-string* parameter specifies the key name. For an empty string use “”. The range is 0 to 128 characters.

Text-based configuration supports TACACS+ server’s secrets in encrypted and nonencrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the “[show running-config](#)” command’s display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	key [ <i>key-string</i>   encrypted <i>key-string</i> ]
Mode	TACACS Config

**port** Use this command in TACACS Configuration mode to specify a server port number. The server *port-number* range is 0 to 65535.

Default	49
Format	port <i>port-number</i>
Mode	TACACS Config

**priority** Use this command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The *priority* parameter specifies the priority for servers. The highest priority is 0 (zero), the default, and the range is 0 to 65535.

Default	0
Format	priority <i>priority</i>
Mode	TACACS Config

## timeout

Use this command in TACACS Configuration mode to specify the timeout value, in seconds. If no timeout value is specified, the global value is used. The *timeout* parameter has a range of 1 to 30 and is the timeout value in seconds.

Format	<code>timeout timeout</code>
Mode	TACACS Config

## show tacacs

This command displays the configuration and statistics of a TACACS+ server.

Format	<code>show tacacs [ip-address/hostname]</code>
Mode	Privileged EXEC

Output	Description
Host Address	The IP address or hostname of the configured TACACS+ server.
Port	The configured TACACS+ server port number.
TimeOut	The timeout in seconds for establishing a TCP connection.
Priority	The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.

# Telnet Commands

---

Introduction

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.

ip telnet server enable

This command enables Telnet connections to the system and enables the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default	enabled
Format	ip telnet server enable
Mode	Privileged EXEC

no ip telnet server enable

This command disables Telnet access to the system and disables the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format	no ip telnet server enable
Mode	Privileged EXEC

transport input telnet

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

**Note**

If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the command “[ip telnet server enable](#)” on page 83 to enable Telnet Server Admin mode.

Default	enabled
Format	transport input telnet
Mode	Line Config

## **no transport input telnet**

This command prevents new Telnet sessions from being established.

Format	no transport input telnet
Mode	Line Config

## **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

## **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

## **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 set. The time is a decimal value from 1 to 160.

### **Note**

When you change the timeout value, the new value is immediately applied to all active and inactive sessions. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Default	5
Format	telnetcon timeout 1-160
Mode	Privileged EXEC



**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 accessed again. Also, any keystroke activates the new timeout duration.

Format	no telnetcon timeout
Mode	Privileged EXEC

**show telnetcon**

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format	show telnetcon
Modes	◆ Privileged EXEC ◆ User EXEC

Output	Description
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	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

# User Account Commands

## Introduction

This section describes the commands you use to add, manage, and delete system users. FASTPATH software 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. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

## aaa authentication login

This command sets authentication at login. The default and optional list names created with the command are used with the `aaa authentication login` command. Create a list by entering the `aaa authentication login list-name method` command for a particular protocol, where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `RADIUS`, no authentication is used if the `RADIUS` server is down.

Default	<ul style="list-style-type: none"><li>◆ <code>defaultList</code>. Used by the console and only contains the method <code>none</code>.</li><li>◆ <code>networkList</code>. Used by Telnet and SSH and only contains the method <code>local</code>.</li></ul>
Format	<code>aaa authentication login {default   list-name} method1 [method2...]</code>
Mode	Global Config

Parameter	Description
<code>default</code>	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
<code>list-name</code>	Character string of up to 12 characters used to name the list of authentication methods activated when a user logs in.
<code>method1...</code> <code>[method2...]</code>	At least one from the following: <ul style="list-style-type: none"> <li>◆ <code>enable</code>. Uses the enable password for authentication.</li> <li>◆ <code>line</code>. Uses the line password for authentication.</li> <li>◆ <code>local</code>. Uses the local username database for authentication.</li> <li>◆ <code>none</code>. Uses no authentication.</li> <li>◆ <code>radius</code>. Uses the list of all RADIUS servers for authentication.</li> <li>◆ <code>tacacs</code>. Uses the list of all TACACS+ servers for authentication.</li> </ul>

**Example:** The following shows an example of the command:

```
(CN1601)(config)# aaa authentication login default radius local
enable none
```

## no aaa authentication login

This command returns to the default.

Format	<code>no aaa authentication login {default   list-name}</code>
Mode	Global Config

**aaa authentication enable**

This command sets authentication for accessing higher privilege levels. The default enable list is enableList. It is used by console, Telnet, and SSH and only contains the method none.

The default and optional list names created with the aaa authentication enable command are used with the enable authentication command. Create a list by entering the aaa authentication enable list-name method command where list-name is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line.

**Note**  
Enable will not succeed for a level one user if no authentication method is defined. A level one user must authenticate to get to privileged EXEC mode. For example, if none is specified as an authentication method after radius, no authentication is used if the RADIUS server is down.

**Note**  
Requests sent by the switch to a RADIUS server include the username \$enabx\$, where x is the requested privilege level. For enable to be authenticated on RADIUS servers, add \$enabx\$ users to them. The login user ID is now sent to TACACS+ servers for enable authentication.

Default	default
Format	aaa authentication enable {default   list-name} method1 [method2...]
Mode	Global Config

Parameter	Description
default	Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.

Parameter	Description
<i>list-name</i>	Character string used to name the list of authentication methods activated, when using access higher privilege levels. The range is 1 to 12 characters.
<i>method1</i> [ <i>method2...</i> ]	Specify at least one from the following: <ul style="list-style-type: none"> <li>◆ enable. Uses the enable password for authentication.</li> <li>◆ line. Uses the line password for authentication.</li> <li>◆ none. Uses no authentication.</li> <li>◆ radius. Uses the list of all RADIUS servers for authentication.</li> <li>◆ tacacs. Uses the list of all TACACS+ servers for authentication.</li> </ul>

**Example:** The following example sets authentication when accessing higher privilege levels:

```
(CN1601)(config)# aaa authentication enable default enable
```

### no aaa authentication enable

This command returns to the default configuration.

Format	no aaa authentication enable {default   <i>list-name</i> }
Mode	Global Config

### enable authentication

This command specifies the authentication method list when accessing a higher privilege level from a remote Telnet or console.

Format	enable authentication {default   <i>list-name</i> }
Mode	Line Config

Parameter	Description
default	Uses the default list created with the aaa authentication enable command.

Parameter	Description
<i>list-name</i>	Uses the indicated list created with the <code>aaa authentication enable</code> command.

**Example:** The following example specifies the default authentication method when accessing a higher privilege level console:

```
(CN1601) (config) # line console
(CN1601) (config-line) # enable authentication default
```

## no enable authentication

This command returns to the default specified by the `enable authentication` command.

Format	<code>no enable authentication</code>
Mode	Line Config

## username

This command adds a new user to the local user database. The default privilege level is 1. Using the `encrypted` keyword allows the administrator to transfer local user passwords between devices without having to know the passwords. When the `password` parameter is used along with `encrypted` parameter, the password must be exactly 128 hexadecimal characters in length. If the password strength feature is enabled, this command checks for password strength and returns an appropriate error if it fails to meet the password strength criteria. Giving the optional parameter `override-complexity-check` disables the validation of the password strength.

Format	<code>username name password password [level level] [encrypted] [override-complexity-check]</code>
Mode	Global Config

Parameter	Description
<i>name</i>	The name of the user. The name can be 1 to 32 characters in length.

Parameter	Description
<i>password</i>	The authentication password for the user. The range is 8 to 64 characters in length. This value can be zero if the <code>no passwords min-length</code> command has been executed. The special characters allowed in the password include ! # \$ % & ' ( ) * + , - . / : ; < = > @ [ \ ] ^ _ ` {   } ~.
<i>level</i>	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. The levels range from 0 to 15. Enter access level 1 for Read Access or 15 for Read/Write Access.
encrypted	Encrypted password entered or copied from another switch configuration.
override-complexity-check	Disables the validation of the password strength.

**Example:** The following example configures user bob with password xxxxyyyzzzz and user level 15:

```
(CN1601)(config)# username bob password xxxxyyyzzzz level 15
```

**Example:** The following example configures user test with password testPassword and assigns a user level of 1 (read-only). The password strength will not be validated.

```
(CN1601)(config)# username test password testPassword level 1
override-complexity-check
```

## no username

This command removes a user name.

Format	no username <i>name</i>
Mode	Global Config

**username name  
nopassword**

This command removes an existing user’s password (NULL password).

Format	username name nopassword [ <i>level level</i> ]
Mode	Global Config

Parameter	Description
<i>name</i>	The name of the user. The range is 1 to 32 characters in length.
<i>level</i>	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user’s access. The range of user levels is 0 to 15.

**username name  
unlock**

This command allows a locked user account to be unlocked. Only a user with read/write access can re-activate a locked user account.

Format	username name unlock
Mode	Global Config

**username 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. You must enter the *username* in the same case you used when you added the user. To see the case of the *username*, enter the *show users* command.

Default	<ul style="list-style-type: none"><li>◆ admin - readwrite</li><li>◆ other - readonly</li></ul>
Format	username snmpv3 accessmode username { <i>readonly</i> / <i>readwrite</i> }
Mode	Global Config



**no username  
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	<code>no username snmpv3 accessmode username</code>
Mode	Global Config

**username 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. You must enter the *username* in the same case you used when you added the user. To see the case of the *username*, enter the `show users` command.

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

**no username  
snmpv3  
authentication**

This command specifies 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	<code>no username snmpv3 authentication username</code>
Mode	Global Config

## username 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. You must enter the *username* in the same case you used when you added the user. To see the case of the *username*, enter the `show users` command.

Default	none (no encryption)
Format	username snmpv3 encryption username {none   des[key]}
Mode	Global Config

## no username snmpv3 encryption

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

Format	no username snmpv3 encryption username
Mode	Global Config

## username snmpv3 encryption encrypted

This command specifies the `des` encryption protocol and the required encryption key for the specified user. The encryption key must be 8 to 64 characters long.

Default	no encryption
Format	username snmpv3 encryption encrypted username des key
Mode	Global Config

## show users

This command displays the configured user names and their settings. The `show users` command displays truncated user names. Use the `show users long` command to display the complete usernames. The `show users` command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

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

Output	Description
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 <code>admin</code> user has Read/Write access and the <code>guest</code> has Read Only access.
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to <code>ReadWrite</code> , the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to <code>ReadOnly</code> , 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	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

**show users long**

This command displays the complete usernames of the configured users on the switch.

Format	show users long
Mode	Privileged EXEC

**Example:** The following shows an example of this command:

```
(CN1601)#show users long
User Name
-----
admin
guest
test1111test1111test1111test1111
```

**show users accounts**

This command displays the local user status with respect to user account lockout and password aging. This command displays truncated user names. Use the show users long command to display the complete usernames.

Format	show users accounts [detail]
Mode	Privileged EXEC

Output	Description
UserName	The local user account’s username.
Access Level	The user’s access level (1 for read-only or 15 for read/write).
Password Aging	Number of days, since the password was configured, until the password expires.
Password Expiry Date	The current password expiration date in date format.
Lockout	Indicates whether the user account is locked out (true or false).

If the detail keyword is used, the following additional fields are displayed.

Output	Description
Override Complexity Check	Displays the user's password override complexity check status. By default it is disabled.
Password Strength	Displays the user password's strength (Strong or Weak). This field is displayed only if the Password Strength feature is enabled.

**Example:** The following example displays information about the local user database:

```
(CN1601)#show users accounts
```

UserName	Privilege	Password Aging	Password Expiry date	Lockout
admin	15	---	---	False
guest	1	---	---	False

```
console#show users accounts detail
```

```
UserName..... admin
Privilege..... 15
Password Aging..... ---
Password Expiry..... ---
Lockout..... False
Override Complexity Check..... Disable
Password Strength..... ---
```

## show users login-history

This command displays information about the login history of users.

Format	show users login-history [long]
Mode	Privileged EXEC

Output	Description
Username	Name of the user. The name is 1 to 20 characters in length.

**Example:** The following example shows user login history output:

Login Time	Username	Protocol	Location
Jan 19 2005 08:23:48	Bob	Serial	
Jan 19 2005 08:29:29	Robert	HTTP	172.16.0.8
Jan 19 2005 08:42:31	John	SSH	172.16.0.1
Jan 19 2005 08:49:52	Betty	Telnet	172.16.1.7

## login authentication

This command specifies the login authentication method list for a line (console, Telnet, or SSH). The default configuration uses the default set with the command `aaa authentication login`.

Format	login authentication {default   <i>list-name</i> }
Mode	Line Configuration

Parameter	Description
default	Uses the default list created with the <code>aaa authentication login</code> command.
<i>list-name</i>	Uses the indicated list created with the <code>aaa authentication login</code> command.

**Example:** The following example specifies the default authentication method for a console:

```
(CN1601) (config)# line console
(CN1601) (config-line)# login authentication default
```

### no login authentication

This command returns to the default specified by the authentication login command.

Format	no login authentication
Mode	Line Configuration

### password (Line Configuration)

This command specifies a password on a line. The default configuration is that no password is specified.

Format	password <i>password</i> [encrypted]
Mode	Line Config

Parameter	Description
<i>password</i>	Password for this level. The length is from 8 to 64 characters.
encrypted	Encrypted password to be entered or copied from another switch configuration.

**Example:** The following example specifies a password mcmxxyyy on a line:

```
(CN1601) (config-line)# password mcmxxyyy
```

### no password (Line Configuration)

This command removes the password on a line.

Format	no password password
Mode	Line Config

## password (User EXEC)

This command allows a user to change the password for only that user. This command should be used after the password has aged. The user is prompted to enter the old password and the new password.

Format	password
Mode	User EXEC

**Example:** The following example shows the prompt sequence for executing the password command:

```
(CN1601)>password
Enter old password: *****
Enter new password: *****
Confirm new password: *****
```

## enable password

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case-sensitive.

Format	enable password <i>password</i>
Mode	Privileged EXEC

## no enable password

This command removes the password requirement.

Format	no enable password
Mode	Privileged EXEC

## enable password encrypted

This command allows the administrator to transfer the enable password between devices without having to know the password. The *password* parameter must be exactly 128 hexadecimal characters.

Format	enable password encrypted [ <i>encrypted</i> ]
Mode	Privileged EXEC



Parameter	Description
encrypted	Encrypted password entered or copied from another switch configuration.

### passwords min-length

This command enforces a minimum password length for local users. The value also applies to the enable password. The valid range is 8 to 64 characters.

Default	8
Format	passwords min-length 8-64
Mode	Global Config

### no passwords min-length

This command sets the minimum password length to the default value.

Format	no passwords min-length
Mode	Global Config

### passwords history

This command sets the number of previous passwords to be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in the password history. This ensures that users cannot reuse their passwords often. The valid range is 0 to 10. The default is 0.

Default	0
Format	passwords history 0-10
Mode	Global Config

### no passwords history

This command sets the password history to the default value.

Format	no passwords history
Mode	Global Config

## passwords aging

This command implements aging on passwords for local users. When a user's password expires, the user will be prompted to change it before logging in again. The valid range is 1 to 365 days. The default is 0, or no aging.

Default	0
Format	passwords aging 1-365
Mode	Global Config

## no passwords aging

This command sets the password aging to the default value.

Format	no passwords aging
Mode	Global Config

## passwords lock-out

This command strengthens the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can re-activate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 0 to 5. The default is 0, or no lockout count enforced.

Default	0
Format	passwords lock-out 0-5
Mode	Global Config

## no passwords lock-out

This command sets the password lock-out count to the default value.

Format	no passwords lock-out
Mode	Global Config

### **passwords strength-check**

This command enables the password strength feature. It is used to verify the strength of a password during configuration.

Default	disable
Format	passwords strength-check
Mode	Global Config

### **no passwords strength-check**

This command enables the password strength checking to the default value.

Format	no passwords strength-check
Mode	Global Config

### **passwords strength minimum uppercase-letters**

This command enforces a minimum number of uppercase letters that a password should contain. The valid range is 0 to 16. The default is 2; 0 means there is no restriction on that set of characters.

Default	2
Format	passwords strength minimum uppercase-letters <i>0-16</i>
Mode	Global Config

### **no passwords strength minimum uppercase-letters**

This command resets the minimum number of uppercase letters required in a password to the default value.

Format	no passwords strength minimum uppercase-letters
Mode	Global Config

**passwords strength  
minimum  
lowercase-letters**

This command enforces a minimum number of lowercase letters that a password should contain. The valid range is 0 to 16. The default is 2; 0 means that there is no restriction on that set of characters.

Default	2
Format	<code>passwords strength minimum lowercase-letters 0-16</code>
Mode	Global Config

**no passwords  
strength minimum  
lowercase-letters**

This command resets the minimum number of lowercase letters required in a password to the default value.

Format	<code>no passwords strength minimum lowercase-letters</code>
Mode	Global Config

**passwords strength  
minimum numeric-  
characters**

This command enforces a minimum number of numeric characters that a password should contain. The valid range is 0 to 16. The default is 2; 0 means that there is no restriction on that set of characters.

Default	2
Format	<code>passwords strength minimum numeric-characters 0-16</code>
Mode	Global Config

**no passwords  
strength minimum  
numeric-characters**

This command resets the minimum number of numeric characters required in a password to the default value.

Format	<code>no passwords strength minimum numeric-characters</code>
Mode	Global Config

### passwords strength minimum special-characters

This command enforces a minimum number of special characters that a password should contain. The valid range is 0 to 16. The default is 2; 0 means that there is no restriction on that set of characters.

Default	2
Format	passwords strength minimum special-characters 0-16
Mode	Global Config

### no passwords strength minimum special-characters

This command resets the minimum number of special characters required in a password to the default value.

Format	no passwords strength minimum special-characters
Mode	Global Config

### passwords strength minimum consecutive-characters

This command enforces a minimum number of consecutive characters that a password should contain. An example of consecutive characters is abcd. The valid range is 0 to 16. If a password has consecutive characters more than the configured limit, it fails to configure. The default is 0, which means that there is no restriction on that set of characters.

Default	0
Format	passwords strength minimum consecutive-characters 0-16
Mode	Global Config

### no passwords strength minimum consecutive-characters

This command resets the minimum number of consecutive characters required in a password to the default value.

Format	no passwords strength minimum consecutive-characters
Mode	Global Config

### passwords strength minimum repeated-characters

This command enforces a minimum number of repeated characters that a password should contain. An example of repeated characters is aaaa. The valid range is 0 to 16. If a password has a repetition of characters more than the configured limit, it fails to configure. The default is 0, which means that there is no restriction on that set of characters.

Default	0
Format	passwords strength minimum repeated-characters 0-16
Mode	Global Config

### no passwords strength minimum repeated-characters

This command resets the minimum number of repeated characters required in a password to the default value.

Format	no passwords strength minimum repeated-characters
Mode	Global Config

### passwords strength minimum character-classes

This command enforces a minimum number of characters classes that a password should contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. The valid range is 0 to 4. The default is 4.

Default	4
Format	passwords strength minimum character-classes 0-4
Mode	Global Config

### no passwords strength minimum character-classes

This command resets the minimum number of characters classes required in a password to the default value.

Format	no passwords strength minimum character-classes
Mode	Global Config

### passwords strength exclude-keyword

This command excludes the specified keyword while configuring the password. The password does not accept the keyword in any form (in between the string, case-insensitive and reverse) as a substring. The user can configure up to a maximum of three keywords.

Format	<code>passwords strength exclude-keyword <i>keyword</i></code>
Mode	Global Config

### no passwords strength exclude-keyword

This command resets the restriction for the specified keyword or all the keywords configured.

Format	<code>no passwords strength exclude-keyword [<i>keyword</i>]</code>
Mode	Global Config

### user password

This command allows the currently logged in user to change his or her password without having read/write privileges.

Format	<code>user <i>name</i> password <i>pwd</i></code>
Mode	User EXEC

### show passwords configuration

This command displays the configured password management settings.

Format	<code>show passwords configuration</code>
Mode	Privileged EXEC

Output	Description
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length, in days, that a password is valid.

Output	Description
Lockout Attempts	Number of failed password login attempts before lockout.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when configuring passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when configuring passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when configuring passwords.
Maximum Password Consecutive Characters	Maximum number of consecutive characters required that the password should contain when configuring passwords.
Maximum Password Repeated Characters	Maximum number of repetition of characters that the password should contain when configuring passwords.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric, and special) required when configuring passwords.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.

## show passwords result

This command displays the last password set result information.

Format	show passwords result
Mode	Privileged EXEC

Output	Description
Last User Whose Password is Set	Shows the name of the user with the most recently set password.



Output	Description
Password Strength Check	Shows whether password strength checking is enabled.
Last Password Set Result	Shows whether the attempt to set a password was successful. If the attempt failed, the reason for the failure is included.

### memory free low-watermark processor

This command configures the CPU Free Memory monitoring threshold. The valid range is 1 to 776966.

Format	<code>memory free low-watermark processor 1-776966</code>
Mode	Global Config

### write memory

This command saves running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running-config nvram:startup-config`.

Format	<code>write memory</code>
Mode	Privileged EXEC

### aaa ias-user username

The Internal Authentication Server (IAS) database is a dedicated internal database used for local authentication of users for network access through the IEEE 802.1X feature.

This command adds the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format	<code>aaa ias-user username user</code>
Mode	Global Config

**no aaa ias-user  
username**

This command removes the specified user from the internal user database.

Format	no aaa ias-user username <i>user</i>
Mode	Global Config

**password (AAA IAS  
User Configuration)**

This command specifies a password for a user in the IAS database.

Format	password password [encrypted]
Mode	AAA IAS User Config

Parameter	Description
password	Password for this level. The range is 8 to 64 characters in length.
encrypted	Encrypted password to be entered or copied from another switch configuration.

**no password (AAA  
IAS User  
Configuration)**

This command removes the password for the user.

Format	no password password [encrypted]
Mode	AAA IAS User Config

**clear aaa ias-users**

This command removes all users from the IAS database.

Format	clear aaa ias-users
Mode	Privileged EXEC

**show aaa ias-users**      This command displays configured IAS users and their attributes. Passwords configured are not shown in the `show` command output.

Format	<code>show aaa ias-users</code>
Mode	Privileged EXEC



## About this chapter

This chapter describes the utility commands available in the CN1601 command line interface (CLI).

## Topics in this chapter

This chapter includes the following sections:

- ◆ “[AutoInstall Commands](#)” on page 114
- ◆ “[Cable Test Command](#)” on page 118
- ◆ “[DNS Client Commands](#)” on page 134
- ◆ “[Dual Image Commands](#)” on page 140
- ◆ “[Email Alerting and Mail Server Commands](#)” on page 142
- ◆ “[IP Address Conflict Commands](#)” on page 150
- ◆ “[Serviceability Packet Tracing Commands](#)” on page 157
- ◆ “[Simple Network Time Protocol Commands](#)” on page 167
- ◆ “[System Information and Statistics Commands](#)” on page 174
- ◆ “[System Utility and Clear Commands](#)” on page 198

---

## CAUTION

The commands in this chapter 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.
-

# AutoInstall Commands

---

## Introduction

The AutoInstall feature enables the automatic update of the image and configuration of the switch. This feature enables touchless or low-touch provisioning to simplify switch configuration and imaging.

AutoInstall includes the following support:

- ◆ Downloading an image from a TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.
- ◆ Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.
- ◆ Automatically downloading an image from a TFTP server in the following situations:
  - ❖ When the switch is booted with no saved configuration found.
  - ❖ When the switch is booted with a saved configuration that has AutoInstall enabled.

When the switch boots and no configuration file is found, it attempts to obtain an IP address from a network DHCP server. The response from the DHCP server includes the IP address of the TFTP server where the image and configuration files are located.

After acquiring an IP address and the additional relevant information from the DHCP server, the switch downloads the image file or configuration file from the TFTP server. A downloaded image is automatically installed. A downloaded configuration file is saved to nonvolatile memory.

---

### Note

AutoInstall from a TFTP server can run on any IP interface, including the network port, service port, and in-band routing interfaces (if supported). To support AutoInstall, the DHCP client is enabled operationally on the service port, if it exists, or the network port, if there is no service port.

---

## boot autoinstall

This command operationally starts or stops the AutoInstall process on the switch. The command is nonpersistent and is not saved in the startup or running configuration file.

Default	stopped
Format	boot autoinstall {start   stop}
Mode	Privileged EXEC

### **boot host retrycount**

This command sets the number of attempts to download a configuration file from the TFTP server. The valid range is 1 to 3 attempts. The default is 3.

Default	3
Format	boot host retrycount 1-3
Mode	Privileged EXEC

### **no boot host retrycount**

This command sets the number of attempts to download a configuration file to the default value.

Format	no boot host retrycount
Mode	Privileged EXEC

### **boot host dhcp**

This command enables AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM. The default is disabled.

Default	disabled
Format	boot host dhcp
Mode	Privileged EXEC

### **no boot host dhcp**

This command disables AutoInstall for the next reboot cycle.

Format	no boot host dhcp
Mode	Privileged EXEC

### **boot host autosave**

This command automatically saves the downloaded configuration file to the startup-config file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to nonvolatile memory by using the `write`

memory or copy system:running-config nvram:startup-config command. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled. The default value is disabled.

Default	disabled
Format	boot host autosave
Mode	Privileged EXEC

### **no boot host autosave**

This command automatically disables saving the downloaded configuration on the switch.

Format	no boot host autosave
Mode	Privileged EXEC

### **boot host autoreboot**

This command allows the switch to automatically reboot after successfully downloading an image. When auto reboot is enabled, no administrative action is required to activate the image and reload the switch. The default value is enabled.

Default	enabled
Format	boot host autoreboot
Mode	Privileged EXEC

### **no boot host autoreboot**

This command prevents the switch from automatically rebooting after the image is downloaded by using the AutoInstall feature.

Format	no boot host autoreboot
Mode	Privileged EXEC

### **erase startup-config**

This command erases the text-based configuration file stored in nonvolatile memory. If the switch boots and no startup-config file is found, the AutoInstall process automatically begins.

Format	erase startup-config
Mode	Privileged EXEC



**show autoinstall**

This command displays the current status of the AutoInstall process.

Format	show autoinstall
Mode	Privileged EXEC

**Example:** The following example shows CLI display output for the command:  
(CN1601)#show autoinstall

```
AutoInstall Mode..... Stopped
AutoInstall Persistent Mode..... Disabled
AutoSave Mode..... Disabled
AutoReboot Mode..... Enabled
AutoInstall Retry Count..... 3
```

# Cable Test Command

**Introduction**                      The cable test feature enables you to determine the cable connection status on a selected port.

**Note** \_\_\_\_\_  
The cable test feature is supported only for copper cable. It is not supported for optical fiber cable and NetApp twinax cables.

**cablestatus**                      This command returns the status of the specified port.

**Note** \_\_\_\_\_  
The shipped configuration and supported molex cables are not supported by this command. For example:  
(NetApp CS) #cablestatus 0/9  
  
Invalid cable type.  
Cable status can only be tested on a copper cable.

Format	cablestatus slot/port
Mode	Privileged EXEC

Output	Description
Cable Status	One of the following statuses is returned: <ul style="list-style-type: none"><li>◆ Normal: The cable is working correctly.</li><li>◆ Open: The cable is disconnected or there is a faulty connector.</li><li>◆ Short: There is an electrical short in the cable.</li><li>◆ Cable Test Failed: The cable status could not be determined. The cable may in fact be working.</li></ul>

Output	Description
Cable Length	<p>If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.</p>

# DHCP Server Commands

---

Introduction

This section describes the commands you use to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

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

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

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 unique-identifier
Mode	DHCP Pool Config

**no client-identifier**

This command deletes the client identifier.

Format	no client-identifier
Mode	DHCP Pool Config

**client-name**

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

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

**no client-name**

This command removes the client name.

Format	no client-name
Mode	DHCP Pool Config

**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 <i>address1</i> [ <i>address2</i> ... <i>address8</i> ]
Mode	DHCP Pool Config

**no default-router**

This command removes the default router list.

Format	no default-router
Mode	DHCP Pool Config

## dns-server

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

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

## no dns-server

This command removes the DNS server list.

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

## hardware-address

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

Default	ethernet
Format	<code>hardware-address hardwareaddress type</code>
Mode	DHCP Pool Config

## no hardware-address

This command removes the hardware address of the DHCP client.

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

## host

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

Default	none
---------	------

Format	<code>host address [{mask   prefix-length}]</code>
Mode	DHCP Pool Config

## no host

This command removes the IP address of the DHCP client.

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

## 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 to 86400 minutes. If you specify `infinite`, the lease is set for 60 days. You can also specify a lease duration: `days` is an integer from 0 to 59, `hours` is an integer from 0 to 23, `minutes` is an integer from 0 to 59.

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

## no lease

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

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

## network (DHCP Pool Config)

This command configures the subnet number and mask for a DHCP address pool on the server. The `networknumber` is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The `mask` is the IP subnet mask for the specified address pool. The `prefixlength` is an integer from 0 to 32.

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

**no network**

This command removes the subnet number and mask.

Format	no network
Mode	DHCP Pool Config

**bootfile**

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

Format	bootfile <i>filename</i>
Mode	DHCP Pool Config

**no bootfile**

This command deletes the boot image name.

Format	no bootfile
Mode	DHCP Pool Config

**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 <i>domain</i>
Mode	DHCP Pool Config

**no domain-name**

This command removes the domain name.

Format	no domain-name
Mode	DHCP Pool Config

**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 you 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 <i>address</i> [ <i>address2</i> ... <i>address8</i> ]
Mode	DHCP Pool Config

### **no netbios-name-server**

This command removes the NetBIOS name server list.

Format	no netbios-name-server
Mode	DHCP Pool Config

### **netbios-node-type**

This command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. The *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 <i>type</i>
Mode	DHCP Pool Config

### **no netbios-node-type**

This command removes the NetBIOS node type.

Format	no netbios-node-type
Mode	DHCP Pool Config

## next-server

This command configures the next server in the boot process of a DHCP client. The *address* parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

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

## no next-server

This command removes the boot server list.

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

## option

This command configures DHCP server options. The *code* parameter specifies the DHCP option code and ranges from 1 to 254. The *ascii string* parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The *hex string* parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, `a3.4f.22.0c`), colon (for example, `a3:4f:22:0c`), or white space (for example, `a3 4f 22 0c`).

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

## no option

This command removes the DHCP server options. The *code* parameter specifies the DHCP option code.

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

### **ip dhcp excluded-address**

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. The *low-address* and *high-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	ip dhcp excluded-address <i>lowaddress</i> [ <i>highaddress</i> ]
Mode	Global Config

### **no ip dhcp excluded-address**

This command removes the excluded IP addresses for a DHCP client. The *low-address* and *high-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.

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

### **ip dhcp ping packets**

This command specifies the number, in a range from 2 to 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, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

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

### **no ip dhcp ping packets**

This command restores the number of ping packets to the default value.

Format	no ip dhcp ping packets
Mode	Global Config

### **service dhcp**

This command enables the DHCP server.

Default	disabled
---------	----------

Format	service dhcp
Mode	Global Config

### **no service dhcp**

This command disables the DHCP server.

Format	no service dhcp
Mode	Global Config

### **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

### **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

### **ip dhcp conflict logging**

This command enables conflict logging on DHCP server.

Default	enabled
Format	ip dhcp conflict logging
Mode	Global Config

### **no ip dhcp conflict logging**

This command disables conflict logging on DHCP server.

Format	no ip dhcp conflict logging
Mode	Global Config

### 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.

Format	clear ip dhcp binding { <i>address</i>   *}
Mode	Privileged EXEC

### clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format	clear ip dhcp server statistics
Mode	Privileged EXEC

### 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 { <i>address</i>   *}
Mode	Privileged EXEC

### 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 [ <i>address</i> ]
Modes	◆ Privileged EXEC ◆ User EXEC

Output	Description
IP address	The IP address of the client.
Hardware Address	The MAC Address or the client identifier.

Output	Description
Lease expiration	The lease expiration time of the IP address assigned to the client.
Type	The manner in which IP address was assigned to the client.

## show ip dhcp global configuration

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

Format	show ip dhcp global configuration
Modes	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
Service DHCP	The field to display the status of the 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.

## 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	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
Pool Name	The name of the configured pool.
Pool Type	The pool type.

Output	Description
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 the Dynamic pool type:

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

The following additional fields are displayed for Manual pool type:

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

## show ip dhcp server statistics

This command displays DHCP server statistics.

Format	<code>show ip dhcp server statistics</code>
Modes	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
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.

Output	Description
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server.

The following fields are also displayed with Message Received:

Message	Description
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.

The following fields are also displayed with Message Sent:

Message	Description
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.

## show ip dhcp conflict

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

Format	show ip dhcp conflict [ <i>ip-address</i> ]
Modes	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
IP address	The IP address of the host as recorded on the DHCP server.



Output	Description
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.

# DNS Client Commands

---

Introduction

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components of FASTPATH.

ip domain lookup

This command enables the DNS client.

Default	enabled
Format	ip domain lookup
Mode	Global Config

no ip domain lookup

This command disables the DNS client.

Format	no ip domain lookup
Mode	Global Config

ip domain name

This command defines a default domain name that FASTPATH software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. *name* may not be longer than 255 characters and should not include an initial period. This *name* should be used only when the default domain name list, configured using the `ip domain list` command, is empty.

Default	none
Format	ip domain name <i>name</i>
Mode	Global Config

**Example:** The CLI command `ip domain name yahoo.com` will configure `yahoo.com` as a default domain name. For an unqualified hostname `xxx`, a DNS query is made to find the IP address corresponding to `xxx.yahoo.com`.

**no ip domain name** This command removes the default domain name configured using the `ip domain name` command.

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

**ip domain list** This command defines a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the `ip domain name` command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default	<code>none</code>
Format	<code>ip domain list name</code>
Mode	Global Config

**no ip domain list** This command deletes a name from a list.

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

**ip name server** This command configures the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter `server address` is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they were entered.

Format	<code>ip name server address1 address2</code>
Mode	Global Config

## no ip name server

This command removes a name server.

Format	<code>no ip name server <i>address1 address2</i></code>
Mode	Global Config

## ip host

This command defines static host name-to-address mapping in the host cache. The parameter *name* is the host name and *ipaddress* is the IP address of the host. The host name can include from 1 to 158 alphanumeric characters, periods, hyphens, underscores, and nonconsecutive spaces. Host names that include one or more spaces must be enclosed in quotation marks, for example “lab-pc 45”.

Default	none
Format	<code>ip host <i>name ipaddress</i></code>
Mode	Global Config

## no ip host

This command removes the name-to-address mapping.

Format	<code>no ip host <i>name</i></code>
Mode	Global Config

## ipv6 host

This command defines static host name-to-IPv6 address mapping in the host cache. The parameter *name* is host name and *v6 address* is the IPv6 address of the host. The host name can include 1 to 158 alphanumeric characters, periods, hyphens, and spaces. Host names that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default	none
Format	<code>ipv6 host <i>name v6 address</i></code>
Mode	Global Config

## no ipv6 host

This command removes the static host name-to-ipv6 address mapping in the host cache.

Format	no ipv6 host <i>name</i>
Mode	Global Config

## ip domain retry

This command specifies the number of times to retry sending Domain Name System (DNS) queries. The parameter *number* indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Default	2
Format	ip domain retry <i>number</i>
Mode	Global Config

## no ip domain retry

This command returns to the default.

Format	no ip domain retry <i>number</i>
Mode	Global Config

## ip domain timeout

This command specifies the amount of time to wait for a response to a DNS query. The parameter *seconds* specifies the time, in seconds, to wait for a response to a DNS query. The parameter *seconds* ranges from 0 to 3600. The default is 3 seconds.

Default	3
Format	ip domain timeout <i>seconds</i>
Mode	Global Config

## no ip domain timeout

This command returns to the default setting.

Format	no ip domain timeout <i>seconds</i>
--------	-------------------------------------

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

## clear host

This command deletes entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format	clear host { <i>name</i>   all}
Mode	Privileged EXEC

Parameter	Description
<i>name</i>	A particular host entry to remove. The parameter <i>name</i> ranges from 1 to 255 characters.
all	Removes all entries.

## show hosts

This command displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. The parameter *name* ranges from 1 to 255 characters. This command displays both IPv4 and IPv6 entries.

Format	show hosts [ <i>name</i> ]
Mode	User EXEC

Output	Description
Host name	Domain host name.
Default domain	Default domain name.
Default domain list	Default domain list.
Domain name lookup	DNS client enabled/disabled.

Output	Description
Number of retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry timeout period	Amount of time to wait for a response to a DNS query.
Name servers	Configured name servers.

**Example:** The following shows example CLI display output for the command:

```
(CN1601)> show hosts
```

```
Host name..... Device
Default domain..... gm.com
Default domain list..... yahoo.com, Stanford.edu,
rediff.com
Domain Name lookup..... Enabled
Number of retries..... 5
Retry timeout period..... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19
Configured host name-to-address mapping:
```

```
Host                               Addresses
-----
accounting.gm.com                  176.16.8.8
```

```
Host          Total  Elapsed  Type      Addresses
-----
www.stanford.edu    72    3      IP      171.64.14.203
```

# Dual Image Commands

---

**Introduction** FASTPATH software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced downtime when you upgrade or downgrade the software.

**delete backup** This command deletes the backup image file from the permanent storage.

Format	delete backup
Mode	Privileged EXEC

**boot system** This command activates the specified image. It will be the active image for subsequent reboots and will be loaded by the boot loader. The current active image is marked as the backup image for subsequent reboots. If the specified image does not exist on the system, this command returns an error message.

Format	boot system {active   backup}
Mode	Privileged EXEC

**show bootvar** This command displays the version information and the activation status for the current active and backup images. The command also displays any text description associated with an image. This command displays the switch activation status.

Format	show bootvar
Mode	Privileged EXEC

**filedescr** This command associates a given text description with an image. Any existing description will be replaced.



Format	<code>filedescr {active   backup} <i>text-description</i></code>
Mode	Privileged EXEC

## update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active image for subsequent reboots.

Format	<code>update bootcode</code>
Mode	Privileged EXEC

# Email Alerting and Mail Server Commands

---

## Introduction

Email Alerting is an extension of the logging system. The logging system allows you to configure a set of destinations for log messages. The feature includes email configuration, through which the log messages are sent to a configured SMTP server such that an administrator may receive the log in an email account of the administrator’s choice.

## logging email

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires. 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), info (6), or debug (7).

Default	disabled; when enabled, log messages at or above severity warning (4) are emailed
Format	logging email [ <i>severitylevel</i> ]
Mode	Global Config

## no logging email

This command disables email alerting.

Format	no logging email
Mode	Global Config

## logging email urgent

This command sets the lowest severity level at which log messages are emailed immediately in a single email message. 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), info (6), or debug (7). Specify none to indicate that log messages are collected and sent in a batch email at a specified interval.

Default	Alert (1) and emergency (0) messages are sent immediately.
Format	logging email urgent { <i>severitylevel</i>   none}
Mode	Global Config

### no logging email urgent

This command resets the urgent severity level to the default value.

Format	no logging email urgent
Mode	Global Config

### logging email message-type to-addr

This command configures the email address to which messages are sent. The message types supported are urgent, non-urgent, and both. For each supported severity level, multiple email addresses can be configured. The *to-email-addr* variable is a standard email address, for example admin@yourcompany.com. No dashes or dots can be included in the hostname in the e-mail addresses.

Format	logging email message-type {urgent  non-urgent  both} to-addr <i>to-email-addr</i>
Mode	Global Config

### no logging email message-type to-addr

This command removes the configured to-addr field of email.

Format	no logging email message-type {urgent  non-urgent  both} to-addr <i>to-email-addr</i>
Mode	Global Config

### logging email from-addr

This command configures the email address of the sender (the switch). No dashes or dots can be included in the hostname in the e-mail addresses.

Default	switch@NetApp.com
Format	logging email from-addr <i>from-email-addr</i>

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

### no logging email from-addr

This command removes the configured email source address.

Format	no logging email from-addr <i>from-email-addr</i>
Mode	Global Config

### logging email message-type subject

This command configures the subject line of the email for the specified type.

Default	For urgent messages: Urgent Log Messages For non-urgent messages: Non Urgent Log Messages
Format	logging email message-type {urgent  non-urgent  both} subject <i>subject</i>
Mode	Global Config

### no logging email message-type subject

This command removes the configured email subject for the specified message type and restores it to the default email subject.

Format	no logging email message-type {urgent  non-urgent  both} subject
Mode	Global Config

### logging email logtime

This command configures how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval. The valid range is every 30 to 1440 minutes.

Default	30 minutes
Format	logging email logtime <i>minutes</i>
Mode	Global Config

### no logging email logtime

This command resets the non-urgent log time to the default value.

Format	no logging email logtime
Mode	Global Config

### logging traps

This command sets the severity at which SNMP traps are logged and sent in an email. 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), info (6), or debug (7).

Default	Info (6) messages and higher are logged.
Format	logging traps <i>severitylevel</i>
Mode	Global Config

### no logging traps

This command resets the SNMP trap logging severity level to the default value.

Format	no logging traps
Mode	Global Config

### logging email test message-type

This command sends an email to the SMTP server to test the email alerting function.

Format	logging email test message-type {urgent  non-urgent  both} message-body <i>message-body</i>
Mode	Global Config

### show logging email config

This command displays information about the email alert configuration.

Format	show logging email config
Mode	Global Config

Output	Description
Email Alert Logging	The administrative status of the feature: enabled or disabled.
Email Alert From Address	The email address of the sender (the switch).
Email Alert Urgent Severity Level	The lowest severity level that is considered urgent. Messages of this type are sent immediately.
Email Alert Non Urgent Severity Level	The lowest severity level that is considered non-urgent. Messages of this type, up to the urgent level, are collected and sent in a batch email. Log messages that are less severe are not sent in an email message at all.
Email Alert Trap Severity Level	The lowest severity level at which traps are logged.
Email Alert Notification Period	The amount of time to wait between non-urgent messages.
Email Alert To Address Table	The configured email recipients.
Email Alert Subject Table	The subject lines included in urgent (Type 1) and non-urgent (Type 2) messages.
For Msg Type urgent, subject is	The configured email subject for sending urgent messages.
For Msg Type non-urgent, subject is	The configured email subject for sending non-urgent messages.

## show logging email statistics

This command displays email alerting statistics.

Format	show logging email statistics
Mode	Privileged EXEC

Output	Description
Email Alert Operation Status	The operational status of the email alerting feature.
No of Email Failures	The number of email messages that have attempted to be sent but were unsuccessful.
No of Email Sent	The number of email messages that were sent from the switch since the counter was cleared.
Time Since Last Email Sent	The amount of time that has passed since the last email was sent from the switch.

### clear logging email statistics

This command resets the email alerting statistics.

Format	clear logging email statistics
Mode	Privileged EXEC

### mail-server

This command configures the SMTP server to which the switch sends email alert messages and changes the mode to Mail Server Configuration mode. The server address can be in the IPv4, IPv6, or DNS name format.

Format	mail-server { <i>ip-address</i>   <i>ipv6-address</i>   <i>hostname</i> }
Mode	Privileged EXEC

### no mail-server

This command removes the specified SMTP server from the configuration.

Format	no mail-server { <i>ip-address</i>   <i>ipv6-address</i>   <i>hostname</i> }
Mode	Privileged EXEC

## security

This command sets the email alerting security protocol by enabling the switch to use TLS authentication with the SMTP Server. If the TLS mode is enabled on the switch but the SMTP sever does not support TLS mode, no email is sent to the SMTP server.

Default	none
Format	security {tls <sup>v</sup> 1   none}
Mode	Mail Server Config

## port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLS<sup>v</sup>1 is 465, and for no security (that is, none) it is 25. However, any nonstandard port in the range 1 to 65535 is also allowed.

Default	25
Format	port {465   25   1-65535}
Mode	Mail Server Config

## username

This command configures the login ID the switch uses to authenticate with the SMTP server.

Default	admin
Format	username <i>name</i>
Mode	Mail Server Config

## password

This command configures the password the switch uses to authenticate with the SMTP server.

Default	admin
Format	password <i>password</i>
Mode	Mail Server Config



## show mail-server config

This command displays information about the email alert configuration.

Format	show mail-server { <i>ip-address</i>   <i>hostname</i>   all} config
Mode	Privileged EXEC

Output	Description
No. of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4/IPv6 address or DNS host name of the configured SMTP server.
Email Alert Mail Server Port	The TCP port the switch uses to send email to the SMTP server
Email Alert Security Protocol	The security protocol (TLS or none) the switch uses to authenticate with the SMTP server.
Email Alert Username	The username the switch uses to authenticate with the SMTP server.
Email Alert Password	The password the switch uses to authenticate with the SMTP server.

# IP Address Conflict Commands

---

## Introduction

The commands in this section help troubleshoot IP address conflicts.

### **ip address-conflict-detect run**

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format	<code>ip address-conflict-detect run</code>
Mode	Global Config

### **show ip address-conflict**

This command displays the status information corresponding to the last detected address conflict.

Format	<code>show ip address-conflict</code>
Modes	◆ Privileged EXEC ◆ User EXEC

Output	Description
Address Conflict Detection Status	Identifies whether the switch has detected an address conflict on any IP address.
Last Conflicting IP Address	The IP address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes, and seconds since the last address conflict was detected.

### **clear ip address-conflict-detect**

This command clears the detected address conflict status information.

Format	<code>clear ip address-conflict-detect</code>
Modes	◆ Privileged EXEC ◆ User EXEC

# Logging Commands

---

**Introduction**

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

**logging buffered**

This command enables logging to an in-memory log that keeps up to 128 logs.

Default	disabled; critical when enabled
Format	logging buffered
Mode	Global Config

**no logging buffered**

This command disables logging to an in-memory log.

Format	no logging buffered
Mode	Global Config

**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

**no logging buffered 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

### logging cli-command

This command enables the CLI command logging feature, which enables the FASTPATH software to log all CLI commands entered on the system.

Default	enabled
Format	logging cli-command
Mode	Global Config

### no logging cli-command

This command disables the CLI command logging feature.

Format	no logging cli-command
Mode	Global Config

### 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), info (6), or debug (7).

Default	disabled; critical when enabled
Format	logging console [ <i>severitylevel</i> ]
Mode	Global Config

### no logging console

This command disables logging to the console.

Format	no logging console
Mode	Global Config

### logging host

This command enables logging to a host. You can configure up to eight hosts. The *ipaddr|hostname* is the IP address of the logging host. The *addresstype* indicates the type of address ipv4 or ipv6 or DNS being passed. 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), info (6), or debug (7).

Default	<ul style="list-style-type: none"> <li>◆ <code>port: 514</code></li> <li>◆ <code>severitylevel: critical (2)</code></li> </ul>
Format	<code>logging host {ipaddr hostname} addresstype [port] [severitylevel]</code>
Mode	Global Config

### logging host reconfigure

This command enables logging host reconfiguration. The *hostindex* is the Logging Host index for which to change the IP address.

Format	<code>logging host reconfigure hostindex</code>
Mode	Global Config

### logging host remove

This command disables logging to host. See “[show logging hosts](#)” on page 155 for a list of host indexes.

Format	<code>logging host remove hostindex</code>
Mode	Global Config

### 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. The default is 514.

Default	514
Format	<code>logging port portid</code>
Mode	Global Config

### no logging port

This command resets the local logging port to the default.

Format	no logging port
Mode	Global Config

## logging syslog

This command enables syslog logging. The *portid* parameter is an integer with a range of 1 to 65535.

Default	disabled
Format	logging syslog [port <i>portid</i> ]
Mode	Global Config

## no logging syslog

This command disables syslog logging.

Format	no logging syslog
Mode	Global Config

## show logging

This command displays logging configuration information.

Format	show logging
Mode	Privileged EXEC

Output	Description
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
CLI Command Logging	Shows whether CLI command logging is enabled.
Console Logging	Shows whether console logging is enabled.

Output	Description
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	Shows whether buffered logging is enabled.
Syslog Logging	Shows whether syslog logging is enabled.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

### show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format	show logging buffered
Mode	Privileged EXEC

Output	Description
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In-Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

### show logging hosts

This command displays all configured logging hosts.

Format	show logging hosts
Mode	Privileged EXEC

Output	Description
Host Index	(Used for deleting hosts.)
IP Address / Hostname	IP address or hostname of the logging host.
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	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.

## show logging traplogs

This command displays SNMP trap events and statistics.

Output	Description
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.



# Serviceability Packet Tracing Commands

---

Introduction

These commands improve the capability of diagnosing conditions affecting FASTPATH.

Attention

The output of debug commands can be long and may adversely affect system performance.

debug clear

This command disables all previously enabled “debug” traces.

Default	disabled
Format	debug clear
Mode	Privileged EXEC

debug console

This command enables the display of “debug” trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default	disabled
Format	debug console
Mode	Privileged EXEC

no debug console

This command disables the display of “debug” trace output on the login session in which it is executed.

Format	no debug console
Mode	Privileged EXEC

**debug dhcp packet** This command displays “debug” information about DHCPv4 client activities and traces DHCPv4 packets to and from the local DHCPv4 client.

Default	disabled
Format	debug dhcp packet [transmit   receive]
Mode	Privileged EXEC

**no debug dhcp packet** This command disables the display of “debug” trace output for DHCPv4 client activity.

Format	no debug dhcp packet [transmit   receive]
Mode	Privileged EXEC

**debug dot1x packet** This command enables dot1x packet debug trace on the transmit or receive path.

Default	disabled
Format	debug dot1x packet [transmit receive]
Mode	Privileged EXEC

**no debug dot1x packet** This command disables dot1x packet debug trace.

Format	no debug dot1x packet
Mode	Privileged EXEC

**debug igmpsnooping packet** This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default	disabled
Format	debug igmpsnooping packet

Mode	Privileged EXEC
------	-----------------

### no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format	no debug igmpsnooping packet
Mode	Privileged EXEC

### debug igmpsnooping packet transmit

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	debug igmpsnooping packet transmit
Mode	Privileged EXEC

A sample output of the trace message is shown in this example:

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMP Snoop[185429992]:
igmp_snooping_debug.c(116) 908 % Pkt TX - Intf: 1/0/20(20),
Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01
Src_IP: 9.1.1.1 Dest_IP: 225.0.0.1 Type: V2_Membership_Report
Group: 225.0.0.1
```

The following parameters are displayed in the trace message:

Output	Description
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. The format used is slot/port (internal interface number). The unit is always shown as 1 for interfaces on a nonstacking device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.

Output	Description
Dest_IP	The destination multicast IP address in the packet.
Type	<p>The type of IGMP packet. Type can be one of the following:</p> <ul style="list-style-type: none"> <li>◆ Membership Query – IGMP Membership Query</li> <li>◆ V1_Membership_Report – IGMP Version 1 Membership Report</li> <li>◆ V2_Membership_Report – IGMP Version 2 Membership Report</li> <li>◆ V3_Membership_Report – IGMP Version 3 Membership Report</li> <li>◆ V2_Leave_Group – IGMP Version 2 Leave Group</li> </ul>
Group	Multicast group address in the IGMP header.

### no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format	no debug igmpsnooping transmit
Mode	Privileged EXEC

### debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	debug igmpsnooping packet receive
Mode	Privileged EXEC

A sample output of the trace message is shown in this example:

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMP Snoop [185429992]:
igmp_snooping_debug.c(116) 908 % Pkt RX - Intf: 1/0/20(20),
Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05
```

Src\_IP: 11.1.1.1 Dest\_IP: 225.0.0.5 Type: Membership\_Query Group: 225.0.0.5

The following parameters are displayed in the trace message:

Output	Description
RX	A packet received by the device.
Intf	The interface that the packet went out on. The format used is slot/port (internal interface number). The unit is always shown as 1 for interfaces on a nonstacking device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.
Dest_IP	The destination multicast IP address in the packet.
Type	The type of IGMP packet. Type can be one of the following: <ul style="list-style-type: none"><li>◆ Membership_Query – IGMP Membership Query</li><li>◆ V1_Membership_Report – IGMP Version 1 Membership Report</li><li>◆ V2_Membership_Report – IGMP Version 2 Membership Report</li><li>◆ V3_Membership_Report – IGMP Version 3 Membership Report</li><li>◆ V2_Leave_Group – IGMP Version 2 Leave Group</li></ul>
Group	Multicast group address in the IGMP header.

### **no debug igmpsnooping packet receive**

This command disables tracing of received IGMP Snooping packets.

Format	no debug igmpsnooping packet receive
Mode	Privileged EXEC

## debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/ serviceport for switching packages. For routing packages, pings are traced on the routing ports as well.

Default	disabled
Format	debug ping packet
Mode	Privileged EXEC

A sample output of the trace message is shown in the following example:

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]:  
sim_debug.c(128) 20 % Pkt TX - Intf: 1/0/1(1),  
SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST
```

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]:  
sim_debug.c(82) 21 % Pkt RX - Intf: 1/0/1(1), S  
RC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

Output	Description
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. The format used is slot/port (internal interface number). Unit is always shown as 1 for interfaces on a nonstacking device.
SRC_IP	The source IP address in the IP header in the packet.
DEST_IP	The destination IP address in the IP header in the packet.
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

## no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format	no debug ping packet
--------	----------------------

Mode	Privileged EXEC
------	-----------------

### debug spanning-tree bpd

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Default	disabled
Format	debug spanning-tree bpd [receive transmit]
Mode	Privileged EXEC

### no debug spanning-tree bpd

This command disables tracing of spanning tree BPDUs.

Format	no debug spanning-tree bpd
Mode	Privileged EXEC

### debug spanning-tree bpd receive

This command enables tracing of spanning tree BPDUs received by the switch. The spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default	disabled
Format	debug spanning-tree bpd receive
Mode	Privileged EXEC

A sample output of the trace message is shown in the following example:

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]:
dot1s_debug.c(1249) 101 % Pkt RX - Intf: 1/0/9(9), Source_Mac:
00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root
Priority: 0x8000 Path Cost: 0
```

The following parameters are displayed in the trace message:

Output	Description
RX	A packet received by the device.

Output	Description
Intf	The interface that the packet came in on. The format used is slot/port (internal interface number). The unit is always shown as 1 for interfaces on a nonstacking device.
Source_Mac	The Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root Mac	MAC address of the CIST root bridge.
Root Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path Cost	External root path cost component of the BPDU.

### no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format	no debug spanning-tree bpdu receive
Mode	Privileged EXEC

### debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. The spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default	enabled
Format	debug spanning-tree bpdu transmit
Mode	Privileged EXEC

A sample output of the trace message is shown in the following example:

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]:
dot1s_debug.c(1249) 101 % Pkt TX - Intf: 1/0/7(7), Source_Mac:
00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00,
Root_Priority: 0x8000 Path_Cost: 0
```



The following parameters are displayed in the trace message:

Output	Description
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. The format used is slot/port (internal interface number). The unit is always shown as 1 for interfaces on a nonstacking device.
Source_MAC	The Source MAC address of the packet.
Version	The spanning tree protocol version (0 to 3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

### no debug spanning-tree bpdud transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format	no debug spanning-tree bpdud transmit
Mode	Privileged EXEC

### logging persistent

This command configures the persistent logging for the switch. The severity level of logging messages is specified at severity level. Possible values for severity level are emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7.

Default	disabled
Format	logging persistent severity level
Mode	Global Config

### **no logging persistent**

This command disables the persistent logging in the switch.

Format	no logging persistent
Mode	Global Config

### **show debugging**

Use this command to display enabled packet tracing configurations.

Format	show debugging
Mode	Privileged EXEC

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#debug arp  
Arp packet tracing enabled.
```

```
(CN1601)# show debugging  
Arp packet tracing enabled.
```

### **no show debugging**

Use this command to disable packet tracing configurations.

Format	no show debugging
Mode	Privileged EXEC

# Simple Network Time Protocol Commands

---

Introduction	This section describes the commands you use to automatically configure the system time and date by using Simple Network Time Protocol (SNTP).						
<b>sntp broadcast client poll-interval</b>	<p>This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where <i>poll-interval</i> can be a value from 6 to 16. The default is 6 seconds.</p> <table><tr><td>Default</td><td>6</td></tr><tr><td>Format</td><td>sntp broadcast client poll-interval <i>poll-interval</i></td></tr><tr><td>Mode</td><td>Global Config</td></tr></table>	Default	6	Format	sntp broadcast client poll-interval <i>poll-interval</i>	Mode	Global Config
Default	6						
Format	sntp broadcast client poll-interval <i>poll-interval</i>						
Mode	Global Config						
<b>no sntp broadcast client poll-interval</b>	<p>This command resets the poll interval for SNTP broadcast client back to the default value.</p> <table><tr><td>Format</td><td>no sntp broadcast client poll-interval</td></tr><tr><td>Mode</td><td>Global Config</td></tr></table>	Format	no sntp broadcast client poll-interval	Mode	Global Config		
Format	no sntp broadcast client poll-interval						
Mode	Global Config						
<b>sntp client mode</b>	<p>This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.</p> <table><tr><td>Default</td><td>disabled</td></tr><tr><td>Format</td><td>sntp client mode [<i>broadcast   unicast</i>]</td></tr><tr><td>Mode</td><td>Global Config</td></tr></table>	Default	disabled	Format	sntp client mode [ <i>broadcast   unicast</i> ]	Mode	Global Config
Default	disabled						
Format	sntp client mode [ <i>broadcast   unicast</i> ]						
Mode	Global Config						
<b>no sntp client mode</b>	<p>This command disables Simple Network Time Protocol (SNTP) client mode.</p> <table><tr><td>Format</td><td>no sntp client mode</td></tr></table>	Format	no sntp client mode				
Format	no sntp client mode						

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

### **sntp client port**

This command sets the SNTP client port ID to a value from 1 to 65535. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying operating system.

Default	0
Format	<code>sntp client port <i>portid</i></code>
Mode	Global Config

### **no sntp client port**

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

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

### **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. The default is 6 seconds.

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

### **no sntp unicast client poll-interval**

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

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

**sntp unicast client  
poll-timeout**

This command will set the poll timeout for SNTP unicast clients, in seconds, to a value from 1 to 30. The default is 5 seconds.

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

**no sntp unicast  
client poll-timeout**

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

Format	no sntp unicast client poll-timeout
Mode	Global Config

**sntp unicast client  
poll-retry**

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10. The default is 1 retry.

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

**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

**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. The default is 6 seconds.

Default	6
---------	---

Format	<code>sntp multicast client poll-interval <i>poll-interval</i></code>
Mode	Global Config

### **no sntp multicast client poll-interval**

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

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

### **sntp server**

This command configures an SNTP server (a maximum of three). The server address can be either an IPv4 address or an IPv6 address. The optional priority can be a value of 1 to 3, the version a value of 1 to 4, and the port ID a value of 1 to 65535.

Format	<code>sntp server {<i>ipaddress</i>   <i>ipv6address</i>   <i>hostname</i>} [<i>priority</i> [<i>version</i> [<i>portid</i>]]]</code>
Mode	Global Config

### **no sntp server**

This command deletes a server from the configured SNTP servers.

Format	<code>no sntp server remove {<i>ipaddress</i>   <i>ipv6address</i>   <i>hostname</i>}</code>
Mode	Global Config

### **show sntp**

This command is used to display SNTP settings and status.

Format	<code>show sntp</code>
Mode	Privileged EXEC

Output	Description
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.

## show sntp client

This command displays SNTP client settings.

Format	show sntp client
Mode	Privileged EXEC

Output	Description
Client Supported Modes	Supported SNTP modes (Broadcast, Unicast, or Multicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP client port. The field displays the value 0 if it is the default value. When the client port value is 0, if the client is in broadcast mode, it binds to port 123; if the client is in unicast mode, it binds to the port assigned by the underlying operating system.
Client Mode	Configured SNTP Client Mode.

**show sntp server**

This command displays SNTP server settings and configured servers.

Format	show sntp server
Mode	Privileged EXEC

Output	Description
Server IP Address / Hostname	IP address or hostname of the configured SNTP server.
Server Type	Address type of server (IPv4, IPv6, or DNS).
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 Maximum Entries	Total number of SNTP servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Output	Description
IP Address / Hostname	IP address or hostname of the configured SNTP server.
Address Type	Address Type of configured SNTP server (IPv4, IPv6, or DNS).
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.



Output	Description
Last Update 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.

# System Information and Statistics Commands

---

**Introduction** This section describes the commands you use to view information about system features, components, and configurations.

**show arp switch** This command displays the contents of the IP stack’s Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces, which are the network or service ports. ARP entries associated with routing interfaces are not listed.

Format	show arp switch
Mode	Privileged EXEC

Output	Description
IP address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is <i>Management</i> . For a network port, the output is the slot/port of the physical interface.

**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.

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

Format	show eventlog
Mode	Privileged EXEC

Output	Description
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.

## show hardware

This command displays inventory information for the switch.

### Note

The `show version` command and the `show hardware` command display the same information. In future releases of the software, the `show hardware` command will not be available. For a description of the command output, see the command “[show version](#)” on page 175.

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

## show version

This command displays inventory information for the switch.

### Note

The `show version` command will replace the `show hardware` command in future releases of the software.

Format	<code>show version</code>
Mode	Privileged EXEC

Output	Description
System Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data.
Machine Model	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	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	The additional packages incorporated into this system.

## 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}
Mode	Privileged EXEC

The output display, when the argument is slot/port, is as follows:

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

The output display, when the argument is `switchport`, is as follows:

Output	Description
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.

Output	Description
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

## show interface ethernet

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

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

When you specify a value for slot/port, the command displays the following information:

Output	Description
Packets Received	<ul style="list-style-type: none"> <li>◆ Total Packets Received (Octets) - 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.</li> <li>◆ 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).</li> <li>◆ 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).</li> </ul>

Output	Description
	<ul style="list-style-type: none"> <li>◆ 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).</li> <li>◆ 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).</li> <li>◆ 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).</li> <li>◆ 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).</li> <li>◆ Packets Received &gt; 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.</li> </ul> <ul style="list-style-type: none"> <li>◆ Packets RX and TX 64 Octets - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).</li> <li>◆ Packets RX and TX 65-127 Octets - The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</li> <li>◆ Packets RX and TX 128-255 Octets - The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</li> </ul>



Output	Description
Packets Received (con't)	<ul style="list-style-type: none"> <li>◆ Packets RX and TX 256-511 Octets - The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</li> <li>◆ Packets RX and TX 512-1023 Octets - The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).</li> <li>◆ Packets RX and TX 1024-1518 Octets - The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).</li> <li>◆ Packets RX and TX 1519-1522 Octets - The total number of packets (including bad packets) received and transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).</li> <li>◆ Packets RX and TX 1523-2047 Octets - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.</li> <li>◆ Packets RX and TX 2048-4095 Octets - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.</li> <li>◆ Packets RX and TX 4096-9216 Octets - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.</li> </ul>

Output	Description
Packets Received Successfully	<ul style="list-style-type: none"> <li>◆ Total Packets Received Without Error - The total number of packets received that were without errors.</li> <li>◆ Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.</li> <li>◆ 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.</li> <li>◆ 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.</li> </ul>

Output	Description
Packets Received with MAC Errors	<ul style="list-style-type: none"> <li>◆ Total - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</li> <li>◆ 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.</li> <li>◆ Fragments/Undersize Received - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).</li> <li>◆ 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.</li> <li>◆ 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.</li> <li>◆ Overruns - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.</li> </ul>

Output	Description
Received Packets Not Forwarded	<ul style="list-style-type: none"> <li>◆ Total - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process</li> <li>◆ Local Traffic Frames - The total number of frames dropped in the forwarding process because the destination address was located off of this port.</li> <li>◆ 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.</li> <li>◆ Unacceptable Frame Type - The number of frames discarded from this port due to being an unacceptable frame type.</li> <li>◆ 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.</li> <li>◆ 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.</li> <li>◆ Broadcast Storm Recovery - The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.</li> <li>◆ CFI Discards - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.</li> <li>◆ Upstream Threshold - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.</li> </ul>

Output	Description
Packets Transmitted Octets	<ul style="list-style-type: none"> <li>◆ 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.</li> <li>◆ 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).</li> <li>◆ 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).</li> <li>◆ 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).</li> <li>◆ 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).</li> <li>◆ 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).</li> <li>◆ 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).</li> <li>◆ Max Frame Size - The maximum size of the Info (non-MAC) field that this port will receive or transmit.</li> </ul>

Output	Description
Packets Transmitted Successfully	<ul style="list-style-type: none"> <li>◆ Total - The number of frames that have been transmitted by this port to its segment.</li> <li>◆ 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.</li> <li>◆ 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.</li> <li>◆ 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.</li> </ul>
Transmit Errors	<ul style="list-style-type: none"> <li>◆ Total Errors - The sum of Single, Multiple, and Excessive Collisions.</li> <li>◆ 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.</li> <li>◆ 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.</li> <li>◆ Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.</li> </ul>

Output	Description
Transmit Discards	<ul style="list-style-type: none"> <li>◆ Total Discards - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.</li> <li>◆ 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.</li> <li>◆ 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.</li> <li>◆ Excessive Collisions - A count of frames for which transmission on a particular interface fails due to excessive collisions.</li> <li>◆ Port Membership Discards - The number of frames discarded on egress for this port due to egress filtering being enabled.</li> </ul>

Output	Description
Protocol Statistics	<ul style="list-style-type: none"> <li>◆ 802.3x Pause Frames Transmitted - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.</li> <li>◆ GVRP PDUs Received - The count of GVRP PDUs received in the GARP layer.</li> <li>◆ GVRP PDUs Transmitted - The count of GVRP PDUs transmitted from the GARP layer.</li> <li>◆ GVRP Failed Registrations - The number of times attempted GVRP registrations could not be completed.</li> <li>◆ GMRP PDUs Received - The count of GMRP PDUs received in the GARP layer.</li> <li>◆ GMRP PDUs Transmitted - The count of GMRP PDUs transmitted from the GARP layer.</li> <li>◆ GMRP Failed Registrations - The number of times attempted GMRP registrations could not be completed.</li> <li>◆ STP BPDUs Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>◆ STP BPDUs Received - Spanning Tree Protocol Bridge Protocol Data Units received.</li> <li>◆ RST BPDUs Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>◆ RSTP BPDUs Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received.</li> <li>◆ MSTP BPDUs Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>◆ MSTP BPDUs Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.</li> </ul>
Dot1x Statistics	<ul style="list-style-type: none"> <li>◆ EAPOL Frames Received - The number of valid EAPOL frames of any type that have been received by this authenticator.</li> <li>◆ EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.</li> </ul>



Output	Description
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 use the *switchport* keyword, the following information appears:

Output	Description
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.

Output	Description
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.

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

## show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter the `all` parameter to display the entire table. Enter a MAC address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the `count` parameter to view summary information about the forwarding database table. Use the `interface slot/port` parameter to view MAC addresses on a specific interface. Use the `vlan vlan_id` parameter to display information about MAC addresses on a specified VLAN.

Format	<code>show mac-addr-table [{macaddr vlan_id   all   count   interface slot/port   vlan vlan_id}]</code>
Mode	Privileged EXEC

The following information displays if you do not enter a parameter, the keyword `all`, or the MAC address and VLAN ID:

Output	Description
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is six 2-digit hexadecimal numbers that are separated by colons, for example: 01:23:45:67:89:AB.
Interface	The port through which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.

Output	Description
Status	<p>The status of this entry. The meanings of the values are:</p> <ul style="list-style-type: none"> <li>◆ <b>Static</b>—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be releamed.</li> <li>◆ <b>Learned</b>—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.</li> <li>◆ <b>Management</b>—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing.</li> <li>◆ <b>Self</b>—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address).</li> <li>◆ <b>GMRP Learned</b>—The value of the corresponding was learned via GMRP and applies to Multicast.</li> <li>◆ <b>Other</b>—The value of the corresponding instance does not fall into one of the other categories.</li> </ul>

If you enter `vlan vlan_id`, only the MAC Address, Interface, and Status fields appear. If you enter the `interface slot/port` parameter, in addition to the MAC Address and Status fields, the VLAN ID field also appears.

The following information displays if you enter the `count` parameter:

Output	Description
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user.

Output	Description
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle.

### process cpu threshold type total rising

This command configures CPU Utilization monitoring threshold parameters.

Format	show process cpu threshold type total rising 1-100 interval 5-86400 falling 1-100 interval 5-86400
Mode	Privileged EXEC

### show process cpu

This command provides the percentage utilization of the CPU by different tasks.

#### Note

It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

#### Note

This command is available in VxWorks and Linux 2.6 only.

Format	show process cpu
Mode	Privileged EXEC

**Example:** The following shows example CLI display output for the command using Linux:

```
(CN1601) #show process cpu
Memory Utilization Report
status      bytes
-----
free       106450944
alloc      423227392

CPU Utilization:
```

PID	Name	5 Secs	60 Secs	300 Secs
765	_interrupt_thread	0.00%	0.01%	0.02%
767	bcmL2X.0	0.58%	0.35%	0.28%
768	bcmCNTR.0	0.77%	0.73%	0.72%
773	bcmRX	0.00%	0.04%	0.05%
786	cpuUtilMonitorTask	0.19%	0.23%	0.23%
834	dot1s_task	0.00%	0.01%	0.01%
810	hapiRxTask	0.00%	0.01%	0.01%
805	dt1Task	0.00%	0.02%	0.02%
863	spmTask	0.00%	0.01%	0.00%
894	ip6MapLocalDataTask	0.00%	0.01%	0.01%
908	RMONTask	0.00%	0.11%	0.12%
Total CPU Utilization		1.55%	1.58%	1.50%

**Example:** The following shows example CLI display output for the command using VxWorks:

```
(CN1601)#show process cpu
```

Memory Utilization Report

status bytes

free 192980480

alloc 53409968

Task Utilization Report

Task Utilization

```
-----
bcmL2X.0          0.75%
bcmCNTR.0         0.20%
bcmLINK.0         0.35%
DHCP snoop        0.10%
Dynamic ARP Inspection 0.10%
dot1s_timer_task  0.10%
dhcpsPingTask     0.20%
```

## show running-config

This command displays or captures the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the all option.

---

**Note**

The `show running-config` command does not display the User Password, even if you set one different from the default.

---

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.

---

**Note**

If you enter the `show running-config` command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

---

---

**Note**

If you use a text-based configuration file, the `show running-config` command will only display configured physical interfaces, for example, if any interface only contains the default configuration, then that interface will be skipped from the `show running-config` command output. This is true for any configuration mode that contains nothing but the default configuration. That is, the command to enter a particular config mode, followed immediately by its exit command, are both omitted from the `show running-config` command output (and hence from the startup-config file when the system configuration is saved.)

---

Format	<code>show running-config [all   <i>scriptname</i>]</code>
Mode	Privileged EXEC

## show sysinfo

This command displays switch information.

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

Output	Description
Switch Description	Text used to identify this switch.

Output	Description
System Name	Name used to identify the switch. The factory default is blank. To configure the system name, see “ <a href="#">snmp-server</a> ” on page 67.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see “ <a href="#">snmp-server</a> ” on page 67.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see “ <a href="#">snmp-server</a> ” on page 67.
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.

## show tech-support

Use the `show tech-support` command to display system and configuration information when you contact technical support. The output of the `show tech-support` command combines the output of the following commands:

- ◆ `show version`
- ◆ `show sysinfo`
- ◆ `show port all`
- ◆ `show isdp neighbors`
- ◆ `show logging`
- ◆ `show event log`
- ◆ `show logging buffered`
- ◆ `show trap log`
- ◆ `show running config`

Format	<code>show tech-support</code>
Mode	Privileged EXEC



## terminal length

This command sets the number of lines of output to be displayed on the screen, that is, pagination, for the `show running-config` and `show running-config all` commands. The terminal length size is either 0 (zero) or a number in the range of 5 to 48. After the user-configured number of lines is displayed in one page, the system prompts the user for `--More--` or `(q)uit`. Press `q` or `Q` to quit, or press any key to display the next set of 5 to 48 lines. The command `terminal length 0` disables pagination and, as a result, the output of the `show running-config` command is displayed immediately.

Default	24 lines per page
Format	<code>terminal length 0/5-48</code>
Mode	Privileged EXEC

## no terminal length

This command sets the terminal length to the default value.

Format	<code>no terminal length</code>
Mode	Privileged EXEC

## show terminal length

This command displays the value of the user-configured terminal length size.

Format	<code>show terminal length</code>
Mode	Privileged EXEC

# System Utility and Clear Commands

## Introduction

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

## traceroute

This command finds the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The `traceroute` command continues to provide a synchronous response when initiated from the CLI.

Default	<ul style="list-style-type: none"><li>◆ count: 3 probes</li><li>◆ interval: 3 seconds</li><li>◆ size: 0 bytes</li><li>◆ port: 33434</li><li>◆ maxTtl: 30 hops</li><li>◆ maxFail: 5 probes</li><li>◆ initTtl: 1 hop</li></ul>
Format	<code>traceroute {ipaddr hostname} [initTtl initTtl] [maxTtl maxTtl] [maxFail maxFail] [interval interval] [count count] [port port] [size size]</code>
Mode	Privileged EXEC

Using the following options, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	Description
<i>ipaddr/hostname</i>	The <i>ipaddr</i> value should be a valid IP address. The <i>hostname</i> value should be a valid hostname.

Parameter	Description
initTtl	Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use maxTtl to specify the maximum TTL. The range is 1 to 255.
maxFail	Use maxFail to terminate the traceroute after failing to receive a response for this number of consecutive probes. The range is 0 to 255.
interval	If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. The range is 1 to 60 seconds.
count	Use this optional parameter to specify the number of probes to send for each TTL value. The range is 1 to 10 probes.
port	Use this optional parameter to specify the destination UDP port of the probe. This should be an unused port on the remote destination system. The range is 1 to 65535.
size	Use this optional parameter to specify the size, in bytes, of the payload of the Echo Requests sent. The range is 0 to 65507 bytes.

The following are examples that use the traceroute command:

Example of a successful traceroute:

```
(CN1601)# traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0
interval 1 count 3 port 33434 size 43
Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1    708 msec    41 msec    11 msec
2 10.240.10.115  0 msec      0 msec      0 msec
```

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6

Example of a traceroute failure:

```
(CN1601)# traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count
3
port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
 1 10.240.4.1    19 msec      18 msec      9 msec
 2 10.240.1.252  0 msec       0 msec       1 msec
 3 172.31.0.9    277 msec     276 msec     277 msec
 4 10.254.1.1    289 msec     327 msec     282 msec
 5 10.254.21.2   287 msec     293 msec     296 msec
 6 192.168.76.2  290 msec     291 msec     289 msec
 7 0.0.0.0       0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

traceroute ipv6

Use this command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The `{ipv6-address | hostname}` parameter must be a valid IPv6 address or hostname. 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. The range for `port` is zero (0) to 65535. The default value is 33434.

Default	port: 33434
Format	traceroute ipv6 { <i>ipv6-address   hostname</i> } [ <i>port port</i> ]
Mode	Privileged EXEC

clear config

This command resets the configuration to the factory defaults without powering off the switch. When you enter this command, a prompt appears to confirm that the reset should proceed. When you enter `y`, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Format	clear config
Mode	Privileged EXEC

## 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

## 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

## clear pass

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

Format	clear pass
Mode	Privileged EXEC

## clear traplog

This command clears the trap log.

Format	clear traplog
Mode	Privileged EXEC

## clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format	clear vlan
Mode	Privileged EXEC

logout

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

**Note** Save the configuration changes before logging out.

Format	logout
Mode	◆ Privileged EXEC ◆ User EXEC

ping

This command determines whether another computer is on the network. It provides a synchronous response when initiated from the CLI and Web interfaces.

Default	◆ The default count is 1. ◆ The default interval is 3 seconds. ◆ The default size is 0 bytes.
Format	ping { <i>ipaddress</i>   <i>hostname</i> }[count <i>count</i> ] [interval <i>interval</i> ] [size <i>size</i> ]
Mode	◆ Privileged EXEC ◆ User EXEC

Using the following options, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Description
count	Use this parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the ip-address field. The range for count is 1 to 15 requests.
interval	Use this parameter to specify the time between Echo Requests, in seconds. The range is 1 to 60 seconds.

Parameter	Description
size	Use this parameter to specify the size, in bytes, of the payload of the Echo Requests sent. The range is 0 to 65507 bytes.

The following are examples that use the ping command.

Example of a successful ping:

```
(CN1601) #ping 10.254.2.160 count 3 interval 1 size 255
```

Pinging 10.254.2.160 with 255 bytes of data:

```
Received response for icmp_seq = 0. time = 275268 usec
```

```
Received response for icmp_seq = 1. time = 274009 usec
```

```
Received response for icmp_seq = 2. time = 279459 usec
```

```
----10.254.2.160 PING statistics----
```

```
3 packets transmitted, 3 packets received, 0% packet loss
```

```
round-trip (msec) min/avg/max = 274/279/276
```

Example of a ping failure:

Unreachable Destination:

```
(CN1601)# ping 192.168.254.222 count 3 interval 1 size 255
```

Pinging 192.168.254.222 with 255 bytes of data:

```
Received Response: Unreachable Destination
```

```
Received Response :Unreachable Destination
```

```
Received Response :Unreachable Destination
```

```
----192.168.254.222 PING statistics----
```

```
3 packets transmitted,3 packets received, 0% packet loss
```

```
round-trip (msec) min/avg/max = 0/0/0
```

Request Timed Out example:

```
(CN1601)# ping 1.1.1.1 count 1 interval 3
```

Pinging 1.1.1.1 with 0 bytes of data:

```
----1.1.1.1 PING statistics----
```

```
1 packets transmitted,0 packets received, 100% packet loss
```

```
round-trip (msec) min/avg/max = 0/0/0
```

## quit

This command closes the current Telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format	quit
Mode	◆ Privileged EXEC ◆ User EXEC

## reload

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

Format	reload
Mode	Privileged EXEC

## copy

This command uploads and downloads files to and from the switch. You can also use the `copy` command to manage the dual images (active and backup) on the file system. Upload and download files from a server by using TFTP or Xmodem.

Format	<i>copy source destination</i>
Mode	Privileged EXEC

Replace the *source* and *destination* parameters with the options in the following Source/Destination/Description table. For the *url* source or destination, use the following value:

```
{xmodem | tftp://ipaddr|hostname |  
ip6address|hostname/filepath/filename [noval]}
```

---

### Note

The maximum length for the file path is 160 characters, and the maximum length for the file name is 32 characters.

---



For TFTP, SFTP and SCP, the *ipaddr/hostname* parameter is the IP address or host name of the server, *filepath* is the path to the file, and *filename* is the name of the file you want to upload or download. For SFTP and SCP, the *username* parameter is the username for logging into the remote server via SSH.

#### Note

*ip6address* is also a valid parameter for routing packages that support IPv6.

#### CAUTION

Remember to upload the existing *fastpath.cfg* file off the switch prior to loading a new release image in order to make a backup.

Source	Destination	Description
<code>nvram:backup-config</code>	<code>nvram:startup-config</code>	Copies the backup configuration to the startup configuration.
<code>nvram:clibanner</code>	<i>url</i>	Copies the CLI banner to a server.
<code>nvram:errorlog</code>	<i>url</i>	Copies the error log file to a server.
<code>nvram:fastpath.cfg</code>	<i>url</i>	Uploads the binary config file to a server.
<code>nvram:log</code>	<i>url</i>	Copies the log file to a server.
<code>nvram:script scriptname</code>	<i>url</i>	Copies a specified configuration script file to a server.
<code>nvram:startup-config</code>	<code>nvram:backup-config</code>	Copies the startup configuration to the backup configuration.
<code>nvram:startup-config</code>	<i>url</i>	Copies the startup configuration to a server.
<code>nvram:traplog</code>	<i>url</i>	Copies the trap log file to a server.
<code>system:running-config</code>	<code>nvram:startup-config</code>	Saves the running configuration to nvram.
<i>url</i>	<code>nvram:clibanner</code>	Downloads the CLI banner to the system.
<i>url</i>	<code>nvram:fastpath.cfg</code>	Downloads the binary configuration file to the system.

Source	Destination	Description
<i>url</i>	<i>nvram:script destfilename</i>	Downloads a configuration script file to the system. During the download of a configuration script, the <code>copy</code> 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.
<i>url</i>	<i>nvram:script destfilename noval</i>	When you use this option, the <code>copy</code> command will not validate the downloaded script file. An example of the CLI command follows:  <pre>(CN1601)#copy tftp://1.1.1.1/file.scr nvram:script file.scr noval</pre> <pre>(CN1601)#copy tftp://1.1.1.1/file.scr nvram:script file.scr noval</pre>
<i>url</i>	<i>nvram:sshkey- dsa</i>	Downloads an SSH key file. For more information, see “ <a href="#">Secure Shell Commands</a> ” on page 64.
<i>url</i>	<i>nvram:sshkey- rsa1</i>	Downloads an SSH key file.
<i>url</i>	<i>nvram:sshkey- rsa2</i>	Downloads an SSH key file.
<i>url</i>	<i>nvram:startup- config</i>	Downloads the startup configuration file to the system.
<i>url</i>	<i>nvram:system- image</i>	Downloads a code image to the system.
<i>url</i>	<i>kernel</i>	Downloads a code file to the system.
<i>url</i>	<i>ias-users</i>	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user’s database is replaced with the users and their attributes available in the downloaded file.
<i>url</i>	<i>{active   backup}</i>	Downloads an image from the remote server to either image.

Source	Destination	Description
{active   backup}	url	Uploads either image to the remote server.
active	backup	Copies the active image to the backup image.
backup	active	Copies the backup image to the active image.

## environment temprange

This command sets the allowed temperature range for normal operations.

Format	environment temprange min -100-100 max -100-100
Mode	Global Config

Parameter	Description
min	Minimum allowed temperature for normal operation. The value is within the range -100 to 100 degrees Fahrenheit.
max	Maximum allowed temperature for normal operation. The value is within the range -100 to 100 degrees Fahrenheit.

## environment trap fan

This command enables the fan status trap.

Format	environment trap fan
Mode	Global Config

## environment trap powersupply

This command enables the power supply status trap.

Format	environment trap powersupply
--------	------------------------------

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

## environment trap temperature

This command enables the temperature status trap.

Format	environment trap temperature
Mode	Global Config

## show environment

This command displays vital environment status data.

Format	show environment
Mode	Privileged EXEC

## slot

This command configures a slot in the system. The slot/port is the slot identifier of the slot. The *cardindex* is the index into the database of the supported card types, indicating the type of card being preconfigured in the specified slot. The card index is a 32-bit integer. If a card is currently present in the slot that is unconfigured, the configured information will be deleted and the slot will be reconfigured with default information for the card.

Format	slot slot/port <i>cardindex</i>
Mode	Global Config

### Note

You can get the *cardindex* by entering the show supported cardtype command in User EXEC mode.

## no slot

This command removes configured information from an existing slot in the system.

Format	no slot slot/port <i>cardindex</i>
Mode	Global Config

---

**Note**

You can get the *cardindex* by entering the `show supported cardtype` command in User EXEC mode.

---

**set slot disable**

This command configures the administrative mode of the slot(s). If you specify `[all]`, the command is applied to all slots, otherwise the command is applied to the slot identified by slot/port.

If a card or other module is present in the slot, the administrative mode will effectively be applied to the contents of the slot. If the slot is empty, the administrative mode will be applied to any module that is inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as unplugged on management screens.

Format	<code>set slot disable [slot/port]   all</code>
Mode	Global Config

**no set slot disable**

This command unconfigures the administrative mode of the slot(s). If you specify `[all]`, the command removes the configuration from all slots, otherwise the configuration is removed from the slot identified by slot/port.

Format	<code>no set slot disable [slot/port]   all</code>
Mode	Global Config

**set slot power**

This command configures the power mode of the slot(s), and allows power to be supplied to a card located in the slot. If you specify `all`, the command is applied to all slots, otherwise the command is applied to the slot identified by slot/port.

Format	<code>set slot power [slot/port]   all</code>
Mode	Global Config

**no set slot power**

This command unconfigures the power mode of the slot(s), and prohibits power from being supplied to a card located in the slot. If you specify `all`, the command prohibits power to all slots, otherwise the command prohibits power to the slot identified by slot/port.

Format	set slot power [slot/port]   all
Mode	Global Config

**show slot**

This command displays information about all the slots in the system or for a specific slot.

Format	show slot [slot]
Mode	User EXEC

Output	Description
Slot	The slot identifier.
Slot Status	The slot is empty, full, or has encountered an error
Admin State	The slot administrative mode is enabled or disabled.
Power State	The slot power mode is enabled or disabled.
Configured Card Model Identifier	The model identifier of the card preconfigured in the slot. Model Identifier is a 32-character field used to identify a card.
Pluggable	Cards are pluggable or non-pluggable in the slot.
Power Down	Indicates whether the slot can be powered down.

If you supply a value for slot, the following additional information appears:

Output	Description
Inserted Card Model Identifier	The model identifier of the card inserted in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full.
Inserted Card Description	The card description. This field is displayed only if the slot is full.
Configured Card Description	10BASE-T half duplex.

**Example:** The following shows example CLI display output for the `show slot` command:

```
(CN1601) #show slot
```

Slot	Status	Admin State	Power State	Configured Model ID	Card Pluggable	Power Down
0	Full	Enable	Enable	BCM53716-16FE	No	No

**Example:** The following shows example CLI display output for the `show slot [slot]` command:

```
(CN1601) #show slot 0
```

```
Slot..... 0
Slot Status..... Full
Admin State..... Enable
Power State..... Enable
Inserted Card:
  Model Identifier..... BCM53716-16FE
  Card Description..... Broadcom BCM53716 - 16 Port 10GB
  Ethernet
                                Line Card
Configured Card:
  Model Identifier..... BCM53716-16FE
  Card Description..... Broadcom BCM53716 - 16 Port 10GB
  Ethernet
                                Line Card
Pluggable..... No
Power Down..... No
```

**show supported  
cardtype**

This command displays information about all card types or specific card types supported in the system.

Format	show supported cardtype [ <i>cardindex</i> ]
Mode	User EXEC

If you do not supply a value for *cardindex*, the following output appears:

Output	Description
Card Index (CID)	The index into the database of the supported card types. This index is used when preconfiguring a slot.
Card Model Identifier	The model identifier for the supported card type.

If you supply a value for *cardindex*, the following output appears:

Output	Description
Card Type	The 32-bit numeric card type for the supported card.
Model Identifier	The model identifier for the supported card type.
Card Description	The description for the supported card type.

**Example:** The following shows example CLI display output for the command:

```
(CN1601) #show supported cardtype
CID                Card Model ID
-----
3      BCM53716-16FE
```

**Example:** The following shows example CLI display output for the command when you supply a value for *cardindex*:

```
(CN1601) #show supported cardtype 3

Card Type..... 0x56820001
Model Identifier..... BCM53716-16FE
Card Description..... Broadcom BCM53716 - 16 Port 10GB
Ethernet Line Card
```



## About this chapter

This chapter describes the switching commands available in the CN1601 command line interface (CLI).

## Topics in this chapter

This chapter includes the following sections:

- ◆ “[Denial of Service Commands](#)” on page 215
- ◆ “[802.1X Supplicant Commands](#)” on page 226
- ◆ “[GARP Commands](#)” on page 231
- ◆ “[GMRP Commands](#)” on page 234
- ◆ “[GVRP Commands](#)” on page 238
- ◆ “[IGMP Snooping Configuration Commands](#)” on page 241
- ◆ “[IGMP Snooping Querier Commands](#)” on page 251
- ◆ “[ISDP Commands](#)” on page 256
- ◆ “[LLDP \(802.1AB\) Commands](#)” on page 262
- ◆ “[LLDP-MED Commands](#)” on page 273
- ◆ “[MAC Database Commands](#)” on page 281
- ◆ “[Port-Based Network Access Control Commands](#)” on page 284
- ◆ “[Port Channel/LAG \(802.3ad\) Commands](#)” on page 304
- ◆ “[Port Configuration Commands](#)” on page 324
- ◆ “[Port Mirroring Commands](#)” on page 330
- ◆ “[Port Security Commands](#)” on page 333
- ◆ “[Protected Ports Commands](#)” on page 337
- ◆ “[Provisioning \(IEEE 802.1p\) Commands](#)” on page 340
- ◆ “[Spanning Tree Protocol Commands](#)” on page 341
- ◆ “[Static MAC Filtering Commands](#)” on page 361
- ◆ “[Storm-Control Commands](#)” on page 366
- ◆ “[VLAN Commands](#)” on page 379
- ◆ “[Voice VLAN Commands](#)” on page 391

---

## CAUTION

The commands in this chapter 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.
-

# Denial of Service Commands

---

## Introduction

This section describes the commands you use to configure Denial of Service (DoS) Control. FASTPATH software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- ◆ **SIP = DIP:** Source IP address = Destination IP address.
- ◆ **First Fragment:** TCP Header size smaller than configured value.
- ◆ **TCP Fragment:** IP Fragment Offset = 1.
- ◆ **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- ◆ **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- ◆ **ICMP:** Limiting the size of ICMP Ping packets.
- ◆ **SMAC = DMAC:** Source MAC address = Destination MAC address.
- ◆ **TCP Port:** Source TCP Port = Destination TCP Port.
- ◆ **UDP Port:** Source UDP Port = Destination UDP Port.
- ◆ **TCP Flag & Sequence:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- ◆ **TCP Offset:** TCP Header Offset = 1.
- ◆ **TCP SYN:** TCP Flag SYN set.
- ◆ **TCP SYN & FIN:** TCP Flags SYN and FIN set.
- ◆ **TCP FIN & URG & PSH:** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- ◆ **ICMP V6:** Limits the size of ICMPv6 Ping packets.
- ◆ **ICMP Fragment:** Checks for fragmented ICMP packets.

## dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Format	dos-control all
Mode	Global Config

**no dos-control all**

This command disables Denial of Service prevention checks globally.

Format	no dos-control all
Mode	Global Config

**dos-control sipdip**

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control sipdip
Mode	Global Config

**no dos-control sipdip**

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format	no dos-control sipdip
Mode	Global Config

**dos-control firstfrag**

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller than the configured value, the packets will be dropped if the mode is enabled. The default is *disabled*. If you enable `dos-control firstfrag`, but do not provide a Minimum TCP Header Size, the system sets that value to 20. The Minimum TCP Header Size can range from 0 to 255.

Default	disabled (20)
Format	dos-control firstfrag [0-255]
Mode	Global Config

**no dos-control firstfrag**

This command sets Minimum TCP Header Size Denial of Service protection to the default value of *disabled*.

Format	no dos-control firstfrag
--------	--------------------------

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

### **dos-control tcpfrag**

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control tcpfrag
Mode	Global Config

### **no dos-control tcpfrag**

This command disables TCP Fragment Denial of Service protection.

Format	no dos-control tcpfrag
Mode	Global Config

### **dos-control tcpflag**

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control tcpflag
Mode	Global Config

### **no dos-control tcpflag**

This command disables TCP Flag Denial of Service protections.

Format	no dos-control tcpflag
Mode	Global Config

## **dos-control l4port**

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

### **Note**

Some applications mirror source and destination L4 ports – RIP, for example, uses 520 for both. If you enable `dos-control l4port`, applications such as RIP may experience packet loss which would render the application inoperable.

Default	disabled
Format	dos-control l4port
Mode	Global Config

## **no dos-control l4port**

This command disables L4 Port Denial of Service protections.

Format	no dos-control l4port
Mode	Global Config

## **dos-control icmp**

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	dos-control icmp 0-1023
Mode	Global Config

## **no dos-control icmp**

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	no dos-control icmp
Mode	Global Config

**dos-control  
smacdmac**

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control smacdmac
Mode	Global Config

**no dos-control  
smacdmac**

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Format	no dos-control smacdmac
Mode	Global Config

**dos-control tcpport**

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control tcpport
Mode	Global Config

**no dos-control  
tcpport**

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format	no dos-control tcpport
Mode	Global Config

**dos-control udpport**

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) DoS protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control udpport
Mode	Global Config

### **no dos-control udpport**

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format	no dos-control udpport
Mode	Global Config

### **dos-control tcpflagseq**

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control tcpflagseq
Mode	Global Config

### **no dos-control tcpflagseq**

This command disables TCP Flag and Sequence Denial of Service protection.

Format	no dos-control tcpflagseq
Mode	Global Config

### **dos-control tcpoffset**

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control tcpoffset



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

### **no dos-control tcpoffset**

This command disables TCP Offset Denial of Service protection.

Format	no dos-control tcpoffset
Mode	Global Config

### **dos-control tcpsyn**

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control tcpsyn
Mode	Global Config

### **no dos-control tcpsyn**

This command disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	no dos-control tcpsyn
Mode	Global Config

### **dos-control tcpsynfin**

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control tcpsynfin
Mode	Global Config

### **no dos-control tcpsynfin**

This command disables TCP SYN & FIN Denial of Service protection.

Format	no dos-control tcpsynfin
--------	--------------------------

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

### **dos-control tcpfinurgpsh**

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control tcpfinurgpsh
Mode	Global Config

### **no dos-control tcpfinurgpsh**

This command disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format	no dos-control tcpfinurgpsh
Mode	Global Config

### **dos-control icmpv4**

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	dos-control icmpv4 0-16384
Mode	Global Config

### **no dos-control icmpv4**

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	no dos-control icmpv4
Mode	Global Config

**dos-control icmpv6**

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	dos-control icmpv6 0-16384
Mode	Global Config

**no dos-control icmpv6**

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	no dos-control icmpv6
Mode	Global Config

**dos-control icmpfrag**

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default	disabled
Format	dos-control icmpfrag
Mode	Global Config

**no dos-control icmpfrag**

This command disables ICMP Fragment Denial of Service protection.

Format	no dos-control icmpfrag
Mode	Global Config

**show dos-control**

This command displays Denial of Service configuration information.

Format	show dos-control
Mode	Privileged EXEC

Output	Description
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0-255>	The factory default is 20.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Pkt Size	The range is 0 to 1023. The factory default is 512.
Max ICMPv6 Pkt Size	The range is 0 to 16384. The factory default is 512.
ICMP Fragment Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
TCP Port Mode	May be enabled or disabled. The factory default is disabled.
UDP Port Mode	May be enabled or disabled. The factory default is disabled.
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
SMACDMAC Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
TCP FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

Output	Description
vlan-list	The VLAN ID. Enter VLAN IDs in the range of 1 to 4093. Use a dash (–) to specify a range. Use a comma (,) to separate non-consecutive IDs in a list. Spaces and zeros are not permitted.

# 802.1X Supplicant Commands

Introduction

CN1601 supports 802.1X (dot1x) supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

dot1x pae

This command sets the port’s dot1x role. The port can serve as either a supplicant or an authenticator.

Format	dot1x pae {supplicant   authenticator}
Mode	Interface Config

dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port’s attribute needs to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

Default	auto
Format	dot1x supplicant port-control {auto   force-authorized   force_unauthorized}
Mode	Interface Config

Parameter	Description
auto	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
force-authorized	Sets the authorization state of the port to Authorized, bypassing the authentication process.

Parameter	Description
<code>force-unauthorized</code>	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

### **no dot1x supplicant port-control**

This command sets the port-control mode to the default, auto.

Format	<code>no dot1x supplicant port-control</code>
Mode	Interface Config

### **dot1x supplicant max-start**

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator.

Default	3
Format	<code>dot1x supplicant max-start &lt;1-10&gt;</code>
Mode	Interface Config

### **no dot1x supplicant max-start**

This command sets the max-start value to the default.

Format	<code>no dot1x supplicant max-start</code>
Mode	Interface Config

### **dot1x supplicant timeout start-period**

This command configures the start period timer interval to wait for the EAP identity request from the authenticator.

Default	30 seconds
Format	<code>dot1x supplicant timeout start-period &lt;1-65535 seconds&gt;</code>
Mode	Interface Config

**no dot1x supplicant  
timeout start-period**

This command sets the start-period value to the default.

Format	no dot1x supplicant timeout start-period
Mode	Interface Config

**dot1x supplicant  
timeout held-period**

This command configures the held-period timer interval to wait for the next authentication on previous authentication fail.

Default	30 seconds
Format	dot1x supplicant timeout held-period <1-65535 seconds>
Mode	Interface Config

**no dot1x supplicant  
timeout held-period**

This command sets the held-period value to the default value.

Format	no dot1x supplicant timeout held-period
Mode	Interface Config

**dot1x supplicant  
timeout auth-period**

This command configures the authentication period timer interval to wait for the next EAP request challenge from the authenticator.

Default	30 seconds
Format	dot1x supplicant timeout auth-period <1-65535 seconds>
Mode	Interface Config

**no dot1x supplicant  
timeout auth-period**

This command sets the auth-period value to the default value.

Format	no dot1x supplicant timeout auth-period
Mode	Interface Config



## dot1x supplicant user

This command maps the given user to the port.

Format	dot1x supplicant user
Mode	Interface Config

## show dot1x statistics

This command displays the dot1x port statistics in detail.

Format	show dot1x statistics <i>slot/port</i>
Mode	◆ Privileged EXEC ◆ User EXEC

Output	Description
EAPOL Frames Received	Displays the number of valid EAPOL frames received on the port.
EAPOL Frames Transmitted	Displays the number of EAPOL frames transmitted via the port.
EAPOL Start Frames Transmitted	Displays the number of EAPOL Start frames transmitted via the port.
EAPOL Logoff Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.
EAP Resp/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
EAP Response Frames Received	Displays the number of valid EAP Respond frames received on the port.
EAP Req/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.

Output	Description
EAP Req Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
EAP Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
Last EAPOL Frames Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frames Source	Displays the source MAC Address attached to the most recently received EAPOL frame.

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#show dot1x statistics 0/1
Port..... 0/1
EAPOL Frames Received..... 0
EAPOL Frames Transmitted..... 0
EAPOL Start Frames Transmitted..... 3
EAPOL Logoff Frames Received..... 0
EAP Resp/Id frames transmitted..... 0
EAP Response frames transmitted..... 0
EAP Req/Id frames transmitted..... 0
EAP Req frames transmitted..... 0
Invalid EAPOL frames received..... 0
EAP length error frames received..... 0
Last EAPOL Frame Version..... 0
Last EAPOL Frame Source..... 00:00:00:00:02:01
```

# GARP Commands

---

## Introduction

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. These commands affect both GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). 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 GVMP).

## set garp timer join

This command sets the GVRP join time per GARP for one interface, a range of interfaces, or all interfaces. The `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 default value 20 centiseconds is 0.2 seconds.

Default	20
Format	set garp timer join 10-100
Mode	◆ Interface Config ◆ Global Config

## no set garp timer join

This command sets the GVRP `join` time to the default and only has an effect when GVRP is enabled.

Format	no set garp timer join
Mode	◆ Interface Config ◆ Global Config

## set garp timer leave

This command sets the GVRP leave time for one interface, a range of interfaces, or all interfaces or all ports and only has an effect when GVRP is enabled. The 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. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds. The leave time must be greater than or equal to three times the join time.

Default	60
Format	<code>set garp timer leave 20-600</code>
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> </ul>

### **no set garp timer leave**

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format	<code>no set garp timer leave</code>
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> </ul>

### **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 default value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode), or on a single port or a range of ports (Interface Config mode) and it only has an effect only when GVRP is enabled. The leave all time must be greater than the leave time.

Default	1000
Format	<code>set garp timer leaveall 200-6000</code>
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> </ul>

### **no set garp timer leaveall**

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format	<code>no set garp timer leaveall</code>
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> </ul>

**show garp**

This command displays GARP information.

Format	show garp
Mode	◆ Privileged EXEC ◆ User EXEC

Output	Description
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

# GMRP Commands

---

Introduction

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 deregister 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.

set gmrp adminmode

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

Default	disabled
Format	set gmrp adminmode
Mode	Privileged EXEC

no set gmrp adminmode

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

Format	no set gmrp adminmode
Mode	Privileged EXEC

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode), a range of interfaces, or all interfaces (Global Config mode). 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
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> </ul>

### no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port channel (LAG), GARP functionality 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
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> </ul>

### show gmrp configuration

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

Format	show gmrp configuration {slot/port   all}
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
Interface	The slot/port of the interface that this row in the table describes.
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Output	Description
Leave Timer	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	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.

### **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

Output	Description
VLAN ID	The VLAN in which the MAC Address is learned.
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.



Output	Description
Type	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:).

# GVRP Commands

---

## Introduction

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.

## set gvrp adminmode

This command enables GVRP on the system.

Default	disabled
Format	set gvrp adminmode
Mode	Privileged EXEC

## no set gvrp adminmode

This command disables GVRP.

Format	no set gvrp adminmode
Mode	Privileged EXEC

## set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode), a range of ports (Interface Range mode), or all ports (Global Config mode).

Default	disabled
Format	set gvrp interfacemode
Mode	<ul style="list-style-type: none"><li>◆ Interface Config</li><li>◆ Interface Range</li><li>◆ Global Config</li></ul>

## no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time, and Leave All Time have no effect.

Format	no set gvrp interfacemode
Mode	◆ Interface Config ◆ Global Config

## show gvrp configuration

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

Format	show gvrp configuration {slot/port   all}
Mode	◆ Privileged EXEC ◆ User EXEC

Output	Description
Interface	slot/port
Join Timer	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	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).

Output	Description
LeaveAll Timer	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 LeaveAll 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	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Timer, Leave Timer, and LeaveAll Timer have no effect.

# IGMP Snooping Configuration Commands

## Introduction

This section describes the commands you use to configure IGMP snooping. FASTPATH software 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.

## set igmp

This command enables IGMP snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) 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 [vlan_id]
Mode	<ul style="list-style-type: none"><li>◆ Global Config</li><li>◆ Interface Config</li><li>◆ VLAN Config</li></ul>

## no set igmp

This command disables IGMP snooping on the system, an interface, a range of interfaces, or a VLAN.

Format	no set igmp [vlan_id]
Mode	<ul style="list-style-type: none"> <li>◆ Global Config</li> <li>◆ Interface Config</li> <li>◆ VLAN Config</li> </ul>

### 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

### no set igmp interfacemode

This command disables IGMP snooping on all interfaces.

Format	no set igmp interfacemode
Mode	Global Config

### set igmp fast-leave

This command enables or disables IGMP snooping fast-leave admin mode on a selected interface, a range of interfaces, or a 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 [vlan_id]
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Interface Range</li> <li>◆ VLAN Config</li> </ul>

### no set igmp fast-leave

This command disables IGMP snooping fast-leave admin mode on a selected interface.

Format	no set igmp fast-leave [vlan_id]
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Interface Range</li> <li>◆ VLAN Config</li> </ul>

### set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface, a range of interfaces, 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 [vlan_id] 2-3600
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> <li>◆ VLAN Config</li> </ul>

### no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format	no set igmp groupmembership-interval [vlan_id]
--------	--

Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> <li>◆ VLAN Config</li> </ul>
------	--

### set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. 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 25 seconds.

Default	10 seconds
Format	set igmp maxresponse [vlan_id] 1-25
Mode	<ul style="list-style-type: none"> <li>◆ Global Config</li> <li>◆ Interface Config</li> <li>◆ VLAN Config</li> </ul>

### no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format	no set igmp maxresponse [vlan_id]
Mode	<ul style="list-style-type: none"> <li>◆ Global Config</li> <li>◆ Interface Config</li> <li>◆ VLAN Config</li> </ul>

### set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. 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, that is, no expiration.

Default	0
---------	---



Format	<code>set igmp mcartrexpertime [vlan_id] 0-3600</code>
Mode	<ul style="list-style-type: none"> <li>◆ Global Config</li> <li>◆ Interface Config</li> <li>◆ VLAN Config</li> </ul>

### **no set igmp mcartrexpertime**

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format	<code>no set igmp mcartrexpertime [vlan_id]</code>
Mode	<ul style="list-style-type: none"> <li>◆ Global Config</li> <li>◆ Interface Config</li> <li>◆ VLAN Config</li> </ul>

### **set igmp mrouter**

This command configures the VLAN ID (*vlan\_id*) that has the multicast router mode enabled.

Format	<code>set igmp mrouter vlan_id</code>
Mode	Interface Config

### **no set igmp mrouter**

This command disables multicast router mode for a particular VLAN ID (*vlan\_id*).

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

### **set igmp mrouter interface**

This command configures the interface or range of interfaces 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	<code>set igmp mrouter interface</code>
Mode	Interface Config

### **no set igmp mrouter interface**

This command disables the status of the interface as a statically configured multicast router interface.

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

### **set igmp router-alert-check**

This command enables Router-Alert validation for IGMP packets.

Format	<code>set igmp router-alert-check</code>
Mode	Global Config

### **no set igmp router-alert-check**

This command disables Router-Alert validation for IGMP packets.

Format	<code>no set igmp router-alert-check</code>
Mode	Global Config

### **show igmpsnooping**

This command displays IGMP snooping information. Configured information is displayed whether or not IGMP snooping is enabled.

Format	<code>show igmpsnooping [slot/port   <i>vlan_id</i>]</code>
Mode	Privileged EXEC

When the optional arguments `slot/port` or `vlan_id` are not used, the command displays the following information.

Output	Description
Admin Mode	Indicates whether or not IGMP snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP snooping is enabled.
VLANs Enabled for IGMP Snooping	The list of VLANs on which IGMP snooping is enabled.

When you specify the slot/port values, the following information appears:

Output	Description
IGMP Snooping Admin Mode	Indicates whether IGMP snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time, in seconds, that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface 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 *vlan\_id*, the following information appears.

Output	Description
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP snooping Fast-leave is active on the VLAN.
Group Membership Interval	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.
Maximum Response Time	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 Expiry Time	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.

**show  
igmpsnooping  
mrouter interface**

This command displays information about statically configured ports.

Format	show igmpsnooping mrouter interface slot/port
Mode	Privileged EXEC

Output	Description
Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.

Output	Description
VLAN ID	The list of VLANs of which the interface is a member.

## show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format	show igmpsnooping mrouter vlan slot/port
Mode	Privileged EXEC

Output	Description
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

## 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

Output	Description
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example, 01:23:45:67:89:AB.
Type	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).

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

# IGMP Snooping Querier Commands

---

## Introduction

IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP snooping queriers on the network and, separately, on VLANs.

## set igmp querier

This command enables IGMP snooping querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the snooping querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP snooping querier enabled and IGMP snooping is operationally disabled on it, IGMP snooping querier functionality is disabled on that VLAN. IGMP snooping functionality is re-enabled if IGMP snooping is operational on the VLAN.

**Note**  
The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP snooping querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default	disabled
Format	set igmp querier [vlan-id] [address ipv4_address]
Mode	◆ Global Config ◆ VLAN Mode

**no set igmp querier**

This command disables IGMP snooping querier on the system. Use the optional address parameter to reset the querier address to 0.0.0.0.

Format	no set igmp querier [vlan-id] [address]
Mode	◆ Global Config ◆ VLAN Mode

**set igmp querier query-interval**

This command sets the IGMP Querier Query Interval time. It is the amount of time, in seconds, that the switch waits before sending another general query.

Default	disabled
Format	set igmp querier query-interval 1-18000
Mode	Global Config

**no set igmp querier query-interval**

This command sets the IGMP Querier Query Interval time to its default value.

Format	no set igmp querier query-interval
Mode	Global Config

**set igmp querier timer expiry**

This command sets the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default	60 seconds
Format	set igmp querier timer expiry 60-300
Mode	Global Config

**no set igmp querier timer expiry**

This command sets the IGMP Querier timer expiration period to its default value.

Format	no set igmp querier timer expiry
--------	----------------------------------



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

### **set igmp querier version**

This command sets the IGMP version of the query that the snooping switch is going to send periodically.

Default	1
Format	set igmp querier version 1-2
Mode	Global Config

### **no set igmp querier version**

This command sets the IGMP Querier version to its default value.

Format	no set igmp querier version
Mode	Global Config

### **set igmp querier election participate**

This command enables the snooping querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the snooping querier finds that the other Querier's source address is better (less) than the snooping querier's address, it stops sending periodic queries. If the snooping querier wins the election, then it will continue sending periodic queries.

Default	disabled
Format	set igmp querier election participate
Mode	VLAN Config

### **no set igmp querier election participate**

This command sets the snooping querier to not participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	no set igmp querier election participate
--------	--

Mode	VLAN Config
------	-------------

## show igmpsnooping querier

This command displays IGMP snooping querier information. Configured information is displayed whether or not IGMP snooping querier is enabled.

Format	show igmpsnooping querier [{detail   vlan <i>vlanid</i> }]
Mode	Privileged EXEC

When the optional argument *vlanid* is not used, the command displays the following information:

Output	Description
Admin Mode	Indicates whether or not IGMP snooping querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a snooping querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid* is not used, the following additional information appears:

Output	Description
VLAN Admin Mode	Indicates whether iGMP snooping querier is active on the VLAN.

Output	Description
VLAN Operational State	Indicates whether IGMP snooping querier is in <i>Querier</i> or <i>Non-Querier</i> state. When the switch is in <i>Querier</i> state, it will send out periodic general queries. When in <i>Non-Querier</i> state, it will wait for moving to <i>Querier</i> state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in <i>Querier</i> state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP snooping querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

# ISDP Commands

---

## Introduction

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

## isdp run

This command enables ISDP on the switch.

Default	Enabled
Format	<code>isdp run</code>
Mode	Global Config

## no isdp run

This command disables ISDP on the switch.

Format	<code>no isdp run</code>
Mode	Global Config

## isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default	180 seconds
Format	<code>isdp holdtime 10-255</code>
Mode	Global Config

## isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default	30 seconds
Format	<code>isdp timer 5-254</code>
Mode	Global Config

## isdp advertise-v2

This command enables the sending of ISDP Version 2 packets from the device.

Default	Enabled
Format	isdp advertise-v2
Mode	Global Config

## no isdp advertise-v2

This command disables the sending of ISDP Version 2 packets from the device.

Format	no isdp advertise-v2
Mode	Global Config

## isdp enable

This command enables ISDP on an interface or range of interfaces.

### Note

ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command “[isdp run](#)” on page 256.

Default	Enabled
Format	isdp enable
Mode	Interface Config

## no isdp enable

This command disables ISDP on the interface.

Format	no isdp enable
Mode	Interface Config

## clear isdp counters

This command clears ISDP counters.

Format	clear isdp counters
Mode	Privileged EXEC

## clear isdp table

This command clears entries in the ISDP table.

Format	clear isdp table
--------	------------------

Mode	Privileged EXEC
------	-----------------

## show isdp

This command displays global ISDP settings.

Format	show isdp
Mode	Privileged EXEC

Output	Description
Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
ISDPv2 Advertisements	The setting for sending ISDPv2 packets. If disabled, Version 1 packets are transmitted.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	Indicates the Device ID format capability of the device. <ul style="list-style-type: none"> <li>◆ <code>serialNumber</code> indicates that the device uses a serial number as the format for its Device ID.</li> <li>◆ <code>macAddress</code> indicates that the device uses a Layer 2 MAC address as the format for its Device ID.</li> <li>◆ <code>other</code> indicates that the device uses its platform-specific format as the format for its Device ID.</li> </ul>
Device ID Format	Indicates the Device ID format of the device. <ul style="list-style-type: none"> <li>◆ <code>serialNumber</code> indicates that the value is in the form of an ASCII string containing the device serial number.</li> <li>◆ <code>macAddress</code> indicates that the value is in the form of a Layer 2 MAC address.</li> <li>◆ <code>other</code> indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains <code>serialNumber</code> appended/prepended with system name.</li> </ul>

**show isdp interface** This command displays ISDP settings for the specified interface.

Format	show isdp interface {all   slot/port}
Mode	Privileged EXEC

Output	Description
Mode	ISDP mode enabled/disabled status for the interface(s).

**show isdp entry** This command displays ISDP entries. If the device ID is specified, then only entries for that device are shown.

Format	show isdp entry {all   deviceid}
Mode	Privileged EXEC

Output	Description
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.

**show isdp neighbors** This command displays the list of neighboring devices.

Format	show isdp neighbors [{slot/port   detail}]
Mode	Privileged EXEC

Output	Description
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	Displays when the entry was last modified.
Version	The software version that the neighbor is running.

**Example:** The following shows example CLI display output for the command:  
(CN1601)#show isdp neighbors detail

```
Device ID 0001f45f1bc0
Address(es):
    IP Address: 10.27.7.57
Capability Router Trans Bridge Switch IGMP
Platform SecureStack C2
Interface 0/48
Port ID ge.3.14
Holdtime 131
Advertisement Version 2
Entry last changed time 0 days 00:01:59
Version:05.00.56
```

## show isdp traffic

This command displays ISDP statistics.

Format	show isdp traffic
Mode	Privileged EXEC



Output	Description
ISDP Packets Received	Total number of ISDP packets received.
ISDP Packets Transmitted	Total number of ISDP packets transmitted.
ISDPv1 Packets Received	Total number of ISDPv1 packets received.
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted.
ISDPv2 Packets Received	Total number of ISDPv2 packets received.
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted.
ISDP Bad Header	Number of packets received with a bad header.
ISDP Checksum Error	Number of packets received with a checksum error.
ISDP Transmission Failure	Number of packets which failed to transmit.
ISDP Invalid Format	Number of invalid packets received.
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database.
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

### debug isdp packet

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Format	debug isdp packet [{receive   transmit}]
Mode	Privileged EXEC

### no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format	no debug isdp packet [{receive   transmit}]
Mode	Privileged EXEC

## LLDP (802.1AB) Commands

---

### Introduction

This section describes the commands you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

### lldp transmit

This command enables the LLDP advertise capability on an interface or a range of interfaces.

Default	disabled
Format	lldp transmit
Mode	Interface Config

### no lldp transmit

This command returns the local data transmission capability to the default.

Format	no lldp transmit
Mode	Interface Config

### lldp receive

This command enables the LLDP receive capability on an interface or a range of interfaces.

Default	disabled
Format	lldp receive
Mode	Interface Config

### no lldp receive

This command returns the reception of LLDPDUs to the default value.

Format	no lldp receive
Mode	Interface Config

## lldp timers

This command sets the timing parameters for local data transmission on ports enabled for LLDP. The *interval-seconds* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1 to 32768 seconds. The *hold-value* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2 to 10. The *reinit-seconds* is the delay before re-initialization, and the range is 1 to 10 seconds.

Default	<ul style="list-style-type: none"> <li>◆ interval-30 seconds</li> <li>◆ hold-4</li> <li>◆ reinit-2 seconds</li> </ul>
Format	lldp timers [interval <i>interval-seconds</i> ] [hold <i>hold-value</i> ] [reinit <i>reinit-seconds</i> ]
Mode	Global Config

## no lldp timers

This command returns any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format	no lldp timers [interval] [hold] [reinit]
Mode	Global Config

## lldp transmit-tlv

This command specifies which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs from an interface or range of interfaces. Use *sys-name* to transmit the system name TLV. Use *sys-desc* to transmit the system description TLV. Use *sys-cap* to transmit the system capabilities TLV. Use *port-desc* to transmit the port description TLV.

Default	no optional TLVs are included
Format	lldp transmit-tlv [ <i>sys-desc</i> ] [ <i>sys-name</i> ] [ <i>sys-cap</i> ] [ <i>port-desc</i> ]

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

### **no lldp transmit-tlv**

This command removes an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format	no lldp transmit-tlv [ <i>sys-desc</i> ] [ <i>sys-name</i> ] [ <i>sys-cap</i> ] [ <i>port-desc</i> ]
Mode	Interface Config

### **lldp transmit-mgmt**

This command includes transmission of the local system management address information in the LLDPDUs. You can use this command to configure a single interface or a range of interfaces.

Format	lldp transmit-mgmt
Mode	Interface Config

### **no lldp transmit-mgmt**

This command cancels inclusion of the management information in the LLDPDUs.

Format	no lldp transmit-mgmt
Mode	Interface Config

### **lldp notification**

This command enables remote data change notifications on an interface or a range of interfaces.

Default	disabled
Format	lldp notification
Mode	Interface Config

### **no lldp notification**

This command disables notifications.

Default	disabled
Format	no lldp notification
Mode	Interface Config

### lldp notification-interval

This command configures how frequently the system sends remote data change notifications. The *interval* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5 to 3600 seconds.

Default	5
Format	lldp notification-interval <i>interval</i>
Mode	Global Config

### no lldp notification-interval

This command returns the notification interval to the default value.

Format	no lldp notification-interval
Mode	Global Config

### clear lldp statistics

This command resets all LLDP statistics, including MED-related information.

Format	clear lldp statistics
Mode	Privileged Exec

### clear lldp remote-data

This command deletes all information from the LLDP remote data table, including MED-related information.

Format	clear lldp remote-data
Mode	Global Config

**show lldp**

This command displays a summary of the current LLDP configuration.

Format	show lldp
Mode	Privileged EXEC

Output	Description
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before re-initialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

**show lldp interface**

This command displays a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format	show lldp interface {slot/port   all}
Mode	Privileged EXEC

Output	Description
Interface	The interface in a slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.

Output	Description
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

### show lldp statistics

This command displays the current LLDP traffic and remote table statistics for a specified interface or for all interfaces.

Format	<code>show lldp statistics {slot/port   all}</code>
Mode	Privileged EXEC

Output	Description
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Output	Description
Interface	The interface in slot/port format.
Transmit Total	Total number of LLDP packets transmitted on the port.

Output	Description
Receive Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
TVL Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

### show lldp remote-device

This command displays summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format	show lldp remote-device {slot/port   all}
Mode	Privileged EXEC

Output	Description
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

**Example:** The following shows example CLI display output for the command:



```
(CN1601)#show lldp remote-device all
```

#### LLDP Remote Device Summary

```
Local
Interface RemID    Chassis ID          Port ID             System
Name
-----
0/1
0/2
0/3
0/4
0/5
0/6
0/7      2      00:FC:E3:90:01:0F    00:FC:E3:90:01:11
0/7      3      00:FC:E3:90:01:0F    00:FC:E3:90:01:12
0/7      4      00:FC:E3:90:01:0F    00:FC:E3:90:01:13
0/7      5      00:FC:E3:90:01:0F    00:FC:E3:90:01:14
0/7      1      00:FC:E3:90:01:0F    00:FC:E3:90:03:11
0/7      6      00:FC:E3:90:01:0F    00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

### show lldp remote- device detail

This command displays detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format	show lldp remote-device detail slot/port
Mode	Privileged EXEC

Output	Description
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.

Output	Description
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alphanumeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#show lldp remote-device detail 0/7
```

```
LLDP Remote Device Detail
```

```
Local Interface: 0/7
```

```

Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds

```

## show lldp local-device

This command displays summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format	show lldp local-device {slot/port   all}
Mode	Privileged EXEC

Output	Description
Interface	The interface in a slot/port format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

## show lldp local-device detail

This command displays detailed information about the LLDP data a specific interface transmits.

Format	show lldp local-device detail slot/port
Mode	Privileged EXEC

Output	Description
Interface	The interface that sends the LLDPDU.

Output	Description
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alphanumeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

## LLDP-MED Commands

---

### Introduction

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

### lldp med

This command enables MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default	disabled
Format	lldp med
Mode	Interface Config

### no lldp med

This command disables MED.

Format	no lldp med
Mode	Interface Config

### lldp med confignotification

This command configures an interface or a range of interfaces to send the topology change notification.

Default	disabled
Format	lldp med confignotification
Mode	Interface Config

### no lldp med confignotification

This command disables notifications.

Format	no lldp med confignotification
Mode	Interface Config

## lldp med transmit-tlv

This command specifies which optional Type Length Values (TLVs) in the LLDP-MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from this interface or a range of interfaces.

Default	By default, the capabilities and network policy TLVs are included.
Format	lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]
Mode	Interface Config

Parameter	Description
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

## no lldp med transmit-tlv

This command removes a TLV.

Format	no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]
Mode	Interface Config

## lldp med all

This command configures LLDP-MED on all the ports.

Format	lldp med all
Mode	Global Config

## lldp med confignotification all

This command configures all the ports to send the topology change notification.

Format	lldp med confignotification all
Mode	Global Config

### lldp med faststart-repeatcount

This command sets the value of the fast start repeat count. *[count]* is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default	3
Format	lldp med faststartrepeatcount <i>[count]</i>
Mode	Global Config

### no lldp med faststart-repeatcount

This command returns the value of the fast start repeat count to the factory default value.

Format	no lldp med faststartrepeatcount
Mode	Global Config

### lldp med transmit-tlv all

This command specifies which optional Type Length Values (TLVs) in the LLDP-MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default	By default, the capabilities and network policy TLVs are included.
Format	lldp med transmit-tlv all <i>[capabilities]</i> <i>[ex-pd]</i> <i>[ex-pse]</i> <i>[inventory]</i> <i>[location]</i> <i>[network-policy]</i>
Mode	Global Config

Parameter	Description
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

### no lldp med transmit-tlv

This command removes a TLV.

Format	no lldp med transmit-tlv <i>[capabilities]</i> <i>[network-policy]</i> <i>[ex-pse]</i> <i>[ex-pd]</i> <i>[location]</i> <i>[inventory]</i>
--------	--

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

## show lldp med

This command displays a summary of the current LLDP-MED configuration.

Format	show lldp med
Mode	Privileged Exec

**Example:** The following shows example CLI display output for the command:

```
(CN1601) #show lldp med
LLDP-MED Global Configuration
```

```
Fast Start Repeat Count: 3
Device Class: Network Connectivity
```

```
(CN1601) #
```

## show lldp med interface

This command displays a summary of the current LLDP-MED configuration for a specific interface. The slot/port indicates a specific physical interface. *all* indicates all valid LLDP interfaces.

Format	show lldp med interface {slot/port   all}
Mode	Privileged Exec

**Example:** The following shows example CLI display output for the command:

```
(CN1601) #show lldp med interface all
```

Interface	Link	configMED	operMED	ConfigNotify	TLVstx
1/0/1	Down	Disabled	Disabled	Disabled	0,1
1/0/2	Up	Disabled	Disabled	Disabled	0,1
1/0/3	Down	Disabled	Disabled	Disabled	0,1
1/0/4	Down	Disabled	Disabled	Disabled	0,1
1/0/5	Down	Disabled	Disabled	Disabled	0,1
1/0/6	Down	Disabled	Disabled	Disabled	0,1
1/0/7	Down	Disabled	Disabled	Disabled	0,1
1/0/8	Down	Disabled	Disabled	Disabled	0,1
1/0/9	Down	Disabled	Disabled	Disabled	0,1
1/0/10	Down	Disabled	Disabled	Disabled	0,1
1/0/11	Down	Disabled	Disabled	Disabled	0,1
1/0/12	Down	Disabled	Disabled	Disabled	0,1
1/0/13	Down	Disabled	Disabled	Disabled	0,1



```

1/0/14      Down      Disabled Disabled Disabled      0,1

TLV Codes: 0- Capabilities,          1- Network Policy
            2- Location,              3- Extended PSE
            4- Extended Pd,          5- Inventory
--More-- or (q)uit
(CN1601) #show lldp med interface 1/0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
-----
1/0/2      Up      Disabled Disabled   Disabled      0,1

TLV Codes: 0- Capabilities,          1- Network Policy
            2- Location,              3- Extended PSE
            4- Extended Pd,          5- Inventory

(CN1601) #

```

## show lldp med local-device detail

This command displays detailed information about the LLDP MED data that a specific interface transmits. slot/port indicates a specific physical interface.

Format	show lldp med local-device detail slot/port
Mode	Privileged EXEC

**Example:** The following shows example CLI display output for the command:

```
(CN1601) #show lldp med local-device detail 1/0/8
```

```
LLDP-MED Local Device Detail
```

```
Interface: 1/0/8
```

```
Network Policies
```

```
Media Policy Application Type : voice
```

```
Vlan ID: 10
```

```
Priority: 5
```

```
DSCP: 1
```

```
Unknown: False
```

```
Tagged: True
```

```
Media Policy Application Type : streamingvideo
```

```
Vlan ID: 20
```

```
Priority: 1
```

```
DSCP: 2
```

```
Unknown: False
```

```
Tagged: True
```

```
Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx
```

```
Location
Subtype: elin
Info: xxx xxx xxx
```

```
Extended POE
Device Type: pseDevice
```

```
Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical
```

```
Extended POE PD
```

```
Required: 0.2 Watts
Source: local
Priority: low
```

## show lldp med remote-device

This command displays the summary information about remote devices that transmit current LLDP-MED data to the system. You can show information about LLDP-MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format	show lldp med remote-device {slot/port   all}
Mode	Privileged EXEC

Output	Description
Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.

Output	Description
Device Class	Device classification of the remote device.

**Example:** The following shows example CLI display output for the command:  
(CN1601) #show lldp med remote-device all

LLDP-MED Remote Device Summary

```

Local
Interface  Remote ID  Device Class
-----
1/0/8 1Class I
1/0/9 2Not Defined
1/0/10 3Class II
1/0/11 4Class III
1/0/12 5    Network Con

```

## show lldp med remote-device detail

This command displays detailed information about remote devices that transmit current LLDP-MED data to an interface on the system.

Format	show lldp med remote-device detail slot/port
Mode	Privileged EXEC

**Example:** The following shows example CLI display output for the command:  
(CN1601) #show lldp med remote-device detail 1/0/8

LLDP-MED Remote Device Detail

```

Local Interface: 1/0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location,
extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

```

```

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False

```

Tagged: True

Media Policy Application Type : streamingvideo

Vlan ID: 20

Priority: 1

DSCP: 2

Unknown: False

Tagged: True

#### Inventory

Hardware Rev: xxx xxx xxx

Firmware Rev: xxx xxx xxx

Software Rev: xxx xxx xxx

Serial Num: xxx xxx xxx

Mfg Name: xxx xxx xxx

Model Name: xxx xxx xxx

Asset ID: xxx xxx xxx

#### Location

Subtype: elin

Info: xxx xxx xxx

#### Extended POE

Device Type: pseDevice

#### Extended POE PSE

Available: 0.3 Watts

Source: primary

Priority: critical

#### Extended POE PD

Required: 0.2 Watts

Source: local

Priority: low

# MAC Database Commands

---

Introduction

This section describes the commands you use to configure and view information about the Media Access Control (MAC) databases.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The *seconds* parameter must be within the range of 10 to 1,000,000 seconds.

Default	300
Format	bridge aging-time <i>seconds</i>
Mode	Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Format	no bridge aging-time
Mode	Global Config

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

Output	Description
Forwarding DB ID	Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system.

Output	Description
Agetime	◆ In an IVL system, this parameter displays the address aging timeout for the associated forwarding database.

### 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 <i>macaddr</i>
Mode	Privileged EXEC

Output	Description
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example, 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP snooping, GMRP, and Static Filtering.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Forwarding Interfaces	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

### show mac-address-table stats

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

Format	show mac-address-table stats
Mode	Privileged EXEC

Output	Description
Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	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	The current number of entries in the MFDB.

# Port-Based Network Access Control Commands

## Introduction

This section describes the commands you use to configure port-based network access control (IEEE 802.1X). Port-based network access control allows you to permit access to network services only to devices that are authorized and authenticated.

## aaa authentication dot1x default

This command configures the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- ◆ `ias`. Uses the internal authentication server users database for authentication.
- ◆ `local`. Uses the local username database for authentication.
- ◆ `none`. Uses no authentication.
- ◆ `radius`. Uses the list of all RADIUS servers for authentication.

Format	<code>aaa authentication dot1x default <i>method1</i> [<i>method2...</i>]</code>
Mode	Global Config

## clear dot1x statistics

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

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

## clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format	<code>clear dot1x authentication-history [<i>slot/port</i>]</code>
Mode	Privileged EXEC



### clear radius statistics

This command clears all of the RADIUS statistics.

Format	clear radius statistics
Mode	Privileged EXEC

### dot1x guest-vlan

This command configures VLAN as guest vlan on an interface or a range of interfaces. The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Default	disabled
Format	dot1x guest-vlan <i>vlan-id</i>
Mode	Interface Config

### no dot1x guest-vlan

This command disables guest VLAN on the interface.

Format	no dot1x guest-vlan
Mode	Interface Config

### dot1x initialize

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

Format	dot1x initialize slot/port
Mode	Privileged EXEC

### dot1x max-req

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

Default	2
Format	dot1x max-req count

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

### no dot1x max-req

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

Format	no dot1x max-req
Mode	Interface Config

### dot1x max-users

This command sets the maximum number of clients supported on an interface or range of interfaces when MAC-based dot1x authentication is enabled on the port. The maximum users supported per port is dependent on the product. The *count* value is in the range 1 to 16.

Default	16
Format	dot1x max-users <i>count</i>
Mode	Interface Config

### no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format	no dot1x max-users <i>count</i>
Mode	Interface Config

### dot1x port-control

This command sets the authentication mode to use on the specified interface or range of interfaces. Use the *force-unauthorized* parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the *force-authorized* parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the *auto* parameter to specify that the authenticator PAE sets the controlled port mode to reflect the

outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	dot1x port-control {force-unauthorized   force-authorized   auto   mac-based}
Mode	Interface Config

### **no dot1x port-control**

This command sets the 802.1X port control mode on the specified port to the default value.

Format	no dot1x port-control
Mode	Interface Config

### **dot1x port-control all**

This command sets the authentication mode to use on all ports. Select `force-unauthorized` to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select `force-authorized` to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select `auto` to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	dot1x port-control all {force-unauthorized   force-authorized   auto   mac-based}
Mode	Global Config

### **no dot1x port-control all**

This command sets the authentication mode on all ports to the default value.

Format	no dot1x port-control all
Mode	Global Config

### **dot1x re-authenticate**

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

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

### **dot1x re-authentication**

This command enables re-authentication of the supplicant for the specified interface or range of interfaces.

Default	disabled
Format	<code>dot1x re-authentication</code>
Mode	Interface Config

### **no dot1x re-authentication**

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

Format	<code>no dot1x re-authentication</code>
Mode	Interface Config

### **dot1x system-auth-control**

This command enables the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	disabled
Format	<code>dot1x system-auth-control</code>
Mode	Global Config

### **no dot1x system-auth-control**

This command disables the dot1x authentication support on the switch.

Format	no dot1x system-auth-control
Mode	Global Config

### **dot1x system-auth-control monitor**

This command enables the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Default	disabled
Format	dot1x system-auth-control monitor
Mode	Global Config

### **no dot1x system-auth-control monitor**

This command disables the 802.1X Monitor mode on the switch.

Format	no dot1x system-auth-control monitor
Mode	Global Config

### **dot1x timeout**

This command sets the value, in seconds, of the timer used by the authenticator state machine on an interface or range of interfaces.

Default	<ul style="list-style-type: none"><li>◆ guest-vlan-period: 90 seconds</li><li>◆ reauth-period: 3600 seconds</li><li>◆ quiet-period: 60 seconds</li><li>◆ tx-period: 30 seconds</li><li>◆ supp-timeout: 30 seconds</li><li>◆ server-timeout: 30 seconds</li></ul>
---------	--

Format	<code>dot1x timeout {{guest-vlan-period seconds}   {reauth-period seconds}   {quiet-period seconds}   {tx-period seconds}   {supp-timeout seconds}   {server-timeout seconds}}</code>
Mode	Interface Config

Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	Description
<code>guest-vlan-period</code>	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest VLAN (if configured). The guest VLAN timer is only relevant when the guest VLAN has been configured on that specific port.
<code>reauth-period</code>	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 <code>reauth-period</code> must be a value in the range 1 to 65535.
<code>quiet-period</code>	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 <code>quiet-period</code> must be a value in the range 0 to 65535.
<code>tx-period</code>	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 <code>tx-period</code> must be a value in the range 1 to 65535.
<code>supp-timeout</code>	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The <code>supp-timeout</code> must be a value in the range 1 to 65535.

Tokens	Description
<code>server-timeout</code>	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The <code>server-timeout</code> must be a value in the range 1 to 65535.

### **no dot1x timeout**

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

Format	<code>no dot1x timeout {guest-vlan-period   reauth-period   quiet-period   tx-period   supp-timeout   server-timeout}</code>
Mode	Interface Config

### **dot1x unauthenticated-vlan**

This command configures the unauthenticated VLAN associated with the specified interface or range of interfaces. The unauthenticated VLAN ID can be a valid VLAN ID from 0 to maximum supported VLAN ID (4093 for FASTPATH). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, that is, invalid and not operational.

Default	0
Format	<code>dot1x unauthenticated-vlan <i>vlan id</i></code>
Mode	Interface Config

### **no dot1x unauthenticated-vlan**

This command resets the unauthenticated VLAN associated with the port to its default value.

Format	<code>no dot1x unauthenticated-vlan</code>
Mode	Interface Config

**dot1x user**

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

Format	<code>dot1x user user {slot/port   all}</code>
Mode	Global Config

**no dot1x user**

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

Format	<code>no dot1x user user {slot/port   all}</code>
Mode	Global Config

**users defaultlogin**

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

Format	<code>users defaultlogin listname</code>
Mode	Global Config

**users login**

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

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and Telnet sessions will be blocked until the authentication is complete.

**Note**  
The login list associated with the admin user cannot be changed to prevent accidental lockout from the switch.

Format	<code>users login user listname</code>
--------	--



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

## show authentication

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

Format	show authentication
Mode	Privileged EXEC

Output	Description
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.
Method 3	The third method in the specified authentication login list, if any.

## show authentication methods

This command displays information about the authentication methods.

Format	show authentication methods
Mode	Privileged EXEC

**Example:** The following example displays the authentication configuration:

```
(CN1601)#show authentication methods
```

```
Login Authentication Method Lists
-----
defaultList          : local

Enable Authentication Method Lists
-----
enableList           : local
```

```

Line      Login Method List      Enable Method List
-----
Console   defaultList                enableList
Telnet    defaultList                enableList
SSH       defaultList                enableList

HTTPS      :local
HTTP       :local
DOT1X      :none

```

## show authentication users

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

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

## show dot1x

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

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

If you do not use the optional parameters `slot/port` or `all`, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Output	Description
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).

Output	Description
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the dot1x Monitor mode on the switch is enabled or disabled.

If you use the optional parameter *summary* {slot/port | all}, the dot1x configuration for the specified port or all ports are displayed:

Output	Description
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized   force-authorized   auto   mac-based   authorized   unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized   unauthorized.
Reauthentication Enabled	Indicates whether reauthentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized   unauthorized.

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#show dot1x summary 0/1
```

		Operating	
Interface	Control Mode	Control Mode	Port Status
-----	-----	-----	-----
0/1	auto	auto	Authorized

If you use the optional parameter *detail* slot/port, the detailed dot1x configuration for the specified port is displayed:

Output	Description
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.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized force-authorized auto mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
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 to 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 to 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.

Output	Description
Guest VLAN Period	The time, in seconds, for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 to 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 to 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 to 10.
VLAN-assigned	The VLAN assigned to the port by the RADIUS server. This is only valid when the port control mode is not MAC-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 to 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are True or False.

Output	Description
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period, in seconds, is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#show dot1x detail 0/1
Port..... 0/1
Protocol Version..... 1
PAE Capabilities..... Supplicant
Control Mode..... auto
Supplicant PAE State..... Initialize
Supplicant Backend Authentication State..... Initialize
Maximum Start trails..... 3
Start Period (secs)..... 30
Held Period (secs)..... 60
```

```

Authentication Period (secs)..... 30
EAP Method..... MD5-Challenge

```

For each client authenticated on the port, the `show dot1x detail slot/port` command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Output	Description
Supplicant MAC-Address	The MAC address of the 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.
VLAN-Assigned	The VLAN assigned to the client by the RADIUS server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter `statistics slot/port`, the following dot1x statistics for the specified port appear:

Output	Description
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.

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

### **show dot1x authentication-history**

This command displays 802.1X authentication events and information during successful and unsuccessful dot1x authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

Format	show dot1x authentication-history {slot/port   all} [failed-auth-only] [detail]
Mode	Privileged EXEC



Output	Description
Time Stamp	The exact time at which the event occurs.
Interface	Physical port on which the event occurs.
MAC-Address	The supplicant/client MAC address.
VLAN Assigned	The VLAN assigned to the client/port on authentication.
VLAN Assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Monitor Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

## show dot1x clients

This command displays 802.1X client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

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

Output	Description
Clients Authenticated using Monitor Mode	Indicates the number of the dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of dot1x clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with a client.
Interface	The physical port to which the supplicant is associated.

Output	Description
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Monitor Mode, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period, in seconds, is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

## show dot1x users

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

Format	<code>show dot1x users slot/port</code>
--------	---

Mode	Privileged EXEC
------	-----------------

Output	Description
Users	Users configured locally to have access to the specified port.

# Port Channel/LAG (802.3ad) Commands

---

## Introduction

This section describes the commands you use to configure port channels, which are defined in the 802.3ad specification, and that 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. Assign the port channel (LAG) VLAN membership after you create a port channel. If you do not assign VLAN membership, the port channel might become a member of the management VLAN which can result in learning and switching issues.

A port channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port channel interface does not require a partner system to be able to aggregate its member ports.

### Note

---

If you configure the maximum number of dynamic port channels (LAGs) that your platform supports, any additional port channels that you configure are automatically static.

---

## port-channel

This command configures a new port channel (LAG) 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. Use the show port channel command to display the slot/port number for the logical interface.

### Note

---

Before you include a port in a port channel, set the port physical mode. For more information, see “[no shutdown](#)” on page 326.

---

Format	port-channel <i>name</i>
Mode	Global Config

## no port-channel

This command deletes a port channel (LAG).

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

## addport

This command adds one port to the port channel (LAG). The first interface is a logical slot/port number of a configured port channel. You can add a range of ports by specifying the port range when you enter Interface Config mode (for example, interface 1/0/1-1/0/4).

### Note

Before adding a port to a port channel, set the physical mode of the port. For more information, see “[no shutdown](#)” on page 326.

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

## deleteport (Interface Config)

This command deletes a port or a range of ports from the port channel (LAG). The interface is a logical slot/port number of a configured port channel (or range of port channels).

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

## deleteport (Global Config)

This command deletes all configured ports from the port channel (LAG). The interface is a logical slot/port number of a configured port channel. To clear the port channels, see “[clear traplog](#)” on page 201.

Format	deleteport { <i>logical slot/port</i>   all}
Mode	Global Config

**lacp admin key**

This command configures the administrative value of the key for the port channel. The value range of *key* is 0 to 65535. This command can be used to configure a single interface or a range of interfaces.

**Note**\_\_\_\_\_

This command is applicable only to port channel interfaces.

\_\_\_\_\_

Default	0x8000
Format	lacp admin key <i>key</i>
Mode	Interface Config

**no lacp admin key**

This command configures the default administrative value of the key for the port channel.

Format	no lacp admin key
Mode	Interface Config

**lacp collector max-delay**

This command configures the port channel collector max delay. You can use this command to configure a single interface or a range of interfaces. The valid range of *delay* is 0 to 65535.

**Note**\_\_\_\_\_

This command is applicable only to port channel interfaces.

\_\_\_\_\_

Default	0x8000
Format	lacp collector max delay <i>delay</i>
Mode	Interface Config

**no lacp collector max delay**

This command configures the default port channel collector max delay.

Format	no lacp collector max delay
Mode	Interface Config

**lacp actor admin**

This command configures the LACP actor admin parameters.

Format	lacp actor admin
Mode	Interface Config

**lacp actor admin key**

This command configures the administrative value of the LACP actor admin key on an interface or range of interfaces. The valid range for *key* is 0 to 65535.

**Note**\_\_\_\_\_

This command is applicable only to physical interfaces.

Default	Internal Interface Number of this Physical Port
Format	lacp actor admin key <i>key</i>
Mode	Interface Config

**no lacp actor admin key**

This command configures the default administrative value of the key.

Format	no lacp actor admin key
Mode	Interface Config

**lacp actor admin state**

This command configures the administrative value of actor state as transmitted by the actor in the LACPDUs. The valid value range is 0x00 to 0xFF. This command can be used to configure a single interfaces or a range of interfaces.

**Note**\_\_\_\_\_

This command is applicable only to physical interfaces.

Default	0x07
Format	lacp actor admin state {individual longtimeout passive}
Mode	Interface Config

**no lacp actor admin state**

This command configures the default administrative values of actor state as transmitted by the actor in LACPDUs.

Format	no lacp actor admin state {individual longtimeout passive}
Mode	Interface Config

**lacp actor admin state individual**

This command sets the LACP actor admin state to individual.

**Note**

This command is applicable only to physical interfaces.

Format	lacp actor admin state individual
Mode	Interface Config

**no lacp actor admin state individual**

This command sets the LACP actor admin state to aggregation.

Format	no lacp actor admin state individual
Mode	Interface Config

**lacp actor admin state longtimeout**

This command sets the LACP actor admin state to longtimeout.

**Note**

This command is applicable only to physical interfaces.

Format	lacp actor admin state longtimeout
Mode	Interface Config

**no lacp actor admin state longtimeout**

This command sets the LACP actor admin state to short timeout.



**Note**

This command is applicable only to physical interfaces.

Format	no lacp actor admin state longtimeout
Mode	Interface Config

**lacp actor admin  
state passive**

This command sets the LACP actor admin state to passive.

**Note**

This command is applicable only to physical interfaces.

Format	lacp actor admin state passive
Mode	Interface Config

**no lacp actor admin  
state passive**

This command sets the LACP actor admin state to active.

Format	no lacp actor admin state passive
Mode	Interface Config

**lacp actor port**

This command configures LACP actor port priority key.

Format	lacp actor port
Mode	Interface Config

**lacp actor port  
priority**

This command configures the priority value assigned to the aggregation port for an interface or range of interfaces. The valid range for priority is 0 to 255.

**Note**

This command is applicable only to physical interfaces.

Default	0x80
Format	lacp actor port priority 0-255
Mode	Interface Config

### no lacp actor port priority

This command configures the default priority value assigned to the aggregation port.

Format	no lacp actor port priority
Mode	Interface Config

### lacp partner admin key

This command configures the administrative value of the key for the protocol partner. You can use this command to configure a single interface or a range of interfaces. The valid range for *key* is 0 to 65535.

#### Note

This command is applicable only to physical interfaces.

Default	0x0
Format	lacp partner admin key key
Mode	Interface Config

### no lacp partner admin key

This command sets the administrative value of the key for the protocol partner to the default.

Format	no lacp partner admin key
Mode	Interface Config

### lacp partner admin state

This command configures the current administrative value of the actor state for the protocol partner. The valid value range is 0x00 to 0xFF.

**Note**

This command is applicable only to physical interfaces.

Default	0x07
Format	lacp partner admin state {individual longtimeout passive}
Mode	Interface Config

**no lacp partner  
admin state**

This command configures the default current administrative value of the actor state for the protocol partner. You can use this command to configure a single interface or a range of interfaces.

Format	no lacp partner admin state {individual longtimeout passive}
Mode	Interface Config

**lacp partner admin  
state individual**

This command sets LACP partner admin state to individual.

**Note**

This command is applicable only to physical interfaces.

Format	lacp partner admin state individual
Mode	Interface Config

**no lacp partner  
admin state  
individual**

This command sets the LACP partner admin state to aggregation.

Format	no lacp partner admin state individual
Mode	Interface Config

**lacp partner admin  
state longtimeout**

This command sets the LACP partner admin state to longtimeout.

**Note**

This command is applicable only to physical interfaces.

Format	<code>lacp partner admin state longtimeout</code>
Mode	Interface Config

**no lacp partner  
admin state  
longtimeout**

This command sets the LACP partner admin state to short timeout.

**Note**

This command is applicable only to physical interfaces.

Format	<code>no lacp partner admin state longtimeout</code>
Mode	Interface Config

**lacp partner admin  
state passive**

This command sets the LACP partner admin state to passive.

**Note**

This command is applicable only to physical interfaces.

Format	<code>lacp partner admin state passive</code>
Mode	Interface Config

**no lacp partner  
admin state passive**

This command sets the LACP partner admin state to active.

Format	<code>no lacp partner admin state passive</code>
Mode	Interface Config

**lacp partner port id**

This command configures the LACP partner port ID. You can use this command to configure a single interface or a range of interfaces. The valid range for *port-id* is 0 to 65535.

**Note**

This command is applicable only to physical interfaces.

Default	0x80
Format	lacp partner port-id <i>port-id</i>
Mode	Interface Config

**no lacp partner port id**

This command sets the LACP partner port ID to the default.

Format	no lacp partner port-id
Mode	Interface Config

**lacp partner port priority**

This command configures the LACP partner port priority. You can use this command to configure a single interface or a range of interfaces. The valid range for *priority* is 0 to 255.

**Note**

This command is applicable only to physical interfaces.

Default	0x0
Format	lacp partner port priority <i>priority</i>
Mode	Interface Config

**no lacp partner port priority**

This command configures the default LACP partner port priority.

Format	no lacp partner port priority
Mode	Interface Config

**lacp partner system-id**

This command configures the 6-octet MAC Address value representing the administrative value of the aggregation port’s protocol partner’s system ID. You can use this command to configure a single interface or a range of interfaces. The valid range of *system-id* is 00:00:00:00:00:00–FF:FF:FF:FF:FF:FF.

**Note**

This command is applicable only to physical interfaces.

Default	00:00:00:00:00:00
Format	lacp partner system-id <i>system-id</i>
Mode	Interface Config

**no lacp partner system-id**

This command configures the default value representing the administrative value of the aggregation port’s protocol partner’s system ID.

Format	no lacp partner system-id
Mode	Interface Config

**lacp partner system priority**

This command configures the administrative value of the priority associated with the partner’s system ID. You can use this command to configure a single interface or a range of interfaces. The valid range for *priority* is 0 to 65535.

**Note**

This command is applicable only to physical interfaces.

Default	0x0
Format	lacp partner system priority <i>0-65535</i>
Mode	Interface Config

**no lacp partner system priority**

This command configures the default administrative value of priority associated with the partner’s system ID.

Format	no lacp partner system priority
--------	---------------------------------

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

### **port-channel static**

This command enables the static mode on a port channel (LAG) interface or range of interfaces. By default the static mode for a new port channel is disabled, which means the port channel is dynamic. However if the maximum number of allowable dynamic port channels are already present in the system, the static mode for a new port channel is enabled, which means the port channel is static. You can only use this command on port channel interfaces.

Default	disabled
Format	port-channel static
Mode	Interface Config

### **no port-channel static**

This command sets the static mode on a particular port channel (LAG) interface to the default value. This command will be executed only for interfaces of type port channel (LAG).

Format	no port-channel static
Mode	Interface Config

### **port lacpmode**

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default	enabled
Format	port lacpmode
Mode	Interface Config

### **no port lacpmode**

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

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

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

### **port lacpmode all**

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

Format	port lacpmode all
Mode	Global Config

### **no port lacpmode all**

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

Format	no port lacpmode all
Mode	Global Config

### **port lacptimeout (Interface Config)**

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	port lacptimeout {actor   partner} {long   short}
Mode	Interface Config

### **no port lacptimeout (Interface Config)**

This command sets the timeout back to its default value on a physical interface of a particular device type (actor or partner).

Format	no port lacptimeout {actor   partner}
Mode	Interface Config

### **port lacptimeout (Global Config)**

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
---------	------



Format	port lacptimeout {actor   partner} {long   short}
Mode	Global Config

### **no port lacptimeout (Global Config)**

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

Format	no port lacptimeout {actor   partner}
Mode	Global Config

### **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

### **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

### **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

### no port-channel linktrap

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

Format	<code>no port-channel linktrap {<i>logical slot/port</i>   <i>all</i>}</code>
Mode	Global Config

### port-channel load- balance

This command selects the load-balancing option used on a port channel (LAG). Traffic is balanced on a port channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

This command can be configured for a single interface, a range of interfaces, or all interfaces.

Default	3
Format	<code>port-channel load-balance {1   2   3   4   5   6} {<i>slot/port</i>   <i>all</i>}</code>
Mode	◆ Interface Config ◆ Global Config

Parameter	Description
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet

Parameter	Description
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
slot/port   all	Global Config Mode only: The interface is a logical slot/port number of a configured port channel. All applies the command to all currently configured port channels.

### no port-channel load-balance

This command reverts to the default load balancing configuration.

Format	no port-channel load-balance {slot/port / all}
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Global Config</li> </ul>

Parameter	Description
slot/port   all	Global Config Mode only: The interface is a logical slot/port number of a configured port channel. <i>all</i> applies the command to all currently configured port channels.

### 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 { <i>logical</i> slot/port   all   <i>name</i> }
Mode	Global Config

**port-channel  
system priority**

This command configures port channel system priority. The valid range of *priority* is 0 to 65535.

Default	0x8000
Format	port-channel system priority <i>priority</i>
Mode	Global Config

**no port-channel  
system priority**

This command configures the default port channel system priority value.

Format	no port-channel system priority
Mode	Global Config

**show lacp actor**

This command displays LACP actor attributes.

Format	show lacp actor {slot/port all}
Mode	Privileged EXEC

The following output parameters are displayed:

Output	Description
System Priority	The administrative value of the key.
Actor Admin Key	The administrative value of the key.
Port Priority	The priority value assigned to the aggregation port.
Admin State	The administrative values of the actor state as transmitted by the actor in LACPDU.

**show lacp partner**

This command displays LACP partner attributes.

Format	show lacp actor {slot/port all}
Mode	Privileged EXEC

The following output parameters are displayed:

Output	Description
System Priority	The administrative value of priority associated with the partner's system ID.
System-ID	Represents the administrative value of the aggregation port's protocol partner's system ID.
Admin Key	The administrative value of the key for the protocol partner.
Port Priority	The administrative value of the key for protocol partner.
Port-ID	The administrative value of the port number for the protocol partner.
Admin State	The administrative values of the actor state for the protocol partner.

## show port-channel

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

Format	<code>show port-channel {<i>logical slot/port</i>   all}</code>
Mode	<ul style="list-style-type: none"><li>◆ Privileged EXEC</li><li>◆ User EXEC</li></ul>

Output	Description
Logical Interface	The valid slot/port of the logical interface.
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.

Output	Description
Type	The status designating whether a particular port channel (LAG) is statically or dynamically maintained. <ul style="list-style-type: none"> <li>◆ Static - The port channel is statically maintained.</li> <li>◆ Dynamic - The port channel is dynamically maintained.</li> </ul>
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).
Device Timeout	For each port, lists the timeout (long or short) for Device Type (actor or partner).
Port Speed	Speed of the port channel port.
Active Ports	The ports that are actively participating in the port channel.
Load Balance Option	The load balance option associated with this LAG. See “ <a href="#">port-channel load-balance</a> ” on page 318.

## show port-channel brief

This command displays the static capability of all port channel (LAG) interfaces on the device as well as a summary of individual port channel interfaces.

Format	show port-channel brief
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

For each port channel the following information is displayed:

Output	Description
Logical Interface	The slot/port of the logical interface.
Port Channel Name	The name of the port channel (LAG) interface.

Output	Description
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port channel is statically or dynamically maintained.
Mbr Ports	The members of this port channel.
Active Ports	The ports that are actively participating in the port channel.

### **show port-channel system priority**

This command displays the port channel system priority.

Format	show port-channel system priority
Mode	Privileged EXEC

# Port Configuration Commands

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

**interface** This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port). You can also specify a range of ports to configure at the same time by specifying the starting slot/port and ending slot/port, separated by a hyphen.

Format	interface {slot/port   slot/port ( <i>startrange</i> ) - slot/port ( <i>endrange</i> ) }
Mode	Global Config

**Example:** The following example enters Interface Config mode for port 1/0/1:  
(CN1601) #configure  
(CN1601) (config) #interface 1/0/1  
(CN1601) (interface 1/0/1) #

**Example:** The following example enters Interface Config mode for ports 1/0/1 through 1/0/4:  
(CN1601) #configure  
(CN1601) (config) #interface 1/0/1-1/0/4  
(CN1601) (interface 1/0/1-1/0/4) #

**adminmode** This command lets you enter the port channel interface administratively.

Format	adminmode
Mode	Interface Config

**auto-negotiate** This command enables automatic negotiation on a port or range of ports.

Default	enabled
Format	auto-negotiate



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

## 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

## auto-negotiate all

This command enables automatic negotiation on all ports.

Default	enabled
Format	auto-negotiate all
Mode	Global Config

## no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	no auto-negotiate all
Mode	Global Config

## description

This command creates an alphanumeric description of an interface or range of interfaces.

Format	description <i>description</i>
Mode	Interface Config

**mtu**

Use the `mtu` command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the `mtu` command to configure jumbo frame support for physical and port channel (LAG) interfaces. For the standard FASTPATH implementation, the MTU size is a valid integer between 1522 to 9216 for tagged packets and a valid integer between 1518 to 9216 for untagged packets.

**Note**\_\_\_\_\_

To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require.

\_\_\_\_\_

Default	1518 (untagged)
Format	mtu 1518-9216
Mode	Interface Config

**no mtu**

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

Format	no mtu
Mode	Interface Config

**shutdown**

This command disables a port or range of 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
Mode	Interface Config

**no shutdown**

This command enables a port.

Format	no shutdown
--------	-------------

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

## shutdown all

This command disables all ports.

### Note

You can use the `shutdown all` command on physical and port channel (LAG) interfaces, but not on VLAN routing interfaces.

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

## no shutdown all

This command enables all ports.

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

## speed

This command lets you set the speed and duplex setting for an interface or range of interfaces.

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

Acceptable Values	Description
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

**speed all**

This command lets you set the speed and duplex setting for all interfaces.

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

Acceptable Values	Description
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

**show port**

This command displays port information.

Format	show port {slot/port   all}
Mode	Privileged EXEC

Output	Description
Interface	slot/port
Type	<p>If not blank, this field indicates that this port is a special type of port. The possible values are:</p> <ul style="list-style-type: none"><li>◆ Mirror — this port is a monitoring port. For more information, see “<a href="#">Port Mirroring Commands</a>” on page 330.</li><li>◆ PC Mbr — this port is a member of a port channel (LAG).</li><li>◆ Probe — this port is a probe port.</li></ul>

Output	Description
Admin Mode	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	<p>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.</p> <p><b>Note</b>_____</p> <p>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.</p> <p>_____</p>
Physical Status	The port speed and duplex mode.
Link Status	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	LACP is enabled or disabled on this port.

# Port Mirroring Commands

**Introduction** Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

**monitor session** This command configures a probe port and a monitored port for monitor session (port monitoring). Use the `source interface slot/port` parameter to specify the interface to monitor. Use `rx` to monitor only ingress packets, or use `tx` to monitor only egress packets. If you do not specify an `{rx | tx}` option, the destination port monitors both ingress and egress packets. Use the `destination interface slot/port` to specify the interface to receive the monitored traffic. Use the `mode` parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Format	monitor session <i>session-id</i> {source interface slot/port [{rx   tx}]   destination interface slot/port   mode}
Mode	Global Config

**no monitor session** Use this command without optional parameters to remove 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, you must manually add the port to any desired VLANs. Use the `source interface slot/port` parameter or `destination interface` to remove the specified interface from the port monitoring session. Use the `mode` parameter to disable the administrative mode of the session.

**Note** Since the current version of CN1601 software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the `no monitor` command.

Format	no monitor session <i>session-id</i> [{source interface slot/port   destination interface   mode}]
--------	--

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

## 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 standalone no command. This command does not have a normal form.

Default	enabled
Format	no monitor
Mode	Global Config

## show monitor session

This command displays the port monitoring information for a particular mirroring session.

### Note

The *session-id* parameter is an integer value used to identify the session. In the current version of the software, the *session-id* parameter is always one (1).

Format	show monitor session <i>session-id</i>
Mode	Privileged EXEC

Output	Description
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Monitor Session Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <i>session-id</i> . The possible values are Enabled and Disabled.

Output	Description
Probe Port	Probe port (destination port) for the session identified with <i>session-id</i> . If the probe port is not set then this field is blank.
Source Port	The port, which is configured as a mirrored port (source port) for the session identified with <i>session-id</i> . If no source port is configured for the session then this field is blank.
Type	Direction in which the source port is configured for port mirroring. Types are <code>tx</code> for transmitted packets and <code>rx</code> for receiving packets.



# Port Security Commands

---

## Introduction

This section describes the commands 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 [“snmp-server enable traps violation”](#) on page 70.

---

## port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default	disabled
Format	port-security
Mode	◆ Global Config (to enable port locking globally) ◆ Interface Config (to enable port locking on an interface or range of interfaces)

## no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format	no port-security
Mode	◆ Global Config ◆ Interface Config

## port-security max-dynamic

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

Default	600
Format	port-security max-dynamic <i>maxvalue</i>

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

### **no port-security max-dynamic**

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

Format	no port-security max-dynamic
Mode	Interface Config

### **port-security max-static**

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

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

### **no port-security max-static**

This command sets maximum number of statically locked MAC addresses to the default value.

Format	no port-security max-static
Mode	Interface Config

### **port-security mac-address**

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The *vid* is the VLAN ID.

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

### **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 <i>mac-address vid</i>
Mode	Interface Config

### port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format	port-security mac-address move
Mode	Interface Config

### show port-security

This command displays the port security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

Format	show port-security [{slot/port   all}]
Mode	Privileged EXEC

For each interface, or for the interface you specify, the following information appears:

Output	Description
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.

### show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

Format	show port-security dynamic slot/port
Mode	Privileged EXEC

Output	Description
MAC Address	MAC address of dynamically locked MAC.

### show port-security static

This command displays the statically locked MAC addresses for port.

Format	show port-security static slot/port
--------	-------------------------------------

Mode	Privileged EXEC
------	-----------------

Output	Description
MAC Address	MAC address of statically locked MAC.

## show port-security violation

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

Format	show port-security violation slot/port
Mode	Privileged EXEC

Output	Description
MAC Address	MAC address of discarded packet on locked port.

# Protected Ports Commands

---

## Introduction

This section describes the commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a port channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

## switchport protected (Global Config)

This command creates a protected port group. The *groupid* parameter identifies the set of protected ports. Use the name *name* pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

**Note** Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	switchport protected <i>groupid</i> name <i>name</i>
Mode	Global Config

## no switchport protected (Global Config)

This command removes a protected port group. The *groupid* parameter identifies the set of protected ports. The name keyword specifies the name to remove from the group.

Format	no switchport protected <i>groupid</i> name
--------	---

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

### switchport protected (Interface Config)

This command adds an interface to a protected port group. The *groupid* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

#### Note

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	switchport protected <i>groupid</i>
Mode	Interface Config

### no switchport protected (Interface Config)

This command configures a port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Format	no switchport protected <i>groupid</i> name
Mode	Interface Config

### show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format	show switchport protected <i>groupid</i>
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
Group ID	The number that identifies the protected port group.

Output	Description
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.
List of Physical Ports	List of ports, which are configured as protected for the group identified with <i>groupid</i> . If no port is configured as protected for this group, this field is blank.

### show interfaces switchport

This command displays the status of the interface (protected and unprotected) under the *groupid*.

Format	show interfaces switchport slot/port <i>groupid</i>
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
Name	A string associated with this group as a convenience. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected	Indicates whether the interface is protected or not. It displays TRUE or FALSE. If the group is a multiple group, then TRUE is displayed in <i>groupid</i> .

# Provisioning (IEEE 802.1p) Commands

---

**Introduction**

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

**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 to 7. Any subsequent per port configuration will override this configuration setting.

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

**vlan priority**

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

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



# Spanning Tree Protocol Commands

## Introduction

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

**Note** STP is enabled on the switch and on all ports and LAGs by default.

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

## spanning-tree

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

Default	enabled
Format	spanning-tree
Mode	Global Config

## no spanning-tree

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

Format	no spanning-tree
Mode	Global Config

## spanning-tree auto-edge

This command configures a port as an auto-edge.

Default	The default auto-edge is true.
Format	spanning-tree auto-edge
Mode	Interface Config

### no spanning-tree auto-edge

This command sets the spanning-tree auto-edge command to false.

Format	no spanning-tree auto-edge
Mode	Interface Config

### spanning-tree bpdumigration-check

This command forces a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the slot/port parameter to transmit a BPDU from a specified interface, or use the all keyword to transmit BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a no version.

Format	spanning-tree bpdumigrationcheck {slot/port   all}
Mode	Global Config

### spanning-tree configuration name

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

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

### no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	no spanning-tree configuration name
Mode	Global Config

### spanning-tree configuration revision

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

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

### **no spanning-tree configuration revision**

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

Format	no spanning-tree configuration revision
Mode	Global Config

### **spanning-tree cost**

This command specifies an external path cost for the port used by an MST instance. Use an integer in the range of 1 to 200000000.

Format	spanning-tree cost 1-200000000
Mode	Interface Config

### **spanning-tree cost auto**

This command sets the external path cost value automatically on the basis of the link speed.

Format	spanning-tree cost auto
Mode	Interface Config

### **spanning-tree edgeport**

This command specifies that an interface (or range of interfaces) is an edge port within the common and internal spanning tree. This allows this port to transition to the Forwarding State without delay.

Format	spanning-tree edgeport
Mode	Interface Config

### no spanning-tree edgeport

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

Format	no spanning-tree edgeport
Mode	Interface Config

### spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default	802.1s
Format	spanning-tree forceversion {802.1d   802.1s   802.1w}
Mode	Global Config

- ◆ Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).
- ◆ Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- ◆ Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

### no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value.

Format	no spanning-tree forceversion
Mode	Global Config

### spanning-tree forward-time

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

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

### **no spanning-tree forward-time**

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

Format	no spanning-tree forward-time
Mode	Global Config

### **spanning-tree hold-count**

This command sets the Bridge Tx hold-count parameter to a new value for the common and internal spanning tree. The Bridge Tx hold count value is an integer from 1 to 10.

Default	3
Format	spanning-tree hold-count
Mode	Global Config

### **no spanning-tree hold-count**

This command sets the Bridge Tx hold-count parameter to the default value.

Format	spanning-tree hold-count
Mode	Global Config

### **spanning-tree max-age**

This command sets the Bridge max-age parameter to a new value for the common and internal spanning tree. The max-age value is, in seconds, within a range of 6 to 40, with the value being less than or equal to  $2 \times (\text{Bridge Forward Delay} - 1)$ .

Default	20
Format	spanning-tree max-age 6-40
Mode	Global Config

### **no spanning-tree max-age**

This command sets the Bridge max-age parameter for the common and internal spanning tree to the default value.

Format	no spanning-tree max-age
Mode	Global Config

### spanning-tree max-hops

This command sets the MSTP `max-hops` parameters 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

### 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

### 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` value 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, that is, 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	<ul style="list-style-type: none"> <li>◆ <code>cost-auto</code></li> <li>◆ <code>external-cost-auto</code></li> <li>◆ <code>port-priority-128</code></li> </ul>
Format	<code>spanning-tree mst mstid {{cost 1-200000000   auto}   {external-cost 1-200000000   auto}   port-priority 0-240}</code>
Mode	Interface Config

## no spanning-tree mst

This command sets the path cost or port priority for this port, within the multiple spanning tree instance, or in the common and internal spanning tree, to the respective default values. If 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` value, 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, to the default value, that is, a path cost value based on the link speed.

If you specify the `external-cost` option, this command sets the external-path cost for MST instance 0, that is, 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, to the default value.

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

### spanning-tree mst instance

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

Default	none
Format	spanning-tree mst instance <i>mstid</i>
Mode	Global Config

### spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The *mstid* parameter 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 <i>mstid</i> 0-61440
Mode	Global Config

### no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The *mstid* parameter 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* parameter, this command sets the bridge priority parameter for the common and internal spanning tree to the default value.

Format	no spanning-tree mst priority <i>mstid</i>
Mode	Global Config



**spanning-tree mst  
vlan**

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The *mstid* parameter is a number that corresponds to the desired existing multiple spanning tree instance. The *vlanid* can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). The VLAN IDs may or may not exist in the system.

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

**no spanning-tree  
mst vlan**

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

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

**spanning-tree port  
mode**

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

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

**no spanning-tree  
port mode**

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

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

**spanning-tree port  
mode all**

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

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

### no spanning-tree port mode all

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

Format	no spanning-tree port mode all
Mode	Global Config

### show spanning-tree

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

Format	show spanning-tree
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

The following details are displayed:

Output	Description
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.

Output	Description
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.

## show spanning-tree brief

This command displays spanning tree settings for the bridge.

Format	show spanning-tree brief
Mode	◆ Privileged EXEC ◆ User EXEC

The following information is displayed:

Output	Description
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).

## 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.

Format	show spanning-tree interface slot/port
Mode	◆ Privileged EXEC ◆ User EXEC

The following details are displayed on execution of the command:

Output	Description
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for edge delay time, to become an edge port and transition to forwarding faster.
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.
RSTP 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.

### **show spanning-tree mst detailed**

This command displays the detailed settings for an MST instance.

Format	<code>show spanning-tree mst detailed <i>mstid</i></code>
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Parameter	Description
<i>mstid</i>	A multiple spanning tree instance identifier. The value is 0 to 4094.

### 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 *mstid* parameter 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 <i>mstid</i> slot/port
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
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	Indicates whether auto calculation for Port Path Cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.

Output	Description
Designated Root	The identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
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:

Output	Description
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.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.

Output	Description
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the 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 the flag in the 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 Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.

### **show spanning-tree mst port summary**

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The *mstid* parameter indicates a particular MST instance. The {slot/port | all} parameter 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	<code>show spanning-tree mst port summary mstid {slot/port   all}</code>
--------	--



Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>
------	--

Output	Description
MST Instance ID	The MST instance associated with this port.
Interface	slot/port
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
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.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

### show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format	<code>show spanning-tree mst port summary <i>mstid</i> active</code>
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
MST Instance ID	The ID of the existing MST instance.
Interface	slot/port

Output	Description
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
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.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

### show spanning-tree mst summary

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

Format	show spanning-tree mst summary
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

On execution, the following details are displayed:

Output	Description
MST Instance ID List	List of multiple spanning tree IDs currently configured.
For each MSTID: <ul style="list-style-type: none"> <li>◆ Associated FIDs</li> <li>◆ Associated VLANs</li> </ul>	<ul style="list-style-type: none"> <li>◆ List of forwarding database identifiers associated with this instance.</li> <li>◆ List of VLAN IDs associated with this instance.</li> </ul>

## show spanning-tree summary

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

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

The following details are displayed on execution of the command.

Output	Description
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.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
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	A generated key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

## show spanning-tree vlan

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

Format	<code>show spanning-tree vlan <i>vlanid</i></code>
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
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.

# Static MAC Filtering Commands

## Introduction

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

## macfilter

This command adds a static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. The value of the *macaddr* parameter is 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.

The number of static MAC filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured. For example:

- ◆ For unicast MAC address filters and multicast MAC address filters with source port lists, the maximum number of static MAC filters supported is 20.
- ◆ For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 256.

For the NetApp CN1601 switches, you can configure the following combinations:

- ◆ Unicast MAC and source port (max = 20)
- ◆ Multicast MAC and source port (max = 20)
- ◆ Multicast MAC and destination port (only) (max = 256)
- ◆ Multicast MAC and source ports and destination ports (max = 20)

Format	macfilter macaddr vlanid
Mode	Global Config

## 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	<code>no macfilter macaddr vlanid</code>
Mode	Global Config

### **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.

---

#### **Note**

Configuring a destination port list is only valid for multicast MAC addresses.

---

Format	<code>macfilter adddest macaddr vlanid</code>
Mode	Interface Config

### **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	<code>no macfilter adddest macaddr vlanid</code>
Mode	Interface Config

### **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.

---

#### **Note**

Configuring a destination port list is only valid for multicast MAC addresses.

---

Format	<code>macfilter adddest all macaddr vlanid</code>
Mode	Global Config

**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 <i>macaddr</i> <i>vlanid</i>
Mode	Global Config

**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 <i>macaddr</i> <i>vlanid</i>
Mode	Interface Config

**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 <i>macaddr</i> <i>vlanid</i>
Mode	Interface Config

**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 <i>macaddr</i> <i>vlanid</i>
Mode	Global Config

**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	<code>no macfilter addsrc all <i>macaddr</i> <i>vlanid</i></code>
Mode	Global Config

### **show mac-address-table static**

This command displays the static MAC filtering information for all static MAC filters. If you specify *all*, all the static MAC filters in the system are displayed. If you supply a value for *macaddr*, you must also enter a value for *vlanid*, and the system displays static MAC filter information only for that MAC address and VLAN.

Format	<code>show mac-address-table static {<i>macaddr</i> <i>vlanid</i>   all}</code>
Mode	Privileged EXEC

Output	Description
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port (s)	The source port filter set's slot and port(s).

### **Note**

Only multicast address filters will have destination port lists.

### **show mac-address-table staticfiltering**

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

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

Output	Description
VLAN ID	The VLAN in which the MAC address is learned.



Output	Description
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is six 2-digit hexadecimal numbers that are separated by colons, for example, 01:23:45:67:89:AB.
Type	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:).

# Storm-Control Commands

---

## Introduction

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

FASTPATH provides broadcast, multicast, and unicast storm recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the `no` version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the `no` version of the `storm-control` command (not stating a `level`) disables that form of storm-control but maintains the configured `level` (to be active the next time that form of storm-control is enabled.)

---

### Note

The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes – used to calculate a packet-per-second (pps) rate – as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512-byte packets are used.

---

### **storm-control broadcast**

This command enables broadcast storm recovery mode for a specific interface or range of interfaces. If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	disabled
Format	storm-control broadcast
Mode	◆ Global Config ◆ Interface Config

### **no storm-control broadcast**

This command disables broadcast storm recovery mode for a specific interface or range of interfaces.

Format	no storm-control broadcast
Mode	◆ Global Config ◆ Interface Config

### **storm-control broadcast level**

This command configures the broadcast storm recovery threshold for an interface as a percentage of link speed and enables broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	5
Format	storm-control broadcast level <i>0-100</i>
Mode	Interface Config

### **no storm-control broadcast level**

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format	no storm-control broadcast level
--------	----------------------------------

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

### **storm-control broadcast rate**

This command configures the broadcast storm recovery threshold for an interface in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	0
Format	<code>storm-control broadcast rate 0-33554431</code>
Mode	Interface Config

### **no storm-control broadcast rate**

This command configures the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format	<code>no storm-control broadcast rate</code>
Mode	Interface Config

### **storm-control broadcast all**

This command enables broadcast storm recovery mode for all interfaces. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	disabled
Format	<code>storm-control broadcast all</code>
Mode	Global Config

### **no storm-control broadcast all**

This command disables broadcast storm recovery mode for all interfaces.

Format	<code>no storm-control broadcast all</code>
--------	---

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

### **storm-control broadcast all level**

This command configures the broadcast storm recovery threshold for all interfaces as a percentage of link speed and enables broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold. This command also enables broadcast storm recovery mode for all interfaces.

Default	5
Format	<code>storm-control broadcast all level 0-100</code>
Mode	Global Config

### **no storm-control broadcast all level**

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

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

### **storm-control broadcast all rate**

This command configures the broadcast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	0
Format	<code>storm-control broadcast all rate 0-33554431</code>
Mode	Global Config

### **no storm-control broadcast all rate**

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format	no storm-control broadcast all rate
Mode	Global Config

## storm-control multicast

This command enables multicast storm recovery mode for an interface or range of interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	disabled
Format	storm-control multicast
Mode	Interface Config

## no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Format	no storm-control multicast
Mode	Interface Config

## storm-control multicast level

This command configures the multicast storm recovery threshold for an interface as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	storm-control multicast level 0-100
Mode	Interface Config

**no storm-control  
multicast level**

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	<code>no storm-control multicast level 0-100</code>
Mode	Interface Config

**storm-control  
multicast rate**

This command configures the multicast storm recovery threshold for an interface in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	<code>storm-control multicast rate 0-33554431</code>
Mode	Interface Config

**no storm-control  
multicast rate**

Use this command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	<code>no storm-control multicast rate</code>
Mode	Interface Config

**storm-control  
multicast all**

This command enables multicast storm recovery mode for all interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	disabled
Format	<code>storm-control multicast all</code>
Mode	Global Config

### **no storm-control multicast all**

This command disables multicast storm recovery mode for all interfaces.

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

### **storm-control multicast all level**

This command configures the multicast storm recovery threshold for all interfaces as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	<code>storm-control multicast all level 0-100</code>
Mode	Global Config

### **no storm-control multicast all level**

This command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

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

### **storm-control multicast all rate**

This command configures the multicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	<code>storm-control multicast all rate 0-33554431</code>
Mode	Global Config



### **no storm-control multicast all rate**

This command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

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

### **storm-control unicast**

This command enables unicast storm recovery mode for an interface or range of interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	disabled
Format	<code>storm-control unicast</code>
Mode	Interface Config

### **no storm-control unicast**

This command disables unicast storm recovery mode for an interface.

Format	<code>no storm-control unicast</code>
Mode	Interface Config

### **storm-control unicast level**

This command configures the unicast storm recovery threshold for an interface as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold. This command also enables unicast storm recovery mode.

Default	5
Format	<code>storm-control unicast level 0-100</code>
Mode	Interface Config

### **no storm-control unicast level**

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

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

### **storm-control unicast rate**

This command configures the unicast storm recovery threshold for an interface in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default	0
Format	<code>storm-control unicast rate 0-33554431</code>
Mode	Interface Config

### **no storm-control unicast rate**

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Format	<code>no storm-control unicast rate</code>
Mode	Interface Config

### **storm-control unicast all**

This command enables unicast storm recovery mode for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	disabled
Format	<code>storm-control unicast all</code>
Mode	Global Config

**no storm-control  
unicast all**

This command disables unicast storm recovery mode for all interfaces.

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

**storm-control  
unicast all level**

This command configures the unicast storm recovery threshold for all interfaces as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	5
Format	<code>storm-control unicast all level 0-100</code>
Mode	Global Config

**no storm-control  
unicast all level**

This command sets the unicast storm recovery threshold to the default value and disables unicast storm recovery for all interfaces.

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

**storm-control  
unicast all rate**

This command configures the unicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default	0
Format	<code>storm-control unicast all rate 0-33554431</code>
Mode	Global Config

### **no storm-control unicast all rate**

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	no storm-control unicast all rate
Mode	Global Config

### **storm-control flowcontrol**

This command enables 802.3x flow control for the switch and applies only 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	◆ Interface Config ◆ Global Config

### **no storm-control flowcontrol**

This command disables 802.3x flow control for the switch.

---

#### **Note**

This command applies only to full-duplex mode ports.

---

Format	no storm-control flowcontrol
Mode	◆ Interface Config ◆ Global Config

### **show storm-control**

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- ◆ **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.

Use the `all` keyword to display the per-port configuration parameters for all interfaces, or specify the slot/port to display information about a specific interface.

Format	<code>show storm-control [all   slot/port]</code>
Mode	Privileged EXEC

Output	Description
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#show storm-control
802.3x Flow Control Mode..... Disable
```

**Example:** The following shows example CLI display output for the command:

```
(CN1601)#show storm-control 1/0/1
```

Intf	Bcast Mode	Bcast Level	Mcast Mode	Mcast Level	Ucast Mode	Ucast Level
1/0/1	Disable	5%	Disable	5%	Disable	5%

**Example:** The following shows an example of part of the CLI display output for the command:

(CN1601)#show storm-control all

Intf	Bcast Mode	Bcast Level	Mcast Mode	Mcast Level	Ucast Mode	Ucast Level
1/0/1	Disable	5%	Disable	5%	Disable	5%
1/0/2	Disable	5%	Disable	5%	Disable	5%
1/0/3	Disable	5%	Disable	5%	Disable	5%
1/0/4	Disable	5%	Disable	5%	Disable	5%
1/0/5	Disable	5%	Disable	5%	Disable	5%

# VLAN Commands

---

Introduction	This section describes the commands you use to configure VLAN settings.						
vlan database	This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics. <table><tr><td>Format</td><td>vlan database</td></tr><tr><td>Mode</td><td>Privileged EXEC</td></tr></table>	Format	vlan database	Mode	Privileged EXEC		
Format	vlan database						
Mode	Privileged EXEC						
network mgmt_vlan	This command configures the Management VLAN ID. The VLAN range is 1 to 4093. <table><tr><td>Default</td><td>1</td></tr><tr><td>Format</td><td>network mgmt_vlan 1-4093</td></tr><tr><td>Mode</td><td>Privileged EXEC</td></tr></table>	Default	1	Format	network mgmt_vlan 1-4093	Mode	Privileged EXEC
Default	1						
Format	network mgmt_vlan 1-4093						
Mode	Privileged EXEC						
no network mgmt_vlan	This command sets the Management VLAN ID to the default. <table><tr><td>Format</td><td>no network mgmt_vlan</td></tr><tr><td>Mode</td><td>Privileged EXEC</td></tr></table>	Format	no network mgmt_vlan	Mode	Privileged EXEC		
Format	no network mgmt_vlan						
Mode	Privileged EXEC						
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). The VLAN range is 2 to 4093. <table><tr><td>Format</td><td>vlan 2-4093</td></tr><tr><td>Mode</td><td>VLAN Config</td></tr></table>	Format	vlan 2-4093	Mode	VLAN Config		
Format	vlan 2-4093						
Mode	VLAN Config						

## 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 to 4093.

Format	no vlan 2-4093
Mode	VLAN Config

## vlan acceptframe

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

Default	all
Format	vlan acceptframe {vlanonly   all}
Mode	Interface Config

## no vlan acceptframe

This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format	no vlan acceptframe
Mode	Interface Config

## vlan ingressfilter

This command enables ingress filtering on an interface or range of interfaces. 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



**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

**vlan makestatic** This command changes a dynamically created VLAN (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 to 4093.

Format	vlan makestatic 2-4093
Mode	VLAN Config

**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. The ID range is 1 to 4093.

Default	<ul style="list-style-type: none"> <li>◆ VLAN ID 1 - default</li> <li>◆ other VLANs - blank string</li> </ul>
Format	vlan name 1-4093 name
Mode	VLAN Config

**no vlan name** This command sets the name of a VLAN to a blank string.

Format	no vlan name
Mode	VLAN Config

**vlan participation** This command configures the degree of participation for a specific interface or range of interfaces 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} 1-4093
Mode	Interface Config

Participation options are:

Parameter	Description
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 and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

## vlan participation all

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

Format	vlan participation all {exclude   include   auto} 1-4093
Mode	Global Config

Participation options are:

Parameter	Description
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.

Parameter	Description
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 and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

### **vlan port acceptframe all**

This command sets the frame acceptance mode for all interfaces.

Default	all
Format	vlan port acceptframe all {vlanonly   all}
Mode	Global Config

The modes are defined as follows:

Parameter	Description
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.

### **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
------	---------------

### **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

### **no vlan port ingressfilter all**

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

Format	no vlan port ingressfilter all
Mode	Global Config

### **vlan port pvid all**

This command changes the VLAN ID for an interface.

Default	1
Format	vlan port pvid 1-4093
Mode	Global Config

### **no vlan port pvid all**

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

Format	no vlan port pvid
Mode	Global Config

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

Format	vlan port tagging all 1-4093
Mode	Global Config

**no vlan port tagging all** This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	no vlan port tagging all
Mode	Global Config

**vlan pvid** This command changes the VLAN ID on an interface or range of interfaces.

Default	1
Format	vlan pvid 1-4093
Mode	<ul style="list-style-type: none"> <li>◆ Interface Config</li> <li>◆ Interface Range Config</li> </ul>

**no vlan pvid** This command sets the VLAN ID on an interface or range of interfaces to 1.

Format	no vlan pvid
Mode	Interface Config

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

Format	<code>vlan tagging 1-4093</code>
Mode	Interface Config

### **no vlan tagging**

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

Format	<code>vlan tagging 1-4093</code>
Mode	Interface Config

### **vlan association mac**

This command associates a MAC address to a VLAN.

Format	<code>vlan association mac <i>macaddr</i> <i>vlanid</i></code>
Mode	VLAN database

### **no vlan association mac**

This command removes the association of a MAC address to a VLAN.

Format	<code>no vlan association mac <i>macaddr</i></code>
Mode	VLAN database

### **show vlan**

This command displays detailed information, including interface information, for a specified VLAN. The ID is a valid VLAN identification number in the range 1 to 4093.

Format	<code>show vlan <i>vlanid</i></code>
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
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 the default (VLAN ID = 1) or static (one that is configured and permanently defined), or a dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) if a RADIUS-assigned VLAN does not exist on the switch.
Interface	slot/port. It is possible to set the parameters for all ports by using the selectors on the top line.
Current	<p>The degree of participation of this port in this VLAN. The permissible values are:</p> <ul style="list-style-type: none"> <li>◆ Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</li> <li>◆ Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</li> <li>◆ Autodetect - 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.</li> </ul>

Output	Description
Configured	<p>The configured degree of participation of this port in this VLAN. The permissible values are:</p> <ul style="list-style-type: none"> <li>◆ Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</li> <li>◆ Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</li> <li>◆ Autodetect - 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.</li> </ul>
Tagging	<p>The tagging behavior for this port in this VLAN.</p> <ul style="list-style-type: none"> <li>◆ Tagged - Transmit traffic for this VLAN as tagged frames.</li> <li>◆ Untagged - Transmit traffic for this VLAN as untagged frames.</li> </ul>

### show vlan internal usage

This command displays a list of all configured VLANs.

Format	show vlan internal usage
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
Base VLAN ID	Identifies the base VLAN ID for internal allocation of VLANs to the routing interface.
Allocation Policy	Identifies whether the system allocates VLAN IDs in ascending or descending order.



**show vlan brief**

This command displays a list of all configured VLANs.

Format	show vlan brief
Mode	◆ Privileged EXEC ◆ User EXEC

Output	Description
VLAN ID	There is a VLAN identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
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 the default (VLAN ID = 1) or static (one that is configured and permanently defined), or dynamic (one that is created by GVRP registration).

**show vlan port**

This command displays VLAN port information.

Format	show vlan port {slot/port all}
Mode	◆ Privileged EXEC ◆ User EXEC

Output	Description
Interface	slot/port. 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.

Output	Description
Acceptable Frame Types	The types of frames that may be received on this port. The options are <code>VLAN only</code> and <code>Admit All</code> . When set to <code>VLAN only</code> , untagged frames or priority tagged frames received on this port are discarded. When set to <code>Admit All</code> , 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.

# Voice VLAN Commands

---

## Introduction

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

## voice vlan (Global Config)

This command enables the Voice VLAN capability on the switch.

Default	disabled
Format	voice vlan
Mode	Global Config

## no voice vlan (Global Config)

This command disables the Voice VLAN capability on the switch.

Format	no voice vlan
Mode	Global Config

## voice vlan (Interface Config)

This command enables the Voice VLAN capability on the interface or range of interfaces.

Default	disabled
Format	voice vlan {vlanid <i>id</i>   dot1p <i>priority</i>   none   untagged}
Mode	Interface Config

You can configure Voice VLAN in one of four different ways:

Parameter	Description
vlanid	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4093 (the maximum supported by the platform).
dot1p	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid <i>priority</i> range is 0 to 7.
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

### no voice vlan (Interface Config)

This command disables the Voice VLAN capability on the interface.

Format	no voice vlan
Mode	Interface Config

### voice vlan data priority

This command either trusts or untrusts the data traffic arriving on the Voice VLAN interface or range of interfaces being configured.

Default	trust
Format	voice vlan data priority {untrust   trust}
Mode	Interface Config

### show voice vlan

This command displays the global or interface VLAN parameters.

Format	show voice vlan [interface {slot/port   all}]
Mode	Privileged EXEC

When the *interface* parameter is not specified, only the global mode of the Voice VLAN is displayed.

Output	Description
Administrative Mode	The Global Voice VLAN mode.

When the interface is specified:

Output	Description
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID.
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.



## About this chapter

This chapter describes the IPv6 Management commands available in the CN1601 CLI.

## Topics in this chapter

This chapter includes the following sections:

- ◆ “[IPv6 Management Commands](#)” on page 396

---

### CAUTION

The commands in this chapter 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.
-

# IPv6 Management Commands

---

## Introduction

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (that is, independent from the IPv6 Routing package). For Routing/IPv6 builds of FASTPATH, dual IPv4/IPv6 operation over the service port is enabled. FASTPATH has capabilities such as:

- ◆ Static assignment of IPv6 addresses and gateways for the service/network ports.
- ◆ The ability to ping an IPv6 link-local address over the service/network port.
- ◆ Using IPv6 Management commands, you can send SNMP traps and queries via the service/network port.
- ◆ The user can manage a device via the network port (in addition to a Routing Interface or the Service port).

**network ipv6 enable** This command enables IPv6 operation on the network port.

Default	enabled
Format	network ipv6 enable
Mode	Privileged EXEC

**no network ipv6 enable** This command disables IPv6 operation on the network port.

Format	no network ipv6 enable
Mode	Privileged EXEC

**network ipv6 address** This command lets you manually configure IPv6 global address, enable/disable stateless global address autoconfiguration, and enable/disable dhcpv6 client protocol information for the network port. You can configure multiple IPv6 addresses on the network port.



Format	network ipv6 address { <i>address/prefix-length</i> [eui64]   autoconfig   dhcp}
Mode	Privileged EXEC

Parameter	Description
<i>address</i>	IPv6 prefix in IPv6 global address format.
<i>prefix-length</i>	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure DHCPv6 client protocol.

### no network ipv6 address

This command removes all configured IPv6 prefixes.

Use this command with the *address* option to remove the manually configured IPv6 global address on the network port interface.

Use this command with the *autoconfig* option to disable the stateless global address autoconfiguration on the network port.

Use this command with the *dhcp* option to disable the dhcpv6 client protocol on the network port.

Format	no network ipv6 address { <i>address/prefix-length</i> [eui64]   autoconfig   dhcp}
Mode	Privileged EXEC

### network ipv6 gateway

This command configures the IPv6 gateway (that is, default routers) information for the network port.

Format	network ipv6 gateway <i>gateway-address</i>
--------	---

Mode	Privileged EXEC
------	-----------------

Parameter	Description
<i>gateway-address</i>	Gateway address in IPv6 global or link-local address format.

### **no network ipv6 gateway**

This command removes IPv6 gateways on the network port interface.

Format	no network ipv6 gateway
Mode	Privileged EXEC

### **show network ndp**

This command displays NDP cache information for the network port.

Default	enabled
Format	show network ndp
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

Output	Description
IPv6 Address	The IPv6 address of the interface.
MAC Address	The MAC address used.
isRtr	Specifies the router flag.
Neighbor State	The state of the neighbor cache entry. Possible values are Reachable and Delay.
Age Updated	The time, in seconds, that has elapsed since an entry was added to the cache.

**Example:** The following shows example CLI display output for the command:  
(CN1601) #show network ndp

IPv6 Address	MAC Address	isRtr	Neighbor State	Age Updated
-----	-----	-----	-----	-----
3017::204:76FF:FE73:423A	00:04:76:73:42:3a		Reachable	447535
FE80::204:76FF:FE73:423A	00:04:76:73:42:3a		Delay	447540

## clear network ipv6 dhcp statistics

This command clears the DHCPv6 statistics on the network management interface.

Format	clear network ipv6 dhcp statistics
Mode	Privileged EXEC

## ping ipv6

This command determines whether another computer is on the network. It provides a synchronous response when initiated from the CLI and Web interfaces. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *ipv6-address/hostname* parameter to ping an interface by using the global IPv6 address of the interface. Use the optional *size* keyword to specify the size of the ping packet.

You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address *ipv6-global-address/hostname*. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping or traceroute request is routed out the service/network port properly. When referencing an IPv6 link-local address, you must also specify the service or network port interface by using the *serviceport* or *network* parameter.

Default	<ul style="list-style-type: none"> <li>◆ The default count is 1.</li> <li>◆ The default interval is 3 seconds.</li> <li>◆ The default size is 0 bytes.</li> </ul>
---------	---

Format	ping ipv6 { <i>ipv6-global-address</i> / <i>hostname</i>   {interface {slot/port   serviceport   network} <i>link-local-address</i> } [size <i>datagram-size</i> ]}
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

## ping ipv6 interface

This command determines whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *interface* keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. You can use a loopback, network port, serviceport, tunnel, or physical interface as the source. Use the optional *size* keyword to specify the size of the ping packet. The *ipv6-address* is the link local IPv6 address of the device you want to query.

Format	ping ipv6 interface {slot/port   loopback <i>loopback-id</i>   network   serviceport   tunnel <i>tunnel-id</i> } {link-local-address <i>link-local-address</i>   <i>ipv6-address</i> } [size <i>datagram-size</i> ]
Mode	<ul style="list-style-type: none"> <li>◆ Privileged EXEC</li> <li>◆ User EXEC</li> </ul>

## traceroute ipv6

This command discovers the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The *ipv6-address* parameter must be a valid IPv6 address. 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. The range for *port* is 0 (zero) to 65535. The default value is 33434.

Format	traceroute ipv6 <i>ipv6-address</i> [port]
Mode	Privileged EXEC

**show network ipv6  
dhcp statistics**

This command displays the statistics of the DHCPv6 client running on the network management interface.

Format	show network ipv6 dhcp statistics
Mode	◆ Privileged EXEC ◆ User EXEC

Output	Description
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.

Output	Description
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the network interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the network interface.
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the network interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the network interface.

**Example:** The following shows example CLI display output for this command:  
(CN1601) #show network ipv6 dhcp statistics

```
DHCPv6 Client Statistics
-----
DHCPv6 Advertisement Packets Received..... 0
DHCPv6 Reply Packets Received..... 0
Received DHCPv6 Advertisement Packets Discard.. 0
Received DHCPv6 Reply Packets Discarded..... 0
DHCPv6 Malformed Packets Received..... 0
Total DHCPv6 Packets Received..... 0
DHCPv6 Solicit Packets Transmitted..... 0
DHCPv6 Request Packets Transmitted..... 0
DHCPv6 Renew Packets Transmitted..... 0
DHCPv6 Rebind Packets Transmitted..... 0
DHCPv6 Release Packets Transmitted..... 0
Total DHCPv6 Packets Transmitted..... 0
```

## About this chapter

This chapter describes the Quality of Service (QoS) commands available with the CN1601 CLI.

## Topics in this chapter

This chapter includes the following sections:

- ◆ “[Auto-Voice over IP Commands](#)” on page 404
- ◆ “[IP Access Control List Commands](#)” on page 406
- ◆ “[MAC Access Control List Commands](#)” on page 416
- ◆ “[Time Range Commands for Time-Based ACLs](#)” on page 422

---

### CAUTION

The commands in this chapter 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.
-

# Auto-Voice over IP Commands

---

## Introduction

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- ◆ Session Initiation Protocol (SIP)
- ◆ H.323
- ◆ Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

## auto-voip all

This command enables VoIP Profile on the interfaces of the switch.

Default	disabled
Format	auto-voip all
Mode	Global Config

## no auto-voip all

This command disables VoIP Profile on the interfaces of the switch.

Format	no auto-voip all
Mode	Global Config

## auto-voip

This command enables VoIP Profile on an interface or range of interfaces.

Default	disabled
Format	auto-voip
Mode	Interface Config



**no auto-voip**

This command disables VoIP Profile on the interface.

Format	no auto-voip all
Mode	Interface Config

**show auto-voip**

This command displays the VoIP Profile settings on the interface or interfaces of the switch.

Format	show auto-voip interface {slot/port   all}
Mode	Privileged EXEC

Output	Description
AutoVoIP Mode	The Auto VoIP mode on the interface.
Traffic Class	The CoS Queue or Traffic Class to which all VoIP traffic is mapped to. This cannot be configured and defaults to the highest CoS queue available in the system for data traffic.

# IP Access Control List Commands

## Introduction

This section describes the commands you use to configure IP Access Control List (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:

- ◆ FASTPATH software does not support IP ACL configuration for IP packet fragments.
- ◆ The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- ◆ The maximum number of rules per IP ACL is hardware dependent.
- ◆ On CN1601 switches, 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 (1s) in the bit positions that are used for the network address, and has zeros (0s) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0s) 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.

## access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1 to 99 for standard ACLs or 100 to 199 for extended ACLs. The following parameter table describes the parameters for the `access-list` command.

IP Standard ACL:

Format	<code>access-list 1-99 {deny   permit} {every   <i>srcip srcmask</i>} [log] [time-range <i>time-range-name</i>] [assign-queue <i>queue-id</i>] [{mirror   redirect} slot/port]</code>
Mode	Global Config

## IP Extended ACL:

Format	<code>access-list 100-199 {deny   permit} {every   [{icmp   igmp   ip   tcp   udp   number} srcip srcmask [{eq {portkey   0-65535} dstip dstmask [{eq {portkey   0-65535}} [precedence precedence   tos tos tosmask   dscp dscp] [log] [time-range time-range-name] [assign-queue queue-id] [{mirror   redirect} slot/port]</code>
Mode	Global Config

Parameter	Description
<i>1-99 or 100-199</i>	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
<code>{deny   permit}</code>	Specifies whether the IP ACL rule permits or denies an action.
<code>every</code>	Match every packet.
<code>{icmp   igmp   ip   tcp   udp   number}</code>	Specifies the protocol to filter for an extended IP ACL rule.
<code>srcip srcmask</code>	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
<code>[{eq {portkey   0-65535}}]</code>	Specifies the source Layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0 to 65535, or you specify the <i>portkey</i> , which can be one of the following keywords: <i>domain</i> , <i>echo</i> , <i>ftp</i> , <i>ftpdata</i> , <i>http</i> , <i>smtp</i> , <i>snmp</i> , <i>telnet</i> , <i>tftp</i> , and <i>www</i> . Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
<code>dstip dstmask</code>	Specifies a destination IP address and netmask for match condition of the IP ACL rule.

Parameter	Description
[precedence <i>precedence</i>   <i>tos tos</i> <i>tosmask  </i> <i>dscp dscp</i> ]	Specifies the ToS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters <i>dscp</i> , <i>precedence</i> , <i>tos</i> <i>tosmask</i> .
[log]	Specifies that this rule is to be logged.
[time-range <i>time-range-</i> <i>name</i> ]	Allows you to set an imposing time limitation on the ACL rule as defined by the parameter <i>time-range-name</i> . If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with a specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with the specified name becomes inactive.
[assign-queue <i>queue queue-</i> <i>id</i> ]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
[{mirror   redirect} slot/port]	For CN1601 switches, specifies the mirror or redirect interface which is the slot/port to which packets matching this rule are copied or forwarded, respectively. The <i>mirror</i> and <i>redirect</i> parameters are not available on the CN1601 switch.

## no access-list

This command deletes an IP ACL that is identified by the parameter *accesslistnumber* from the system. The range for *accesslistnumber* 1 to 99 for standard access lists and 100 to 199 for extended access lists.

Format	<code>no access-list <i>accesslistnumber</i></code>
Mode	Global Config

**ip access-list** This command creates an extended IP Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv4 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access\_List config mode to allow updating the existing IP ACL.

**Note**—  
The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format	ip access-list <i>name</i>
Mode	Global Config

**no ip access-list** This command deletes the IP Access Control List (ACL) identified by *name* from the system.

Format	no ip access-list <i>name</i>
Mode	Global Config

**ip access-list rename** This command changes the name of an IP Access Control List (ACL). The *name* parameter is the names of an existing IP ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails if an IP ACL by the name *newname* already exists.

Format	ip access-list rename <i>name newname</i>
Mode	Global Config

**{deny|permit} (IP ACL)**

This command creates a new rule for the current IP 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 an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and re-specified.

**Note**  
An implicit `deny all` IP rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the `every` keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified 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.

The `time-range` parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with the specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with the specified name becomes inactive.

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` parameter is valid only for a permit rule.

Format	{deny   permit} {every   {{icmp   igmp   ip   tcp   udp   number} srcip srcmask[ {eq {portkey   0-65535} dstip dstmask [ {eq {portkey   0-65535} ] [precedence precedence   tos tos tosmask   dscp dscp] [log] [time-range time-range-name] [assign-queue queue-id] [{mirror   redirect} slot/port]
Mode	Ipv4-Access-List Config

**ip access-group** This command either attaches a specific IP Access Control List (ACL) identified by *accesslistnumber* to an interface, range of interfaces, or all interfaces; or associates it with a VLAN ID in a given direction. The parameter *name* is the name of the ACL.

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.

**Note**  
The *out* option may or may not be available, depending on the platform.

Default	none
Format	ip access-group <i>accesslistnumber</i> <i>name</i> [vlan <i>vlan-id</i> ] in   out [sequence 1-4294967295]
Mode	◆ Interface Config ◆ Global Config

**no ip access-group** This command removes a specified IP ACL from an interface.

Default	none
Format	no ip access-group <i>accesslistnumber</i> [vlan <i>vlan-id</i> ] in
Mode	◆ Interface Config ◆ Global Config

## acl-trapflags

This command enables the ACL trap mode.

Default	disabled
Format	acl-trapflags
Mode	Global Config

## no acl-trapflags

This command disables the ACL trap mode.

Format	no acl-trapflags
Mode	Global Config

## show ip access-lists

This command displays summary information about all IP ACLs configured on the switch. To view more detailed information about a specific access list, specify the ACL number or name that is used to identify the IP ACL.

Format	show ip access-lists [ <i>accesslistnumber</i>   <i>name</i> ]
Mode	Privileged EXEC

Output	Description
ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).



If you specify an IP ACL number or name, the following information displays:

**Note**

Only the access list fields that you configure are displayed.

Output	Description
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified for IP Precedence.
IP ToS	The value specified for IP ToS.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.

Output	Description
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IP ACL rule.

### **show access-lists interface**

This command displays IP ACLs and MAC access control lists information for a designated interface and direction.

Format	<code>show access-lists interface slot/port in out</code>
Mode	Privileged EXEC

Output	Description
ACL Type	Type of access list (IP or MAC).
ACL ID	Access control list name for a MAC 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).

Output	Description
in out	<ul style="list-style-type: none"> <li>◆ in—Display Access List information for a particular interface in the in direction.</li> <li>◆ out—Display Access List information for a particular interface in the out direction.</li> </ul>

## show access-lists vlan

This command displays Access List information for a particular VLAN ID and direction.

Format	show access-lists vlan <i>vlan-id</i> in out
Mode	Privileged EXEC

Output	Description
vlan-id	A VLAN ID.
in out	<ul style="list-style-type: none"> <li>◆ in—Display Access List information for a particular VLAN ID in the in direction.</li> <li>◆ out—Display Access List information for a particular VLAN ID in the out direction.</li> </ul>

# MAC Access Control List Commands

## Introduction

This section describes the commands you use to configure MAC Access Control List (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 can create is hardware-dependent. The limit applies to all ACLs, regardless of type.
- ◆ The system supports only Ethernet II frame types.
- ◆ The maximum number of rules per MAC ACL is hardware-dependent.
- ◆ For the CN1601 switch, if you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

## 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 <i>name</i>
Mode	Global Config

## no mac access-list extended

This command deletes a MAC ACL identified by *name* from the system.

Format	no mac access-list extended <i>name</i>
Mode	Global Config

**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 <i>name newname</i>
Mode	Global Config

**{deny / permit}  
(MAC ACL)**

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. Rather, the entire MAC ACL must be deleted and re-specified.

**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.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF, as shown in the following table. The currently supported ethertypekey values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mpls multicast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5

Ethertype Keyword	Corresponding Value
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 `time-range` parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter `time-range-name`. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with a specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with the specified name becomes inactive.

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` parameter is valid only for a permit rule.

For the CN1601 switch, the `mirror` parameter allows the traffic matching this rule to be copied to the specified slot/port, while the `redirect` parameter allows the traffic matching this rule to be forwarded to the specified slot/port. The `assign-queue` and `redirect` 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] [[log] [time-range time-range-name] [assign-queue queue-id]] [{mirror   redirect} slot/port]
Mode	Mac-Access-List Config

**mac access-group**

This command either attaches a specific MAC Access Control List (ACL) identified by *name* to an interface, or associates it with a VLAN ID, 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 *vlan* keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

---

**Note**

---

The *out* option may or may not be available, depending on the platform.

---

Format	mac access-group <i>name</i> [vlan <i>vlan-id</i> ] [in out] [sequence 1-4294967295]
Mode	◆ Global Config ◆ Interface Config

## no mac access-group

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

Format	no mac access-group <i>name</i> [vlan <i>vlan-id</i> ] in
Mode	◆ Global Config ◆ Interface Config

## show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the [*name*] parameter to identify a specific MAC ACL to display.

Format	show mac access-lists [ <i>name</i> ]
Mode	Privileged EXEC

Output	Description
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The EtherType keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	On CN1601 switches, the slot/port to which packets matching this rule are copied.



Output	Description
Redirect Interface	On CN1601 switches, the slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the MAC ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the MAC ACL rule.

# Time Range Commands for Time-Based ACLs

---

**Introduction**

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit *deny all* rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined with in an ACL.

**time-range**

This command creates a time range identified by *name*, consisting of one absolute time entry and/or one or more periodic time entries. The *name* parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alphanumeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries.

**Note**

---

When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

---

Format	time-range <i>name</i>
Mode	Global Config

**no time-range**

This command deletes a time range identified by *name*.

Format	no time-range <i>name</i>
Mode	Global Config

## absolute

This command adds an absolute time entry to a time range. Only one absolute time entry is allowed per time range. The *time* parameter is based on the currently configured time zone.

The `[start time date]` parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 AM and 20:00 is 8:00 PM. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The `[end time date]` parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format	absolute {[start time date] [end time date]}
Mode	Time-Range Config

## no absolute

This command deletes the absolute time entry in the time range.

Format	no absolute
Mode	Time-Range Config

## periodic

This command adds a periodic time entry to a time range. The *time* parameter is based off of the currently configured time zone.

The first occurrence of the `days-of-the-week` argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end `days-of-the-week` are the same as the start, they can be omitted.

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- ◆ daily—Monday through Sunday
- ◆ weekdays—Monday through Friday
- ◆ weekend—Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

The first occurrence of the *time* argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 AM and 20:00 is 8:00 PM.

Format	periodic {days-of-the-week <i>time</i> } to {[days-of-the-week] <i>time</i> }
Mode	Time-Range Config

### no periodic

This command deletes a periodic time entry from a time range.

Format	no periodic {days-of-the-week <i>time</i> } to {[days-of-the-week] <i>time</i> }
Mode	Time-Range Config

### clock timezone

This command sets the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either 0 or \0 as appropriate. The *acronym* parameter is the acronym that represents the time zone and can be up to four characters.

Format	clock timezone {hours} [minutes <i>minutes</i> ] [zone <i>acronym</i> ]
Mode	Global Config

### show clock detail

This command displays time zone and summertime configuration.

Format	show clock detail
Mode	Privileged EXEC

**show time-range**

This command displays a time range and all the absolute/periodic time entries that are defined for the time range. Use the *name* parameter to identify a specific time range to display. When *name* is not specified, all the time ranges defined in the system are displayed.

Format	show time-range <i>name</i>
Mode	Privileged EXEC

Output	Description
Number of Time Ranges	Number of time ranges configured in the system.
Time Range Name	Name of the time range.
Time Range Status	Status of the time range (active/inactive)
Absolute start	Start time and day for absolute time entry.
Absolute end	End time and day for absolute time entry.
Periodic Entries	Number of periodic entries in a time-range.
Periodic start	Start time and day for periodic entry.
Periodic end	End time and day for periodic entry.



# Command Index

## Symbols

{deny / permit} (MAC ACL) 417  
{deny|permit} (IP ACL) 410

## Numerics

802.1X Supplicant Commands 226

## A

aaa authentication dot1x default 284  
aaa authentication enable 88  
aaa authentication login 86  
aaa ias-user username 109  
About this chapter 29, 113, 213, 395, 403  
absolute 423  
Access Commands 30  
access-list 406  
acl-trapflags 412  
addport 305  
adminmode 324  
AutoInstall Commands 114  
auto-negotiate 324  
auto-negotiate all 325  
Auto-Voice over IP Commands 404  
auto-voip 404  
auto-voip all 404

## B

boot autoinstall 114  
boot host autoreboot 116  
boot host autosave 115  
boot host dhcp 115  
boot host retrycount 115  
boot system 140  
bootfile 124  
bridge aging-time 281

## C

Cable Test Command 118

cablestatus 118  
clear aaa ias-users 110  
clear config 200  
clear counters 201  
clear dot1x authentication-history 284  
clear dot1x statistics 284  
clear host 138  
clear igmpsnooping 201  
clear ip address-conflict-detect 150  
clear ip dhcp binding 129  
clear ip dhcp conflict 129  
clear ip dhcp server statistics 129  
clear isdp counters 257  
clear isdp table 257  
clear lldp remote-data 265  
clear lldp statistics 265  
clear logging email statistics 147  
clear network ipv6 dhcp statistics 399  
clear pass 201  
clear radius statistics 285  
clear traplog 201  
clear vlan 201  
client-identifier 120  
client-name 121  
clock timezone 424  
configuration 35  
Configuration Scripting Commands 32  
Console Port Access Commands 35  
copy 204  
copy (pre-login banner) 45  
crypto key generate dsa 38  
crypto key generate rsa 38

## D

debug clear 157  
debug console 157  
debug dhcp packet 158  
debug dot1x packet 158  
debug igmpsnooping packet 158  
debug igmpsnooping packet receive 160  
debug igmpsnooping packet transmit 159

- debug isdp packet 261
- debug ping packet 162
- debug spanning-tree bpdu 163
- debug spanning-tree bpdu receive 163
- debug spanning-tree bpdu transmit 164
- default-router 121
- delete backup 140
- deleteport (Global Config) 305
- deleteport (Interface Config) 305
- Denial of Service Commands 215
- description 325
- DHCP Server Commands 120
- disconnect 30
- DNS Client Commands 134
- dns-server 122
- domain-name 124
- dos-control all 215
- dos-control firstfrag 216
- dos-control icmp 218
- dos-control icmpfrag 223
- dos-control icmpv4 222
- dos-control icmpv6 223
- dos-control l4port 218
- dos-control sipdip 216
- dos-control smacdmac 219
- dos-control tcpfinurgpsh 222
- dos-control tcpflag 217
- dos-control tcpflagseq 220
- dos-control tcpfrag 217
- dos-control tcpoffset 220
- dos-control tcpport 219
- dos-control tcpsyn 221
- dos-control tcpsynfin 221
- dos-control udpport 219
- dot1x guest-vlan 285
- dot1x initialize 285
- dot1x max-req 285
- dot1x max-users 286
- dot1x pae 226
- dot1x port-control 286
- dot1x port-control all 287
- dot1x re-authenticate 288
- dot1x re-authentication 288
- dot1x supplicant max-start 227
- dot1x supplicant port-control 226

- dot1x supplicant timeout auth-period 228
- dot1x supplicant timeout held-period 228
- dot1x supplicant timeout start-period 227
- dot1x supplicant user 229
- dot1x system-auth-control 288
- dot1x system-auth-control monitor 289
- dot1x timeout 289
- dot1x unauthenticated-vlan 291
- dot1x user 292
- Dual Image Commands 140

## E

- Email Alerting and Mail Server Commands 142
- enable (Privileged EXEC access) 39
- enable authentication 89
- enable password 100
- enable password encrypted 100
- environment temprange 207
- environment trap fan 207
- environment trap powersupply 207
- environment trap temperature 208
- erase startup-config 116

## F

- filedescr 140

## G

- GARP Commands 231
- GMRP Commands 234
- GVRP Commands 238

## H

- hardware-address 122
- host 122
- hostname 46

## I

- IGMP Snooping Configuration Commands 241
- IGMP Snooping Querier Commands 251
- interface 324
- IP Access Control List Commands 406



- ip access-group 411
- ip access-list 409
- ip access-list rename 409
- IP Address Conflict Commands 150
- ip address-conflict-detect run 150
- ip dhcp bootp automatic 128
- ip dhcp conflict logging 128
- ip dhcp excluded-address 127
- ip dhcp ping packets 127
- ip dhcp pool 120
- ip domain list 135
- ip domain lookup 134
- ip domain name 134
- ip domain retry 137
- ip domain timeout 137
- ip host 136
- ip name server 135
- ip ssh 64
- ip ssh protocol 64
- ip ssh server enable 64
- ip telnet server enable 83
- ipv6 host 136
- IPv6 Management Commands 395, 396
- isdp advertise-v2 257
- ISDP Commands 256
- isdp enable 257
- isdp holdtime 256
- isdp run 256
- isdp timer 256

## K

- key 81

## L

- lacp actor admin 307
- lacp actor admin key 307
- lacp actor admin state 307
- lacp actor admin state individual 308
- lacp actor admin state longtimeout 308
- lacp actor admin state passive 309
- lacp actor port 309
- lacp actor port priority 309
- lacp admin key 306
- lacp collector max-delay 306

- lacp partner admin key 310
- lacp partner admin state 310
- lacp partner admin state individual 311
- lacp partner admin state longtimeout 311
- lacp partner admin state passive 312
- lacp partner port id 312
- lacp partner port priority 313
- lacp partner system priority 314
- lacp partner system-id 314
- lease 123
- line 35
- LLDP (802.1AB) Commands 262
- lldp med 273
- lldp med all 274
- lldp med confignotification 273
- lldp med confignotification all 274
- lldp med faststart-repeatcount 275
- lldp med transmit-tlv 274
- lldp med transmit-tlv all 275
- lldp notification 264
- lldp notification-interval 265
- lldp receive 262
- lldp timers 263
- lldp transmit 262
- lldp transmit-mgmt 264
- lldp transmit-tlv 263
- LLDP-MED Commands 273
- logging buffered 151
- logging buffered wrap 151
- logging cli-command 152
- Logging Commands 151
- logging console 152
- logging email 142
- logging email from-addr 143
- logging email logtime 144
- logging email message-type subject 144
- logging email message-type to-addr 143
- logging email test message-type 145
- logging email urgent 142
- logging host 152
- logging host reconfigure 153
- logging host remove 153
- logging persistent 165
- logging port 153
- logging syslog 154

logging traps 145  
login authentication 98  
logout 202

## M

MAC Access Control List Commands 416  
mac access-group 419  
mac access-list extended 416  
mac access-list extended rename 417  
MAC Database Commands 281  
macfilter 361  
macfilter adddest 362  
macfilter adddest all 362  
macfilter addsrc 363  
macfilter addsrc all 363  
mail-server 147  
Management Commands 29  
Management Security Commands 38  
memory free low-watermark processor 109  
monitor session 330  
mtu 326

## N

netbios-name-server 124  
netbios-node-type 125  
network (DHCP Pool Config) 123  
Network Interface Commands 39  
network ipv6 address 396  
network ipv6 enable 396  
network ipv6 gateway 397  
network mac-address 40  
network mac-type 41  
network mgmt\_vlan 379  
network parms 39  
network protocol 39  
next-server 126  
no aaa authentication enable 89  
no aaa authentication login 87  
no aaa ias-user username 110  
no absolute 423  
no access-list 408  
no acl-trapflags 412  
no auto-negotiate 325  
no auto-negotiate all 325

no auto-voip 405  
no auto-voip all 404  
no boot host autoreboot 116  
no boot host autosave 116  
no boot host dhcp 115  
no boot host retrycount 115  
no bootfile 124  
no bridge aging-time 281  
no client-identifier 121  
no client-name 121  
no crypto key generate dsa 38  
no crypto key generate rsa 38  
no debug console 157  
no debug dhcp packet 158  
no debug dot1x packet 158  
no debug igmpsnooping packet 159  
no debug igmpsnooping packet receive 161  
no debug igmpsnooping transmit 160  
no debug isdp packet 261  
no debug ping packet 162  
no debug spanning-tree bpdu 163  
no debug spanning-tree bpdu receive 164  
no debug spanning-tree bpdu transmit 165  
no default-router 121  
no dns-server 122  
no domain-name 124  
no dos-control all 216  
no dos-control firstfrag 216  
no dos-control icmp 218  
no dos-control icmpfrag 223  
no dos-control icmpv4 222  
no dos-control icmpv6 223  
no dos-control l4port 218  
no dos-control sipdip 216  
no dos-control smacdmac 219  
no dos-control tcpfinurgpsh 222  
no dos-control tcpflag 217  
no dos-control tcpflagseq 220  
no dos-control tcpfrag 217  
no dos-control tcpoffset 221  
no dos-control tcpport 219  
no dos-control tcpsyn 221  
no dos-control tcpsynfin 221  
no dos-control udpport 220  
no dot1x guest-vlan 285

- no dot1x max-req 286
- no dot1x max-users 286
- no dot1x port-control 287
- no dot1x port-control all 287
- no dot1x re-authentication 288
- no dot1x supplicant max-start 227
- no dot1x supplicant port-control 227
- no dot1x supplicant timeout auth-period 228
- no dot1x supplicant timeout held-period 228
- no dot1x supplicant timeout start-period 228
- no dot1x system-auth-control 289
- no dot1x system-auth-control monitor 289
- no dot1x timeout 291
- no dot1x unauthenticated-vlan 291
- no dot1x user 292
- no enable authentication 90
- no enable password 100
- no hardware-address 122
- no host 123
- no ip access-group 411
- no ip access-list 409
- no ip dhcp bootp automatic 128
- no ip dhcp conflict logging 128
- no ip dhcp excluded-address 127
- no ip dhcp ping packets 127
- no ip dhcp pool 120
- no ip domain list 135
- no ip domain lookup 134
- no ip domain name 135
- no ip domain retry 137
- no ip domain timeout 137
- no ip host 136
- no ip name server 136
- no ip ssh server enable 65
- no ip telnet server enable 83
- no ipv6 host 137
- no isdp advertise-v2 257
- no isdp enable 257
- no isdp run 256
- no lacp actor admin key 307
- no lacp actor admin state 308
- no lacp actor admin state individual 308
- no lacp actor admin state longtimeout 308
- no lacp actor admin state passive 309
- no lacp actor port priority 310
- no lacp admin key 306
- no lacp collector max delay 306
- no lacp partner admin key 310
- no lacp partner admin state 311
- no lacp partner admin state individual 311
- no lacp partner admin state longtimeout 312
- no lacp partner admin state passive 312
- no lacp partner port id 313
- no lacp partner port priority 313
- no lacp partner system priority 314
- no lacp partner system-id 314
- no ldp med confignotification 273
- no lease 123
- no lldp med 273
- no lldp med faststart-repeatcount 275
- no lldp med transmit-tlv 274, 275
- no lldp notification 264
- no lldp notification-interval 265
- no lldp receive 262
- no lldp timers 263
- no lldp transmit 262
- no lldp transmit-mgmt 264
- no lldp transmit-tlv 264
- no logging buffered 151
- no logging buffered wrap 151
- no logging cli-command 152
- no logging console 152
- no logging email 142
- no logging email from-addr 144
- no logging email logtime 145
- no logging email message-type subject 144
- no logging email message-type to-addr 143
- no logging email urgent 143
- no logging persistent 166
- no logging port 153
- no logging syslog 154
- no logging traps 145
- no login authentication 99
- no mac access-group 420
- no mac access-list extended 416
- no macfilter 361
- no macfilter adddest 362
- no macfilter adddest all 363
- no macfilter addsrc 363
- no macfilter addsrc all 363

- no mail-server 147
- no monitor 331
- no monitor session 330
- no mtu 326
- no netbios-name-server 125
- no netbios-node-type 125
- no network 124
- no network ipv6 address 397
- no network ipv6 enable 396
- no network ipv6 gateway 398
- no network mac-type 41
- no network mgmt\_vlan 379
- no next-server 126
- no option 126
- no password (AAA IAS User Configuration) 110
- no password (Line Configuration) 99
- no passwords aging 102
- no passwords history 101
- no passwords lock-out 102
- no passwords min-length 101
- no passwords strength exclude-keyword 107
- no passwords strength minimum character-classes 106
- no passwords strength minimum consecutive-characters 105
- no passwords strength minimum lowercase-letters 104
- no passwords strength minimum numeric-characters 104
- no passwords strength minimum repeated-characters 106
- no passwords strength minimum special-characters 105
- no passwords strength minimum uppercase-letters 103
- no passwords strength-check 103
- no periodic 424
- no port lacpmode 315
- no port lacpmode all 316
- no port lacptimeout (Global Config) 317
- no port lacptimeout (Interface Config) 316
- no port-channel 304
- no port-channel adminmode 317
- no port-channel linktrap 318
- no port-channel load-balance 319
- no port-channel static 315
- no port-channel system priority 320
- no port-security 333
- no port-security mac-address 334
- no port-security max-dynamic 334
- no port-security max-static 334
- no radius accounting mode 47
- no radius server attribute 4 48
- no radius server host 49
- no radius server msgauth 51
- no radius server retransmit 52
- no radius server timeout 53
- no serial baudrate 36
- no serial timeout 36
- no service dhcp 128
- no set garp timer join 231
- no set garp timer leave 232
- no set garp timer leaveall 232
- no set gmrp adminmode 234
- no set gmrp interfacemode 235
- no set gvrp adminmode 238
- no set gvrp interfacemode 239
- no set igmp 241
- no set igmp fast-leave 243
- no set igmp groupmembership-interval 243
- no set igmp interfacemode 242
- no set igmp maxresponse 244
- no set igmp mcrtexpiretime 245
- no set igmp mrouter 245
- no set igmp mrouter interface 246
- no set igmp querier 252
- no set igmp querier election participate 253
- no set igmp querier query-interval 252
- no set igmp querier timer expiry 252
- no set igmp querier version 253
- no set igmp router-alert-check 246
- no set slot disable 209
- no set slot power 210
- no show debugging 166
- no shutdown 326
- no shutdown all 327
- no slot 208
- no snmp trap link-status 75
- no snmp trap link-status all 75
- no snmp-server community 68

no snmp-server community ipaddr 68  
no snmp-server community ipmask 69  
no snmp-server community mode 69  
no snmp-server enable traps 71  
no snmp-server enable traps linkmode 71  
no snmp-server enable traps multiusers 72  
no snmp-server enable traps stpmode 72  
no snmp-server enable traps violation 70  
no snmptrap 73  
no snmptrap mode 74  
no snmp broadcast client poll-interval 167  
no snmp client mode 167  
no snmp client port 168  
no snmp multicast client poll-interval 170  
no snmp server 170  
no snmp unicast client poll-interval 168  
no snmp unicast client poll-retry 169  
no snmp unicast client poll-timeout 169  
no spanning-tree 341  
no spanning-tree auto-edge 342  
no spanning-tree configuration name 342  
no spanning-tree configuration revision 343  
no spanning-tree edgeport 344  
no spanning-tree forceversion 344  
no spanning-tree forward-time 345  
no spanning-tree hold-count 345  
no spanning-tree max-age 345  
no spanning-tree max-hops 346  
no spanning-tree mst 347  
no spanning-tree mst priority 348  
no spanning-tree mst vlan 349  
no spanning-tree port mode 349  
no spanning-tree port mode all 350  
no sshcon maxsessions 65  
no sshcon timeout 66  
no storm-control broadcast 367  
no storm-control broadcast all 368  
no storm-control broadcast all level 369  
no storm-control broadcast all rate 369  
no storm-control broadcast level 367  
no storm-control broadcast rate 368  
no storm-control flowcontrol 376  
no storm-control multicast 370  
no storm-control multicast all 372  
no storm-control multicast all level 372  
no storm-control multicast all rate 373  
no storm-control multicast level 371  
no storm-control multicast rate 371  
no storm-control unicast 373  
no storm-control unicast all 375  
no storm-control unicast all level 375  
no storm-control unicast all rate 376  
no storm-control unicast level 374  
no storm-control unicast rate 374  
no switchport protected (Global Config) 337  
no switchport protected (Interface Config) 338  
no tacacs-server host 79  
no tacacs-server key 80  
no tacacs-server timeout 80  
no telnetcon maxsessions 84  
no telnetcon timeout 85  
no terminal length 197  
no time-range 422  
no transport input telnet 84  
no username 91  
no username snmpv3 accessmode 93  
no username snmpv3 authentication 93  
no username snmpv3 encryption 94  
no vlan 380  
no vlan acceptframe 380  
no vlan association mac 386  
no vlan ingressfilter 381  
no vlan name 381  
no vlan port acceptframe all 383  
no vlan port ingressfilter all 384  
no vlan port pvid all 384  
no vlan port tagging all 385  
no vlan pvid 385  
no vlan tagging 386  
no voice vlan (Global Config) 391  
no voice vlan (Interface Config) 392

## O

option 126

## P

password 148  
password (AAA IAS User Configuration) 110  
password (Line Configuration) 99

- password (User EXEC) 100
- passwords aging 102
- passwords history 101
- passwords lock-out 102
- passwords min-length 101
- passwords strength exclude-keyword 107
- passwords strength minimum character-classes 106
- passwords strength minimum consecutive-characters 105
- passwords strength minimum lowercase-letters 104
- passwords strength minimum numeric-characters 104
- passwords strength minimum repeated-characters 106
- passwords strength minimum special-characters 105
- passwords strength minimum uppercase-letters 103
- passwords strength-check 103
- periodic 423
- ping 202
- ping ipv6 399
- ping ipv6 interface 400
- port 81, 148
- Port Channel/LAG (802.3ad) Commands 304
- Port Configuration Commands 324
- port lacpmode 315
- port lacpmode all 316
- port lacptimeout (Global Config) 316
- port lacptimeout (Interface Config) 316
- Port Mirroring Commands 330
- Port Security Commands 333
- Port-Based Network Access Control Commands 284
- port-channel 304
- port-channel adminmode 317
- port-channel linktrap 317
- port-channel load-balance 318
- port-channel name 319
- port-channel static 315
- port-channel system priority 320
- port-security 333
- port-security mac-address 334

- port-security mac-address move 335
- port-security max-dynamic 333
- port-security max-static 334
- Pre-login Banner, System Prompt, and Host Name Commands 45
- priority 81
- process cpu threshold type total rising 193
- Protected Ports Commands 337
- Provisioning (IEEE 802.1p) Commands 340

## Q

- Quality of Service Commands 403
- quit 204

## R

- radius accounting mode 47
- RADIUS Commands 47
- radius server attribute 4 47
- radius server host 48
- radius server key 50
- radius server msgauth 51
- radius server primary 51
- radius server retransmit 52
- radius server timeout 53
- reload 204
- renew dhcp network-port 41
- renew dhcp service-port 41

## S

- script apply 33
- script delete 33
- script list 33
- script show 34
- script validate 34
- Secure Shell Commands 64
- security 148
- serial baudrate 36
- serial timeout 36
- service dhcp 127
- Serviceability Packet Tracing Commands 157
- set garp timer join 231
- set garp timer leave 231
- set garp timer leaveall 232

set gmrp adminmode 234  
 set gmrp interfacemode 234  
 set gvrp adminmode 238  
 set gvrp interfacemode 238  
 set igmp 241  
 set igmp fast-leave 242  
 set igmp groupmembership-interval 243  
 set igmp interfacemode 242  
 set igmp maxresponse 244  
 set igmp mcrtrexpiretime 244  
 set igmp mrouter 245  
 set igmp mrouter interface 245  
 set igmp querier 251  
 set igmp querier election participate 253  
 set igmp querier query-interval 252  
 set igmp querier timer expiry 252  
 set igmp querier version 253  
 set igmp router-alert-check 246  
 set prompt 45  
 set slot disable 209  
 set slot power 209  
 show aaa ias-users 111  
 show access-lists interface 414  
 show access-lists vlan 415  
 show arp switch 174  
 show authentication 293  
 show authentication methods 293  
 show authentication users 294  
 show autoinstall 117  
 show auto-voip 405  
 show bootvar 140  
 show clock detail 424  
 show debugging 166  
 show dos-control 223  
 show dot1x 294  
 show dot1x authentication-history 300  
 show dot1x clients 301  
 show dot1x statistics 229  
 show dot1x users 302  
 show environment 208  
 show eventlog 174  
 show forwardingdb agetime 281  
 show garp 233  
 show gmrp configuration 235  
 show gvrp configuration 239  
 show hardware 175  
 show hosts 138  
 show igmpsnooping 246  
 show igmpsnooping mrouter interface 248  
 show igmpsnooping mrouter vlan 249  
 show igmpsnooping querier 254  
 show interface 176  
 show interface ethernet 178  
 show interfaces switchport 339  
 show ip access-lists 412  
 show ip address-conflict 150  
 show ip dhcp binding 129  
 show ip dhcp conflict 132  
 show ip dhcp global configuration 130  
 show ip dhcp pool configuration 130  
 show ip dhcp server statistics 131  
 show ip ssh 66  
 show isdp 258  
 show isdp entry 259  
 show isdp interface 259  
 show isdp neighbors 259  
 show isdp traffic 260  
 show lacp actor 320  
 show lacp partner 320  
 show lldp 266  
 show lldp interface 266  
 show lldp local-device 271  
 show lldp local-device detail 271  
 show lldp med 276  
 show lldp med interface 276  
 show lldp med local-device detail 277  
 show lldp med remote-device 278  
 show lldp med remote-device detail 279  
 show lldp remote-device 268  
 show lldp remote-device detail 269  
 show lldp statistics 267  
 show logging 154  
 show logging buffered 155  
 show logging email config 145  
 show logging email statistics 146  
 show logging hosts 155  
 show logging traplogs 156  
 show login session 30  
 show login session long 31  
 show mac access-lists 420

show mac-address-table gmrp 236  
 show mac-address-table igmpsnooping 249  
 show mac-address-table multicast 282  
 show mac-address-table static 364  
 show mac-address-table staticfiltering 364  
 show mac-address-table stats 282  
 show mac-addr-table 191  
 show mail-server config 149  
 show monitor session 331  
 show network 41  
 show network ipv6 dhcp statistics 401  
 show network ndp 398  
 show passwords configuration 107  
 show passwords result 108  
 show port 328  
 show port-channel 321  
 show port-channel brief 322  
 show port-channel system priority 323  
 show port-security 335  
 show port-security dynamic 335  
 show port-security static 335  
 show port-security violation 336  
 show process cpu 193  
 show radius 53  
 show radius accounting 57  
 show radius accounting statistics 58  
 show radius servers 55  
 show radius statistics 61  
 show running-config 194  
 show serial 37  
 show slot 210  
 show snmpcommunity 75  
 show snmptrap 77  
 show snmp 170  
 show snmp client 171  
 show snmp server 172  
 show spanning-tree 350  
 show spanning-tree brief 352  
 show spanning-tree interface 352  
 show spanning-tree mst detailed 353  
 show spanning-tree mst port detailed 354  
 show spanning-tree mst port summary 356  
 show spanning-tree mst port summary active 357  
 show spanning-tree mst summary 358  
 show spanning-tree summary 359  
 show spanning-tree vlan 359  
 show storm-control 376  
 show supported cardtype 212  
 show switchport protected 338  
 show sysinfo 195  
 show tacacs 82  
 show tech-support 196  
 show telnetcon 85  
 show terminal length 197  
 show time-range 425  
 show trapflags 78  
 show users 95  
 show users accounts 96  
 show users login-history 98  
 show users long 96  
 show version 175  
 show vlan 386  
 show vlan brief 389  
 show vlan internal usage 388  
 show vlan port 389  
 show voice vlan 392  
 shutdown 326  
 shutdown all 327  
 Simple Network Time Protocol Commands 167  
 slot 208  
 SNMP Commands 67  
 snmp trap link-status 74  
 snmp trap link-status all 75  
 snmp-server 67  
 snmp-server community 67  
 snmp-server community ipaddr 68  
 snmp-server community ipmask 68  
 snmp-server community mode 69  
 snmp-server community ro 70  
 snmp-server community rw 70  
 snmp-server enable traps 70  
 snmp-server enable traps linkmode 71  
 snmp-server enable traps multiusers 71  
 snmp-server enable traps stpmode 72  
 snmp-server enable traps violation 70  
 snmptrap 72  
 snmptrap ipaddr 74  
 snmptrap mode 74  
 snmptrap snmpversion 73  
 snmp broadcast client poll-interval 167



- sntp client mode 167
- sntp client port 168
- sntp multicast client poll-interval 169
- sntp server 170
- sntp unicast client poll-interval 168
- sntp unicast client poll-retry 169
- sntp unicast client poll-timeout 169
- Spanning Tree Protocol Commands 341
- spanning-tree 341
- spanning-tree auto-edge 341
- spanning-tree bpdumigration-check 342
- spanning-tree configuration name 342
- spanning-tree configuration revision 342
- spanning-tree cost 343
- spanning-tree cost auto 343
- spanning-tree edgeport 343
- spanning-tree forceversion 344
- spanning-tree forward-time 344
- spanning-tree hold-count 345
- spanning-tree max-age 345
- spanning-tree max-hops 346
- spanning-tree mst 346
- spanning-tree mst instance 348
- spanning-tree mst priority 348
- spanning-tree mst vlan 349
- spanning-tree port mode 349
- spanning-tree port mode all 349
- speed 327
- speed all 328
- sshcon maxsessions 65
- sshcon timeout 65
- Static MAC Filtering Commands 361
- storm-control broadcast 367
- storm-control broadcast all 368
- storm-control broadcast all level 369
- storm-control broadcast all rate 369
- storm-control broadcast level 367
- storm-control broadcast rate 368
- Storm-Control Commands 366
- storm-control flowcontrol 376
- storm-control multicast 370
- storm-control multicast all 371
- storm-control multicast all level 372
- storm-control multicast all rate 372
- storm-control multicast level 370
- storm-control multicast rate 371
- storm-control unicast 373
- storm-control unicast all 374
- storm-control unicast all level 375
- storm-control unicast all rate 375
- storm-control unicast level 373
- storm-control unicast rate 374
- Switching Commands 213
- switchport protected (Global Config) 337
- switchport protected (Interface Config) 338
- System Information and Statistics Commands 174
- System Utility and Clear Commands 198

## T

- TACACS+ Commands 79
- tacacs-server host 79
- tacacs-server key 79
- tacacs-server timeout 80
- Telnet Commands 83
- telnetcon maxsessions 84
- telnetcon timeout 84
- terminal length 197
- Time Range Commands for Time-Based ACLs 422
- timeout 82
- time-range 422
- Topics in this chapter 29, 113, 213, 395, 403
- traceroute 198
- traceroute ipv6 200, 400
- transport input telnet 83

## U

- update bootcode 141
- User Account Commands 86
- user password 107
- username 90, 148
- username name nopassword 92
- username name unlock 92
- username snmpv3 accessmode 92
- username snmpv3 authentication 93
- username snmpv3 encryption 94
- username snmpv3 encryption encrypted 94
- users defaultlogin 292
- users login 292

## V

- vlan 379
- vlan acceptframe 380
- vlan association mac 386
- VLAN Commands 379
- vlan database 379
- vlan ingressfilter 380
- vlan makestatic 381
- vlan name 381
- vlan participation 381
- vlan participation all 382
- vlan port acceptframe all 383

- vlan port ingressfilter all 384
- vlan port priority all 340
- vlan port pvid all 384
- vlan port tagging all 385
- vlan priority 340
- vlan pvid 385
- vlan tagging 385
- voice vlan (Global Config) 391
- voice vlan (Interface Config) 391
- Voice VLAN Commands 391
- voice vlan data priority 392

## W

- write memory 109