Data Center Switch Software (DCSS)
Command Reference Guide

SOFTWARE VERSION 3.2

61700558F1MC-35C
February, 2020

Table of Contents

List of Tables

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, service marks, or trade names of their respective holders.

To the Holder of this Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

Software Licensing Agreement

Each ADTRAN product contains a single license for ADTRAN supplied software. Pursuant to the Licensing Agreement, you may: (a) use the software on the purchased ADTRAN device only and (b) keep a copy of the software for backup purposes. This Agreement covers all software installed on the system, as well as any software available on the ADTRAN website. In addition, certain ADTRAN systems may contain additional conditions for obtaining software upgrades.

901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000
www.adtran.com
61700558F1MC-35C

Service and Warranty

For information on the service and warranty of ADTRAN products, visit the ADTRAN website at http://www.adtran.com/support.

Export Statement

An Export License is required if an ADTRAN product is sold to a Government Entity outside of the EU+8 (Austria, Australia, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the United Kingdom). This requirement is per DOC/BIS ruling G030477 issued 6/6/03. This product also requires that the Exporter of Record file a semi-annual report with the BXA detailing the information per EAR 740.17(5)(e)(2).

DOC - Department of Commerce
BIS - Bureau of Industry and Security
BXA - Bureau of Export Administration

About This Document

Purpose and Audience

This document describes the command line interface (CLI) commands used to view and configure DCSS 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.

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

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

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

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

Document Conventions

The following conventions may be used in this document:

Convention	*Description*
Bold	User input and actions: for example, type **exit**, click **OK,** press **Alt+C**
`Monospace`	Code: `#include <iostream>` Command line commands and command output: `(Routing)# show sysinfo`
`Monospace italic`	Command variables: `interface vlan` *`vlan-id`*
{ }	Mutually-exclusive command line parameters: `network protocol {none | bootp | dhcp}`
[ ]	Indicates *optional* command-line parameters: `write memory [confirm]`

Section 1: Supported Features

Adtran 1748F Supported Features

The following list of features is supported on the ADTRAN 1748F. Any other commands or features available in the product are untested and are used at your own risk. ADTRAN Support recommends not using untested commands or features.

- Basic Layer 2 and Layer 3 VLANs (VLAN port-assignments, IP addressing)
- Layer 3 Static Routing/Switching
- LLDP
- LLDP med
- IP DHCP helper (DHCP forwarding)
- SNMP
- SNTP
- Rapid Spanning Tree
- DNS-Client
- Console/SSH/Telnet Access
- Static LACP
- Logging, debug, and Show Commands associated with the above feature set

Section 2: About DCSS Software

About DCSS Software

The Data Center Switch Software (DCSS) 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

DCSS 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. DCSS software provides a flexible solution to these ever-increasing needs.

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

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

- Command line interface (CLI)
- Simple Network Management Protocol (SNMP)

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

Section 3: Using the CLI

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

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

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 *Command Reference Guide* 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. Table 1 describes the conventions this document uses to distinguish between value types.

Table 1: Parameter Conventions

Symbol	*Example*	*Description*
[] square brackets	`[value]`	Indicates an optional parameter.
`italic font in a parameter`.	*`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. Table 2 describes common parameter values and value formatting.

Table 2: Parameter Descriptions

Parameter	*Description*

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

Interface or `slot/port`	Valid slot and port number separated by a forward slash. For example, 0/1 represents slot number 0 and port number 1.
Logical Interface	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.
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

The DCSS software references physical entities such as cards and ports by using a `slot/port` naming convention. The DCSS software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

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

Table 3: Type of Slots

Slot Type	*Description*
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces. The value of logical slot numbers depend on the type of logical interface and can vary from platform to platform.
CPU slot numbers	The CPU slots immediately follow the logical slots.

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

Table 4: Type of Ports

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

Note: In the CLI, loopback interfaces do not use the `slot/port` format. To specify a loopback interface, you use the loopback 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 reenable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the `no` form.

Executing Show Commands

All show commands can now be issued from any configuration mode (Global Config, Interface Config, VLAN Config, etc.). The show commands provide information about system and feature-specific configuration, status, and statistics. In previous releases, show commands could be issued only in User EXEC or Privileged EXEC modes.

CLI Output Filtering

Many CLI show commands include considerable content to display to the user. This can make output confusing and cumbersome to parse through to find important information. The CLI Output Filtering feature allows the user, when executing CLI show display commands, to optionally specify arguments to filter the CLI output to display only desired information. The result is to simplify the display and make it easier for the user to find the information the user is interested in.

The main functions of the CLI Output Filtering feature are:

- Pagination Control
  - Supports enabling/disabling paginated output for all **show** CLI commands. When disabled, output is displayed in its entirety. When enabled, output is displayed page-by-page such that content does not scroll off the terminal screen until the user presses a key to continue. --More-- or (q)uit is displayed at the end of each page.
  - When pagination is enabled, press the return key to advance a single line, press q or Q to stop pagination, or press any other key to advance a whole page. These keys are not configurable.

Note: Although some DCSS **show** commands already support pagination, the implementation is unique per command and not generic to all commands.

- Output Filtering
  - “Grep”-like control for modifying the displayed output to only show the user-desired content.
    - Filter displayed output to only include lines containing a specified string match.
    - Filter displayed output to exclude lines containing a specified string match.
    - Filter displayed output to only include lines including and following a specified string match.
    - Filter displayed output to only include a specified section of the content (e.g., “interface 0/1”) with a configurable end-of-section delimiter.
    - String matching should be case insensitive.
    - Pagination, when enabled, also applies to filtered output.

Example: The following shows an example of the extensions made to the CLI show commands for the Output Filtering feature.

```
show running-config ?
<cr>      Press enter to execute the command.
all       Show all the running configuration on the switch.
|         Output filter options
```

```
show running-config | ?
include {keyword}
exclude {keyword}
section {begin end}
```

For commands for the feature, see “CLI Output Filtering Commands” on page 77.

Section 4: DCSS Modules

DCSS 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 DCSS software.

The DCSS software suite includes the following modules:

- Switching (Layer 2)
- Data Center
- Routing (Layer 3)
- IPv6 Routing (Layer 3)
- Multicast
- BGP-4
- Quality of Service
- Management (CLI and SNMP)

Not all modules are available for all platforms or software releases.

Command Modes

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

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

Note: The command modes available on your switch depend on the software modules that are installed. For example, a switch that does not support BGPv4 does not have the BGPv4 Router Command Mode.

Table 5: CLI Command Modes

Command Mode	*Prompt*	*Mode Description*
User EXEC	`Switch>`	Contains a limited set of commands to view basic system information.
Privileged EXEC	`Switch#`	Allows you to issue any `EXEC` command, enter the VLAN mode, or enter the Global Configuration mode.

Table 5: CLI Command Modes (Cont.)

Command Mode	*Prompt*	*Mode Description*
Global Config	`Switch (Config)#`	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	`Switch (Vlan)#`	Groups all the VLAN commands.

Interface Config	`Switch (Interface slot/port)#`
	`Switch (Interface vlan vlan-id)#`
	`Switch (Interface lag vlan-id)#`
	`Switch (Interface Loopback id)#`
	`Switch (Interface tunnel id)#`
	`Switch (Interface slot/port (startrange)-slot/port(endrange)#`
		Manages the operation of an interface and provides access to the router interface configuration commands.
		Use this mode to set up a physical port for a specific logical connection operation.
		You can also use this mode to manage the operation of a range of interfaces. For example for the range of interfaces from ports 0/2 to 0/4, the prompt displays as follows:
		`(Routing) (Interface 0/2-0/4)#`

Line Console	`Switch (config-line)#`	Contains commands to configure outbound telnet settings and console interface settings, as well as to configure console login/enable authentication.
Line SSH	`Switch (config-ssh)#`	Contains commands to configure SSH login/ enable authentication.
Line Telnet	`Switch (config-telnet)#`	Contains commands to configure telnet login/ enable authentication.

Table 6 explains how to enter each mode. To exit a mode and return to the previous mode, enter exit. To exit to Privileged EXEC mode, press Ctrl+z.

Note: Pressing Ctrl+z from Privileged EXEC mode exits to User EXEC mode. To exit User EXEC mode, enter logout.

Table 6: CLI Mode Access and Exit

Command Mode	*Access Method*
User EXEC	This is the first level of access.
Privileged EXEC	From the User EXEC mode, enter `enable`.
Global Config	From the Privileged EXEC mode, enter `configure`.
VLAN Config	From the Privileged EXEC mode, enter `vlan database`.

Table 6: CLI Mode Access and Exit (Cont.)

Command Mode	*Access Method*

Interface Config	From the Global Config mode, enter one of the following:
	`interface slot/port`
	`interface vlan vlan-id`
	`interface lag lag-number`
	`interface loopback id`
	`interface tunnel id`
	`interface` *`slot/port`*`(startrange)-`*`slot/port`*`(endrange)`

Line Console	From the Global Config mode, enter `line console`.
Line SSH	From the Global Config mode, enter `line ssh`.
Line Telnet	From the Global Config mode, enter `line telnet`.

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. Table 7 describes the most common CLI error messages.

Table 7: CLI Error Messages

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

CLI Line Editing Conventions

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

Table 8: CLI Editing Conventions

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

Using CLI Help

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

```
(Routing)>?

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.

```
(Routing) #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.

```
(Routing) #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:

```
(Routing) #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 “Network Interface Commands” on page 39.

Section 5: Management Commands

This section describes the following management commands available in the DCSS CLI:

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

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Network Interface Commands

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 218.

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

do (Privileged EXEC commands)

This command executes Privileged EXEC mode commands from any of the configuration modes.

Format `do` *`Priv Exec Mode Command`*

Mode
- Global Config
- Interface Config
- VLAN Config
- Routing Config

Example: The following is an example of the `do` command that executes the Privileged EXEC command `script list` in Global Config Mode.

```
(Routing) #configure

(Routing)(config)#do script list

Configuration Script Name        Size(Bytes)
-------------------------------- -----------
backup-config                           2105
running-config                          4483
startup-config                           445

3 configuration script(s) found.
2041 Kbytes free.

Routing(config)#
```

serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port. You can specify the `none` option to clear the IPv4 address and mask and the default gateway (i.e., reset each of these values to 0.0.0.0).

Format `serviceport ip {ipaddr netmask [gateway] | none}`
Mode Privileged EXEC

serviceport protocol

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

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

serviceport protocol dhcp

This command enables the DHCPv4 client on a Service port and sends DHCP client messages with the client identifier option (DHCP Option 61).

Format `serviceport protocol dhcp [client-id]`
Mode Privileged EXEC

There is no support for the **no** form of the command **serviceport protocol dhcp client-id**. To remove the `client-id` option from the DHCP client messages, issue the command **serviceport protocol dhcp** without the `client-id` option. The command **serviceport protocol none** can be used to disable the DHCP client and client-id option on the interface.

Example: The following shows an example of the command.

```
(Routing) # serviceport protocol dhcp client-id
```

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 (i.e., to reset each of these values to the default value on the switch).

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, 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 dhcp

Format `network protocol {none | bootp | dhcp}`

Mode Privileged EXEC

network protocol dhcp

This command enables the DHCPv4 client on a Network port and sends DHCP client messages with the client identifier option (DHCP Option 61).

Format `network protocol dhcp [client-id]`

Mode Global Config

There is no support for the **no** form of the command **network protocol dhcp client-id**. To remove the `client-id` option from the DHCP client messages, issue the command **network protocol dhcp** without the `client-id` option. The command **network protocol none** can be used to disable the DHCP client and client-id option on the interface.

Example: The following shows an example of the command.

```
(Routing) # network protocol dhcp client-id
```

network mac-address

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

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

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

Format `network mac-address` *`macaddr`*

Mode Privileged EXEC

network mac-type

This command specifies whether the 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

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`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
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.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique 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.

Term	*Definition*
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the **client-id** option on the network port. See "network protocol dhcp" on page 41.

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

```
(Switching) #show network

Interface Status.............................. 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
DHCP Client Identifier........................ 0dcss-0010.1882.160B-vl1
```

show serviceport

This command displays service port configuration information.

Format `show serviceport`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
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.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp | dhcp | none.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the **client-id** option on the service port. See "serviceport protocol" on page 40.

Example: The following example shows CLI display output for the service port.

```
(Switching) #show serviceport

Interface Status.............................. Up
IP Address.................................... 10.230.3.51
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.230.3.1
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... fe80::210:18ff:fe82:640/64
IPv6 Prefix is ............................... 2005::21/128
IPv6 Default Router is ....................... fe80::204:76ff:fe73:423a
Configured IPv4 Protocol ..................... DHCP
Configured IPv6 Protocol ..................... DHCP
DHCPv6 Client DUID ........................... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode.......................... Disabled
Burned In MAC Address......................... 00:10:18:82:06:4D
DHCP Client Identifier........................ 0dcss-0010.1882.160C
```

Console Port Access Commands

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

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

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

```
(Routing)(config)#line telnet
(Routing)(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`
Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect.
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	The parity method used on the Serial Port. The Parity Method is always None.

Telnet Commands

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

ip telnet server enable

Use this command to enable Telnet connections to the system and to enable 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

Use this command to disable Telnet access to the system and to disable 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

ip telnet port

This command configures the TCP port number on which the Telnet server listens for requests.

Default 23
Format `ip telnet port 1-65535`
Mode Privileged EXEC

no ip telnet port

This command restores the Telnet server listen port to its factory default value.

Format `no ip telnet port`
Mode Privileged EXEC

telnet

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

Format `telnet ip-address|hostname port [debug] [line] [localecho]`

Modes
- Privileged EXEC
- User 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 `ip telnet server enable` command to enable Telnet Server Admin Mode.

Default enabled

Format `transport input telnet`

Mode Line Config

no transport input telnet

Use this command to prevent new Telnet sessions from being established.

Format `no transport input telnet`

Mode Line Config

transport output telnet

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

Default enabled

Format `transport output telnet`

Mode Line Config

no transport output telnet

Use this command to prevent new outbound Telnet connection from being established.

Format `no transport output telnet`

Mode Line Config

session-limit

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

Default 5

Format `session-limit 0-5`

Mode Line Config

no session-limit

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

Format `no session-limit`

Mode Line Config

session-timeout

This command sets the Telnet session timeout value.The timeout value unit of time is minutes.

Default 5

Format `session-timeout 1-160`

Mode Line Config

no session-timeout

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

Format `no session-timeout`

Mode Line Config

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 0-5.

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 applied to all active and inactive sessions immediately. 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 telnet

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

Format `show telnet`

Modes
- Privileged EXEC
- User EXEC

Parameter	*Definition*
Outbound Telnet Login Timeout	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
Maximum Number of Outbound Telnet Sessions	The number of simultaneous outbound Telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound Telnet sessions will be allowed.

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

Term	*Definition*
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.
Telnet Server Admin Mode	If Telnet Admin mode is enabled or disabled.
Telnet Server Port	The configured TCP port number on which the Telnet server listens for requests. (The default is 23.)

Secure Shell Commands

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 5 SSH sessions.

ip ssh

Use this command to enable 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 port

Use this command to configure the TCP port number on which the SSH server listens for requests. Valid port numbers are from 1–65535.

Default 22
Format `ip ssh port 1-65535`
Mode Privileged EXEC

no ip ssh port

Use this command to restore the SSH server listen port to its factory default value.

Format `no ip ssh port`
Mode Privileged EXEC

ip ssh protocol

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

Default 1 and 2
Format `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 `no ip ssh server enable`
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 `sshcon maxsessions 0-5`
Mode Privileged EXEC

no sshcon maxsessions

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

Format `no sshcon maxsessions`
Mode Privileged EXEC

sshcon timeout

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

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

Default 5
Format `sshcon timeout 1-160`
Mode Privileged EXEC

no sshcon timeout

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

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

Format `no sshcon timeout`
Mode Privileged EXEC

show ip ssh

This command displays the ssh settings.

Format `show ip ssh`
Mode Privileged EXEC

Parameter	*Definition*
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
SSH Port	The SSH port.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 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.

Management Security Commands

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 rsa

Use this command to generate 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

Use this command to delete the RSA key files from the device.

Format `no crypto key generate rsa`

Mode Global Config

crypto key generate dsa

Use this command to generate 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

Use this command to delete the DSA key files from the device.

Format `no crypto key generate dsa`

Mode Global Config

Access Commands

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

disconnect

Use the `disconnect` command to close 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 loginsession` command.

Format `disconnect {`*`session_id`* `| all}`
Mode Privileged EXEC

dcss-show

Use this command to open a connection and execute the given show command. To start the application, DCSS should be running. If DCSS is not running, the command retries for 60 seconds for DCSS to be ready to accept the dcss-show connection. After 60 seconds, an error message is displayed.

The dcss-show command can execute all the show commands in Privileged EXEC and User Exec mode. The output of the show command is displayed and the application terminates. If the command does not start with a show, show is added automatically before the command internally. The user can terminate the application by pressing ^c at any point of time. The dcss-show command cannot handle auto-fill or tab (to auto-fill) like CLI. User is advised to enter complete command. However, partial unambiguous commands are executed like complete commands and the result is displayed normally. Partial ambiguous commands are terminated with error message. The user can use “?” to know the existing show command options.

Format `dcss-show [show]` *`show option`*
Mode Privileged EXEC

linuxsh

Use the `linuxsh` command to access the Linux shell. Use the `exit` command to exit the Linux shell and return to the DCSS CLI. The shell session will timeout after five minutes of inactivity. The inactivity timeout value can be changed using the command “session-timeout” on page 49 in Line Console mode.

Default ip-port:2324
Format `linuxsh [`*`ip-port`*`]`
Mode Privileged EXEC

Parameter	*Description*
ip-port	The IP port number on which the telnet daemon listens for connections. ip-port is an integer from 1 to 65535. The default value is 2324.

show loginsession

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

Format `show loginsession`

Mode Privileged EXEC

Parameter	*Definition*
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 telnet, serial, or SSH.

show loginsession long

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

Format `show loginsession long`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Routing) #show loginsession long
User Name
------------
admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

SNMP Commands

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.

Default none

Format `snmp-server {sysname name | location loc | contact con}`

Mode Global Config

Note: To clear the snmp-server, enter an empty string in quotes. For example, snmp-server {sysname " "} clears the system name.

snmp-server community

This command adds (and names) a new SNMP community, and optionally sets the access mode, allowed IP address, and create a view for the community.

Note: Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default Two communities are created by default:

- public, with read-only permissions, a view name of Default, and allows access from all IP addresses
- private, with read/write permissions, a view name of Default, and allows access from all IP addresses.

Format `snmp-server community community-string [{ro | rw |su }] [ipaddress ip-address] [view view-name]`

Mode Global Config

Parameter	*Description*
community-name	A name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of *community-name* can be up to 16 case-sensitive characters.
ro | rw | su	The access mode of the SNMP community, which can be public (Read-Only/RO), private (Read-Write/RW), or Super User (SU).

Parameter	*Description*
ip-address	The associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses.
view-name	The name of the view to create or update.

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` *community-name*

Mode Global Config

snmp-server community-group

This command configures a community access string to permit access via the SNMPv1 and SNMPv2c protocols.

Format `snmp-server community-group` *community-string group-name* `[ipaddress` *ipaddress*`]`

Mode Global Config

Parameter	*Description*
community-string	The community which is created and then associated with the group. The range is 1 to 20 characters.
group-name	The name of the group that the community is associated with. The range is 1 to 30 characters.
ipaddress	Optionally, the IPv4 address that the community may be accessed from.

snmp-server enable traps violation

The Port MAC locking component interprets this command and configures violation action to send an SNMP trap with default trap frequency of 30 seconds. The Global command configures the trap violation mode across all interfaces valid for port-security. There is no global trap mode as such.

Default disabled

Format `snmp-server enable traps violation`

Mode
- Global Config
- Interface Config

no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format `no snmp-server enable traps violation`

Mode Interface Config

snmp-server enable traps

This command enables the Authentication Flag.

Default enabled

Format `snmp-server enable traps`

Mode Global Config

no snmp-server enable traps

This command disables the Authentication Flag.

Format `no snmp-server enable traps`

Mode Global Config

snmp-server enable traps bgp

The **bgp** option on the "snmp-server enable traps" command above enables the two traps defined in the standard BGP MIB, RFC 4273. A trap is sent when an adjacency reaches the ESTABLISHED state and when a backward adjacency state transition occurs.

Default enabled

Format `snmp-server enable traps bgp state-changes limited`

Mode Global Config

Parameter	*Description*
state-changes limited	Enabled standard traps defined in RFC 4273.

snmp-server enable traps linkmode

Note: This command may not be available on all platforms.

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.

Default enabled

Format `snmp-server enable traps linkmode`

Mode Global Config

no snmp-server enable traps linkmode

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

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

snmp-server enable traps multiusers

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

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

no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format `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

snmp-server engineID local

This command configures the SNMP engine ID on the local device.

Default The engineID is configured automatically, based on the device MAC address.
Format `snmp-server engineID local {`*`engine-id`*`|default}`

Mode Global Config

Parameter	*Description*
engine-id	A hexadecimal string identifying the engine-id. Engine-id must be an even length in the range of 6 to 32 hexadecimal characters.
default	Sets the engine-id to the default string, based on the device MAC address.

Caution! Changing the engineID will invalidate all SNMP configuration that exists on the box.

no snmp-server engineID local

This command removes the specified engine ID.

Default The engineID is configured automatically, based on the device MAC address.

Format `no snmp-server engineID local`

Mode Global Config

snmp-server filter

This command creates a filter entry for use in limiting which traps will be sent to a host.

Default No filters are created by default.

Format `snmp-server filter` *`filtername oid-tree`* `{included|excluded}`

Mode Global Config

Parameter	*Description*
filtername	The label for the filter being created. The range is 1 to 30 characters.
oid-tree	The OID subtree to include or exclude from the filter. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
included	The tree is included in the filter.
excluded	The tree is excluded from the filter.

no snmp-server filter

This command removes the specified filter.

Default No filters are created by default.

Format `snmp-server filter` *`filtername`* `[`*`oid-tree`*`]`

Mode Global Config

snmp-server group

This command creates an SNMP access group.

Default Generic groups are created for all versions and privileges using the default views.

Format `snmp-server group group-name {v1 | v2c | v3 {noauth | auth | priv}} [context context-name] [read read-view] [write write-view] [notify notify-view]`

Mode Global Config

Parameter	*Description*
group-name	The group name to be used when configuring communities or users. The range is 1 to 30 characters.
v1	This group can only access via SNMPv1.
v2	This group can only access via SNMPv2c.
v3	This group can only access via SNMPv3.
noauth	This group can be accessed only when not using Authentication or Encryption. Applicable only if SNMPv3 is selected.
auth	This group can be accessed only when using Authentication but not Encryption. Applicable only if SNMPv3 is selected.
priv	This group can be accessed only when using both Authentication and Encryption. Applicable only if SNMPv3 is selected.
context-name	The SNMPv3 context used during access. Applicable only if SNMPv3 is selected.
read-view	The view this group will use during GET requests. The range is 1 to 30 characters.
write-view	The view this group will use during SET requests. The range is 1 to 30 characters.
notify-view	The view this group will use when sending out traps. The range is 1 to 30 characters.

no snmp-server group

This command removes the specified group.

Format `no snmp-server group group-name {v1|v2c| 3 {noauth|auth|priv}} [context context-name]`

Mode Global Config

snmp-server host

This command configures traps to be sent to the specified host.

Default No default hosts are configured.

Format `snmp-server host host-addr community-string [informs [timeout seconds] [retries retries]] [version {1 | 2c }] [udp-port port] [filter filter-name]`

Mode Global Config

Parameter	*Description*
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
community-string	Community string sent as part of the notification. The range is 1 to 20 characters.
traps	Send SNMP traps to the host. This option is selected by default.
version 1	Sends SNMPv1 traps. This option is not available if informs is selected.
version 2c	Sends SNMPv2c traps. This option is not available if informs is selected. This option is selected by default.
informs	Send SNMPv2 informs to the host.
seconds	The number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	The number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
port	The SNMP Trap receiver port. The default is port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

no snmp-server host

This command removes the specified host entry.

Format `no snmp-server host` *`host-addr`* `{traps|informs} version (1 | 2}`

Mode Global Config

snmp-server port

This command configures the UDP port number on which the SNMP server listens for requests.

Default 161

Format `snmp-server port` *`1025-65535`*

Mode Privileged EXEC

no snmp-server port

This command restores the SNMP server listen port to its factory default value.

Format `no snmp-server port`

Mode Privileged EXEC

snmp-server proxy

Use this command to enable DCSS to enter SNMP proxy mode, so that it can be managed with the Net-SNMP server. Once enabled, the current DCSS SNMP configuration is ignored, but preserved.

Format `snmp-server proxy`
Mode Global Config

no snmp-server proxy

Use this command to disable Net-SNMP proxy.

Format `no snmp-server proxy`
Mode Global Config

snmp-server trapsend

Use this command to set the UDP port to which traps are sent by the SNMP server.

Default 50505
Format `snmp-server trapsend portid`
Mode Global Config

no snmp-server trapsend

Use this command to send traps to the default UDP port.

Format `no snmp-server trapsend portid`
Mode Global Config

snmp-server user

This command creates an SNMPv3 user for access to the system.

Default No default users are created.
Format `snmp-server user username groupname [remote engineid-string] [ {auth-md5 password | auth-sha password | auth-md5-key md5-key | auth-sha-key sha-key} [priv-des password | priv-des-key des-key]`
Mode Global Config

Parameter	*Description*
username	The username the SNMPv3 user will connect to the switch as. The range is 1 to 30 characters.
group-name	The name of the group the user belongs to. The range is 1 to 30 characters.
engineid-string	The engine-id of the remote management station that this user will be connecting from. The range is 5 to 32 characters.
password	The password the user will use for the authentication or encryption mechanism. The range is 1 to 32 characters.

Parameter	*Description*
md5-key	A pregenerated MD5 authentication key. The length is 32 characters.
sha-key	A pregenerated SHA authentication key. The length is 48 characters.
des-key	A pregenerated DES encryption key. The length is 32 characters if MD5 is selected, 48 characters if SHA is selected.

no snmp-server user

This command removes the specified SNMPv3 user.

Format `no snmp-server user` *username*

Mode Global Config

snmp-server view

This command creates or modifies an existing view entry that is used by groups to determine which objects can be accessed by a community or user.

Default Views are created by default to provide access to the default groups.

Format `snmp-server viewname oid-tree {included|excluded}`

Mode Global Config

Parameter	*Description*
viewname	The label for the view being created. The range is 1 to 30 characters.
oid-tree	The OID subtree to include or exclude from the view. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
included	The tree is included in the view.
excluded	The tree is excluded from the view.

no snmp-server view

This command removes the specified view.

Format `no snmp-server view viewname [oid-tree]`

Mode Global Config

snmp-server v3-host

This command configures traps to be sent to the specified host.

Default No default hosts are configured.

Format `snmp-server v3-host host-addr username [traps | informs [timeout seconds] [retries retries]] [auth | noauth | priv] [udpport port] [filter filtername]`

Mode Global Config

Parameter	*Description*
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
user-name	User used to send a Trap or Inform message. This user must be associated with a group that supports the version and access method. The range is 1 to 30 characters.
traps	Send SNMP traps to the host. This is the default option.
informs	Send SNMP informs to the host.
seconds	Number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	Number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.

Parameter	*Description*
auth	Enables authentication but not encryption.
noauth	No authentication or encryption. This is the default.
priv	Enables authentication and encryption.
port	The SNMP Trap receiver port. This value defaults to port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

snmptrap source-interface

Use this command in Global Configuration mode to configure the global source-interface (Source IP address) for all SNMP communication between the SNMP client and the server.

Format `snmptrap source-interface {`*`slot/port`* `| loopback` *`loopback-id`*`|tunnel` *`tunnel-id`*`|vlan` *`vlan-id`*`}`

Mode Global Config

Parameter	*Description*
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

no snmptrap source-interface

Use this command in Global Configuration mode to remove the global source-interface (Source IP selection) for all SNMP communication between the SNMP client and the server.

Format `no snmptrap source-interface`

Mode Global Config

show snmp

This command displays the current SNMP configuration.

Format `show snmp`

Mode Privileged EXEC

Term		*Definition*
Community Table:	**Community-String**	The community string for the entry. This is used by SNMPv1 and SNMPv2 protocols to access the switch.
	Community-Access	The type of access the community has: • Read only • Read write • su
	View Name	The view this community has access to.
	IP Address	Access to this community is limited to this IP address.
Community Group Table:	**Community-String**	The community this mapping configures
	Group Name	The group this community is assigned to.
	IP Address	The IP address this community is limited to.
Host Table:	**Target Address**	The address of the host that traps will be sent to.
	Type	The type of message that will be sent, either traps or informs.
	Community	The community traps will be sent to.
	Version	The version of SNMP the trap will be sent as.
	UDP Port	The UDP port the trap or inform will be sent to.
	Filter name	The filter the traps will be limited by for this host.
	TO Sec	The number of seconds before informs will time out when sending to this host.
	Retries	The number of times informs will be sent after timing out.

show snmp engineID

This command displays the currently configured SNMP engineID.

Format `show snmp engineID`

Mode Privileged EXEC

Parameter	*Description*
Local SNMP EngineID	The current configuration of the displayed SNMP engineID.

show snmp filters

This command displays the configured filters used when sending traps.

Format `show snmp filters [filtername]`

Mode Privileged EXEC

Parameter	*Description*
Name	The filter name for this entry.
OID Tree	The OID tree this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID Tree.

show snmp group

This command displays the configured groups.

Format `show snmp group [groupname]`

Mode Privileged EXEC

Parameter	*Description*
Name	The name of the group.
Security Model	Indicates which protocol can access the system via this group.
Security Level	Indicates the security level allowed for this group.
Read View	The view this group provides read access to.
Write View	The view this group provides write access to.
Notify View	The view this group provides trap access to.

show snmp-server

This command displays the current SNMP server user configuration.

Format `show snmp-server`

Mode Privileged EXEC

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

```
(Routing)#show snmp-server

SNMP Server Port.............................. 161
SNMP Trap Send Port........................... 162
Net-SNMP Proxy Mode........................... Enable
```

show snmp user

This command displays the currently configured SNMPv3 users.

Format `show snmp user [username]`

Mode Privileged EXEC

Term	*Definition*
Name	The name of the user.
Group Name	The group that defines the SNMPv3 access parameters.
Auth Method	The authentication algorithm configured for this user.
Privilege Method	The encryption algorithm configured for this user.
Remote Engine ID	The engineID for the user defined on the client machine.

show snmp views

This command displays the currently configured views.

Format `show snmp views [viewname]`

Mode Privileged EXEC

Parameter	*Description*
Name	The view name for this entry.
OID Tree	The OID tree that this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID tree.

show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 trapflags. 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

Parameter	*Definition*
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPF traps' information.

show snmptrap source-interface

Use the `show tacacs source-interface` command in Global Config mode to display the configured global source interface details used for an SNMP client. The IP address of the selected interface is used as source IP for all communications with the server.

Format `show snmptrap source-interface`

Mode Privileged EXEC

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

```
(Config)# show snmptrap source-interface

SNMP Client Source Interface     : 0/2
SNMP Client Source IPv4 Address  : 192.168.2.20 [UP]
```

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

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)

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

Default none

Format `copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:clibanner`

`copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>`

Mode Privileged EXEC

set prompt

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

Format `set prompt` *`prompt_string`*

Mode Privileged EXEC

set clibanner

Use this command to configure the pre-login CLI banner before displaying the login prompt.

Format `set clibanner` *`line`*

Mode Global Config

Parameter	*Description*
line	Banner text where “” (double quote) is a delimiting character. The banner message can be up to 2000 characters.

no set clibanner

Use this command to remove the pre-login CLI banner.

Format `no set clibanner`

Mode Global Config

show clibanner

Use this command to display the configured pre-login CLI banner. The pre-login banner is the text that displays before displaying the CLI prompt.

Default	No contents to display before displaying the login prompt.
Format	`show clibanner`
Mode	Privileged EXEC

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

```
(Routing) #show clibanner

Banner Message configured :
=========================


--------------------------
         TEST
--------------------------
```

hostname

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

Format	`hostname` *`hostname`*
Mode	Privileged EXEC

Front Panel TAP Interfaces

Use the commands in this section to enable and monitor FPTI mode.

fpti

Use this command to enable FPTI mode either globally (in Global Config mode) or for a specific interface (in Interface Config mode).

Default Enabled

Format `fpti`

Mode
- Global Config
- Interface Config

no fpti

Use this command to disable FPTI mode.

Format `no fpti`

Mode
- Global Config
- Interface Config

show port fpti

Use this command to display the FPTI mode on all interfaces and the global FPTI mode. If an interface is specified, only the FPTI mode for the specified interface is displayed.

Format `show port fpti [slot/port]`

Mode
- Global Config
- Interface Config

Example:

```
(Switching) show port fpti

Global Front Panel Tap Interface Mode.......... Enabled

 Intf     Mode
--------- ---------------
0/1       Enabled
0/2       Enabled
0/3       Enabled
0/4       Enabled
0/5       Enabled
0/6       Enabled
0/7       Enabled
0/8       Enabled
0/9       Enabled
```

```
0/10      Enabled
0/11      Enabled
0/12      Enabled
0/13      Enabled
0/14      Enabled
0/15      Enabled
0/16      Enabled
0/17      Enabled
0/18      Enabled
0/19      Enabled
0/20      Enabled
0/21      Enabled
0/22      Enabled
0/23      Enabled
0/24      Enabled
```

Example:

```
(Switching) show port fpti 0/1

Port.....................................  0/1
Front Panel Tap Interface Mode.............. Enabled
```

Section 6: Utility Commands

This section describes the following utility commands available in the DCSS CLI:

Note: The commands in this section are in one of five functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Debug commands provide diagnostic information and help troubleshoot network issues.
- Clear commands clear some or all of the settings to factory defaults.

CLI Output Filtering Commands

show *xxx*|include "*string*"

The command ***xxx*** is executed and the output is filtered to only show lines containing the "***string***" match. All other non-matching lines in the output are suppressed.

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

```
(Routing) #show running-config | include "spanning-tree"

spanning-tree configuration name "00-02-BC-42-F9-33"
spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```

show *xxx*|include "*string*" exclude "*string2*"

The command ***xxx*** is executed and the output is filtered to only show lines containing the "***string***" match and not containing the "***string2***" match. All other non-matching lines in the output are suppressed. If a line of output contains both the include and exclude strings then the line is not displayed.

Example: The following example shows output of the CLI command.

```
(Routing) #show running-config | include "spanning-tree" exclude "configuration"

spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```

show *xxx*|exclude "*string*"

The command ***xxx*** is executed and the output is filtered to show all lines not containing the "***string***" match. Output lines containing the "***string***" match are suppressed.

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

```
(Routing) #show interface 0/1

Packets Received Without Error..... 0
Packets Received With Error..... 0
Broadcast Packets Received..... 0
Packets Transmitted Without Errors..... 0
Transmit Packet Errors..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 20 day 21 hr 30 min 9 sec

(Routing) #show interface 0/1 | exclude "Packets"

Transmit Packet Errors..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 20 day 21 hr 30 min 9 sec
```

show *xxx*|begin "*string*"

The command ***xxx*** is executed and the output is filtered to show all lines beginning with and following the first line containing the "***string***" match. All prior lines are suppressed.

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

```
(Routing) #show port all | begin "1/1"

1/1           Enable                         Down   Disable N/A    N/A
1/2           Enable                         Down   Disable N/A    N/A
1/3           Enable                         Down   Disable N/A    N/A
1/4           Enable                         Down   Disable N/A    N/A
1/5           Enable                         Down   Disable N/A    N/A
1/6           Enable                         Down   Disable N/A    N/A

(Routing) #
```

show *xxx*|section "*string*"

The command ***xxx*** is executed and the output is filtered to show only lines included within the section(s) identified by lines containing the "***string***" match and ending with the first line containing the default end-of-section identifier (i.e. "exit").

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

```
(Routing) #show running-config | section "interface 0/1"

interface 0/1
no spanning-tree port mode
exit
```

show *xxx*|section "*string*" "*string2*"

The command ***xxx*** is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the "***string***" match and ending with the first line containing the "***string2***" match. If multiple sessions matching the specified string match criteria are part of the base output, then all instances are displayed.

show *xxx*|section "*string*" include "*string2*"

The command ***xxx*** is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the "***string***" match and ending with the first line containing the default end-of-section identifier (i.e. "exit") and that include the "string2" match. This type of filter command could also include "exclude" or user-defined end-of-section identifier parameters as well.

Dual Image Commands

Note: These commands are only available on selected Linux-based platforms.

DCSS 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 down-time when you upgrade or downgrade the software.

delete

This command deletes the backup image file from the permanent storage or the core dump file from the local file system.

Format	`delete backup` `delete core-dump-file` *`file-name`* `| all`
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 doesn't 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 `filedescr {active | backup} text-description`
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 `update bootcode`
Mode Privileged EXEC

System Information and Statistics Commands

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 - network or service ports. ARP entries associated with routing interfaces are not listed.

Format `show arp switch`
Mode Privileged EXEC

Parameter	*Definition*
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.

Parameter	*Definition*
Interface	For a service port the output is *Management*. For a network port, the output is the slot/port of the physical interface.

dir

Use this command to list the files in the directory /mnt/fastpath in flash from the CLI.

Format dir

Mode Privileged EXEC

```
(Routing) #dir

    0  drwx                2048 May 09 2002 16:47:30 .
    0  drwx                2048 May 09 2002 16:45:28 ..
    0  -rwx                 592 May 09 2002 14:50:24 slog2.txt
    0  -rwx                  72 May 09 2002 16:45:28 boot.dim
    0  -rwx                   0 May 09 2002 14:46:36 olog2.txt
    0  -rwx            13376020 May 09 2002 14:49:10 image1
    0  -rwx                   0 Apr 06 2001 19:58:28 fsyssize
    0  -rwx                1776 May 09 2002 16:44:38 slog1.txt
    0  -rwx                 356 Jun 17 2001 10:43:18 crashdump.ctl
    0  -rwx                1024 May 09 2002 16:45:44 sslt.rnd
    0  -rwx            14328276 May 09 2002 16:01:06 image2
    0  -rwx                 148 May 09 2002 16:46:06 hpc_broad.cfg
    0  -rwx                   0 May 09 2002 14:51:28 olog1.txt
    0  -rwx                 517 Jul 23 2001 17:24:00 ssh_host_key
    0  -rwx               69040 Jun 17 2001 10:43:04 log_error_crashdump
    0  -rwx                 891 Apr 08 2000 11:14:28 sslt_key1.pem
    0  -rwx                 887 Jul 23 2001 17:24:00 ssh_host_rsa_key
    0  -rwx                 668 Jul 23 2001 17:24:34 ssh_host_dsa_key
    0  -rwx                 156 Apr 26 2001 13:57:46 dh512.pem
    0  -rwx                 245 Apr 26 2001 13:57:46 dh1024.pem
    0  -rwx                   0 May 09 2002 16:45:30 slog0.txt
```

show eventlog

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

Format show eventlog

Mode Privileged EXEC

Parameter	*Definition*
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.

Parameter	*Definition*
Code	The event code.
Time	The time this event occurred.

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

show hardware

This command displays inventory information for the switch.

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 84.

Format `show hardware`

Mode Privileged EXEC

show slot

This command displays information about all the slots in the system or for a specific slot.

Format `show slot` *`[unit/slot]`*

Mode User EXEC

Term	*Definition*
Slot	The slot identifier in a *`unit/slot`* format.
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 *`unit/slot`*, the following additional information appears:

Term	*Definition*
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.

Term	*Definition*
Configured Card Description	10BASE-T half duplex

environment temprange

Use this command to set the allowed temperature range for normal operation.

Format `environment temprange min -100-100 max -100-100`

Mode Global Config

Parameter	*Definition*
min	Sets the minimum allowed temperature for normal operation. The range is between −100°C and 100°C. The default is 0°C.
max	Sets the maximum allowed temperature for normal operation. The range is between −100°C and 100°C. The default is 0°C.

environment trap

Use this command to configure environment status traps.

Format `environment trap {fan|powersupply|temperature}`

Mode Global Config

Parameter	*Definition*
fan	Enables or disables the sending of traps for fan status events. The default is enable.
powersupply	Enables or disables the sending of traps for power supply status events. The default is enable.
temperature	Enables or disables the sending of traps for temperature status events. The default is enable.

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 `show version`

Mode Privileged EXEC

Parameter	*Definition*
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 version bootloader

Use this command to display Uboot version information.

Format `show version bootloader`

Mode Privileged EXEC

Example: The following example shows the output of the command:

```
(Switching) #show version bootloader
Querying Active and Backup Software, please wait ....
Running Version.............................. B1.0.0.5
Active Version............................... B1.0.0.5
Backup Version............................... B1.0.0.2
```

show platform vpd

This command displays vital product data for the switch.

Format `show platform vpd`

Mode User Privileged

The following information is displayed.

Term	*Definition*
Operational Code Image File Name	Build Signature loaded into the switch
Software Version	Release Version Maintenance Level and Build (RVMB) information of the switch.
Timestamp	Timestamp at which the image is built

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

```
(Routing) #show platform vpd

Operational Code Image File Name.............. FastPath-DCSS-esw-xgs4-gto-BL20R-CS-
6IQHr3v7m14b35
Software Version.............................. 3.7.14.35
Timestamp..................................... Thu Mar  7 14:36:14 IST 2013
```

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 | lag` *`lag-id`*`}`

Mode Privileged EXEC

The display parameters, when the argument is *`slot/port`*, are as follows:

Parameters	*Definition*
Packets Received Without Error	The total number of packets (including broadcast 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.
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. One possible reason for discarding such a packet could be to free up buffer space.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
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.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.

Parameters	*Definition*
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is “switchport” are as follows:

Parameter	*Definition*
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interfaces status

Use this command to display interface information, including the description, port state, speed and auto-neg capabilities. The command is similar to `show port all` but displays additional fields like interface description and port-capability.

The description of the interface is configurable through the existing command `description <name>` which has a maximum length of 64 characters that is truncated to 28 characters in the output. The long form of the description can be displayed using `show port description`. The interfaces displayed by this command are physical interfaces, LAG interfaces and VLAN routing interfaces.

Format `show interfaces status [{`*`slot/port`*` | vlan `*`id`*`}]`

Mode Privileged EXEC

Field	*Description*
Port	The interface associated with the rest of the data in the row.
Name	The descriptive user-configured name for the interface.

Field	*Description*
Link State	Indicates whether the link is up or down.
Physical Mode	The speed and duplex settings on the interface.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. The physical status for LAGs is not reported. When a port is down, the physical status is unknown.
Media Type	The media type of the interface.
Flow Control Status	The 802.3x flow control status.
Flow Control	The configured 802.3x flow control mode.

show interface counters

This command reports key summary statistics for all the ports (physical/CPU/port-channel).

Format `show interface counters`

Mode Privileged EXEC

Parameter	*Definition*
Port	The physical port, LAG, or CPU interface associated with the rest of the data in the row.
InOctets	The number of inbound octets received by the interface.
InUcastPkts	The number of inbound unicast packets received by the interface.
InMcastPkts	The number of inbound multicast packets received by the interface.
InBcastPkts	The number of inbound broadcast packets received by the interface.
OutOctets	The number of outbound octets transmitted by the interface.
OutUcastPkts	The number of outbound unicast packets transmitted by the interface.
OutMcastPkts	The number of outbound multicast packets transmitted by the interface.
OutBcastPkts	The number of outbound broadcast packets transmitted by the interface.

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

```
(Routing) #show interface counters

Port              InOctets      InUcastPkts      InMcastPkts      InBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1                0              0              0                0
0/2                0              0              0                0
0/3                15098          0              31               39
0/4                0              0              0                0
0/5                0              0              0                0
...
ch1                0              0              0                0
ch2                0              0              0                0
...
ch64               0              0              0                0
CPU                359533         0              3044             217
```

```
Port             OutOctets     OutUcastPkts     OutMcastPkts     OutBcastPkts
---------- ---------------- ---------------- ---------------- ----------------
0/1                0             0                0             0
0/2                0             0                0             0
0/3                131369        0                11            89
0/4                0             0                0             0
0/5                0             0                0             0
...
...
ch1                0             0                0             0
ch2                0             0                0             0
...
ch64               0             0                0             0
CPU                4025293       0                32910         120
```

show interface ethernet

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

Format `show interface ethernet {slot/port|all|switchport}`

Mode Privileged EXEC

When you specify a value for *slot/port*, the command displays the following information.

Parameter	*Definition*
Packets Received	• **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. • **Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Received 65–127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 128–255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Parameter	*Definition*
Packets Received (con't)	• **Packets Received 256–511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 512–1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 1024–1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received > 1518 Octets** - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
–	• **Packets 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). • **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). • **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). • **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).
–	• **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). • **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). • **Packets RX and TX 1519–2047 Octets** - The total number of packets received and transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **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. • **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. • **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.
Packets Received Successfully	• **Total Packets Received Without Error** - The total number of packets received that were without errors. • **Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol. • **Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address.

Parameter	*Definition*
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. One possible reason for discarding such a packet could be to free up buffer space.
Packets Received with MAC Errors	• **Total Packets Received with MAC Errors** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. • **Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. • **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). • **Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. • **Rx FCS Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Received Packets Not Forwarded	• **Total Received Packets Not Forwarded** - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process • **Local Traffic Frames** - The total number of frames dropped in the forwarding process because the destination address was located off of this port. • **802.3x Pause Frames Received** - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. • **Unacceptable Frame Type** - The number of frames discarded from this port due to being an unacceptable frame type. • **Reserved Address Discards** - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system. • **Broadcast Storm Recovery** - The number of frames discarded that are destined for `FF:FF:FF:FF:FF:FF` when Broadcast Storm Recovery is enabled. • **CFI Discards** - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format. • **Upstream Threshold** - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Parameter	*Definition*
Packets Transmitted Octets	• **Total Packets Transmitted (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- • **Packets Transmitted 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted > 1518 Octets** - The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Max Frame Size** - The maximum size of the Info (non-MAC) field that this port will receive or transmit. • **Maximum Transmit Unit** - The maximum Ethernet payload size.
Packets Transmitted Successfully	• **Total Packets Transmitted Successfully**- The number of frames that have been transmitted by this port to its segment. • **Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. • **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.
Transmit Errors	• **Total Transmit Errors** - The sum of Single, Multiple, and Excessive Collisions. • **Tx FCS Errors** - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Oversized** - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s. • **Underrun Errors** - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Parameter	*Definition*
Transmit Discards	• **Total Transmit Packets Discards** - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded. • **Single Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. • **Multiple Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. • **Excessive Collisions** - A count of frames for which transmission on a particular interface fails due to excessive collisions. • **Port Membership Discards** - The number of frames discarded on egress for this port due to egress filtering being enabled.
Protocol Statistics	• **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. • **STP BPDUs Transmitted** - Spanning Tree Protocol Bridge Protocol Data Units sent. • **STP BPDUs Received** - Spanning Tree Protocol Bridge Protocol Data Units received. • **RST BPDUs Transmitted** - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. • **RSTP BPDUs Received** - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. • **MSTP BPDUs Transmitted** - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. • **MSTP BPDUs Received** - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.
Dot1x Statistics	• **EAPOL Frames Transmitted** - The number of EAPOL frames of any type that have been transmitted by this authenticator. • **EAPOL Start Frames Received** - The number of valid EAPOL start frames that have been received by this authenticator.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

If you use the `all` keyword, the following information appears.

Parameter	*Definition*
Total Octets Transmitted	The total number of octets of data (including those in bad packets) transmitted 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.
Total Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.

Parameter	*Definition*
Total Packets Transmitted Successfully	The number of frames that have been transmitted by this port to its segment.
Total Packets Received Without Error	The total number of packets received that were without errors.

If you use the `switchport` keyword, the following information appears.

Parameter	*Definition*
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) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
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.
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.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

Example: The following example shows CLI display output for the command when you use the `all` keyword.

```
(Routing) #show interface ethernet all
```

```
Port   Bytes Tx   Bytes Rx   Packets Tx    Packets Rx
-----  --------   --------   ----------    ----------
0/1    0          0          0             0
0/2    0          0          0             0
..
..
1/1    0          0          0             0
1/2    0          0          0             0
..
..
```

show interface ethernet switchport

This command displays the private VLAN mapping information for the switch interfaces.

Format `show interface ethernet` *`interface-id`* `switchport`

Mode Privileged EXEC

Parameter	*Description*
interface-id	The *slot/port* of the switch.

The command displays the following information.

Term	*Definition*
Private-vlan host-association	The VLAN association for the private-VLAN host ports.
Private-vlan mapping	The VLAN mapping for the private-VLAN promiscuous ports.

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 `all` or no 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`* | `lag` *`lag-id`*} 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 `show mac-addr-table [{`*`macaddr vlan_id`* | `all` | `count` | `interface {`*`slot/port`* | `lag` *`lag-id`* | `vlan` *`vlan_id`*`}` | `vlan` *`vlan_id`*`}]`

Mode Privileged EXEC

The following information displays if you do not enter a parameter, the keyword all, or the MAC address and VLAN ID.

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

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:

Parameter	*Definition*
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.
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

Use this command to configure the CPU utilization thresholds. The Rising and Falling thresholds are specified as a percentage of CPU resources. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds. The CPU utilization threshold configuration is saved across a switch reboot. Configuring the falling utilization threshold is optional. If the falling CPU utilization parameters are not configured, then they take the same value as the rising CPU utilization parameters.

Format `process cpu threshold type total rising` *`1-100`* `interval`

Mode Global Config

Parameter	*Description*
rising threshold	The percentage of CPU resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
rising interval	The duration of the CPU rising threshold violation, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).
falling threshold	The percentage of CPU resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled). A notification is triggered when the total CPU utilization falls below this level for a configured period of time. The falling utilization threshold notification is made only if a rising threshold notification was previously done. The falling utilization threshold must always be equal or less than the rising threshold value. The CLI does not allow setting the falling threshold to be greater than the rising threshold.
falling interval	The duration of the CPU falling threshold, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).

show process app-list

This command displays the user and system applications.

Note: This command is available in Linux 2.6 only.

Format `show process app-list`

Mode Privileged EXEC

Parameter	*Description*
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Admin Status	The administrative status of the process.
Auto Restart	Indicates whether the process will automatically restart if it stops.
Running Status	Indicates whether the process is currently running or stopped.

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

```
                              Admin     Auto      Running
ID    Name            PID     Status    Restart   Status
---- ---------------- ----- --------- --------- -------
   1 dataplane        15309 Enabled   Disabled  Running
   2 switchdrvr       15310 Enabled   Disabled  Running
   3 syncdb           15314 Enabled   Disabled  Running
   4 lighttpd         18718 Enabled   Enabled   Running
   5 syncdb-test          0 Disabled  Disabled  Stopped
   6 proctest             0 Disabled  Enabled   Stopped
   7 user.start           0 Enabled   Disabled  Stopped
```

show process proc-list

This command displays the configured and in-use processes.

Note: This command is available in Linux 2.6 only.

Format `show process proc-list`

Mode Privileged EXEC

Parameter	*Description*
PID	The number the software uses to identify the process.
Process Name	The name that identifies the process.
Application ID-Name	The application identifier and its associated name.
Child	Indicates whether the process has spawned a child process.
VM Size	Virtual memory size.
VM Peak	The maximum amount of virtual memory the process has used at a given time.
FD Count	The file descriptors count for the process.

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

```
(Routing) #show process proc-list

      Process         Application              VM Size  VM Peak
PID   Name            ID-Name              Chld  (KB)     (KB)    FD Count
---- ---------------- -------------------- ---- -------- -------- --------
15260 procmgr          0-procmgr             No       1984     1984        8
15309 dataplane        1-dataplane           No     293556   293560       11
15310 switchdrvr       2-switchdrvr          No     177220   177408       57
15314 syncdb           3-syncdb              No       2060     2080        8
18718 lighttpd         4-lighttpd            No       5508     5644       11
18720 lua_magnet       4-lighttpd            Yes     12112    12112        7
18721 lua_magnet       4-lighttpd            Yes     25704    25708        7
```

show process app-resource-list

This command displays the configured and in-use resources of each application.

Note: This command is available in Linux 2.6 only.

Format `show process app-resource-list`

Mode Privileged EXEC

Parameter	*Description*
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Memory Limit	The maximum amount of memory the process can consume.
CPU Share	The maximum percentage of CPU utilization the process can consume.
Memory Usage	The amount of memory the process is currently using.
Max Mem Usage	The maximum amount of memory the process has used at any given time since it started.

```
(Routing) #show process app-resource-list

                          Memory      CPU       Memory      Max Mem
ID   Name             PID  Limit       Share     Usage       Usage
---- ---------------- ---- ----------- --------- ----------- -----------
   1 switchdrvr        251   Unlimited Unlimited      380 MB      381 MB
   2 syncdb            252   Unlimited Unlimited        0 MB        0 MB
   3 syncdb-test         0   Unlimited Unlimited        0 MB        0 MB
   4 proctest            0       10 MB       20%        0 MB        0 MB
   5 utelnetd            0   Unlimited Unlimited        0 MB        0 MB
   6 lxshTelnetd         0   Unlimited Unlimited        0 MB        0 MB
   7 user.start          0   Unlimited Unlimited        0 MB        0 MB
```

show process cpu threshold

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.

Format `show process cpu threshold`

Mode Privileged EXEC

The following example shows CLI display output for the command using Linux.

```
(Switching) #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    dtlTask                   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%
```

show running-config

Use this command to display or capture 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: Show running-config 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 issue 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, i.e. if any interface only contains the default configuration, that interface will be skipped from the `show running-config` command output. This is true for any configuration mode that contains nothing but 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.)

Use the following keys to navigate the command output.

Key	*Action*
Enter	Advance one line.
Space Bar	Advance one page.
q	Stop the output and return to the prompt.

Note that `--More-- or (q)uit` is displayed at the bottom of the output screen until you reach the end of the output.

This command captures the current settings of OSPFv2 trapflag status:

- If all the flags are enabled, then the command displays `trapflags all`.
- If all the flags in a particular group are enabled, then the command displays `trapflags` *`group name`* `all`.
- If some, but not all, of the flags in that group are enabled, the command displays `trapflags` *`groupname flag-name`*.

Format `show running-config [all | scriptname]`

Mode Privileged EXEC

show running-config interface

Use this command to display the running configuration for a specific interface. Valid interfaces include physical, LAG, loopback, tunnel and VLAN interfaces.

Format `show running-config interface {interface | lag {lag-intf-num} | loopback {loopback-id} | tunnel {tunnel-id} | vlan {vlan-id}}`

Mode Privileged EXEC

Parameter	*Description*
interface	Running configuration for the specified interface.
lag-intf-num	Running configuration for the LAG interface.
loopback-id	Running configuration for the loopback interface.
tunnel-id	Running configuration for the tunnel interface.
vlan-id	Running configuration for the VLAN routing interface.

The following information is displayed for the command.

Parameter	*Description*
slot|port	Enter an interface in slot/port format.
lag	Display the running config for a specified lag interface.
loopback	Display the running config for a specified loopback interface.
tunnel	Display the running config for a specified tunnel interface.
vlan	Display the running config for a specified vlan routing interface.

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

```
(Routing) #show running-config interface 0/1
!Current Configuration:
!
interface  0/1
addport 3/1
exit
(Routing) #
```

show

This command displays the content of text-based configuration files from the CLI. The text-based configuration files (startup-config, backup-config and factory-defaults) are saved compressed in flash. With this command, the files are decompressed while displaying their content.

Format `show { startup-config | backup-config | factory-defaults }`

Mode Privileged EXEC

Parameter	*Description*
startup-config	Display the content of the startup-config file.
backup-config	Display the content of the backup-config file.
factory-defaults	Display the content of the factory-defaults file.

Example: The following example shows CLI display output for the command using the startup-config parameter.

```
(Routing) #show startup-config
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-Boot 2009.06 (Apr 19 2011 -
15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

Example: The following example shows CLI display output for the command using the backup-config parameter.

```
(Routing) #show backup-config
```

```
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-Boot 2009.06 (Apr 19 2011 -
15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

Example: The following example shows CLI display output for the command using the factory-defaults parameter.

```
(Routing) #show factory-defaults
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-Boot 2009.06 (Apr 19 2011 -
15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
!
```

```
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

show sysinfo

This command displays switch information.

Format `show sysinfo`

Mode Privileged EXEC

Parameter	*Definition*
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see “snmp-server” on page 58.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see “snmp-server” on page 58.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see “snmp-server” on page 58.
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 for the whole system, or for bgp, bgp-ipv6, ospf, or ospfv3 when you contact technical support. The output includes log history files from previous runs. The output of the `show tech-support` command combines the output of the following commands and includes log history files from previous runs:

- show version
- show sysinfo
- show port all
- show isdp neighbors
- show logging
- show event log
- show logging buffered
- show trap log
- show previous run persistent logs
- show running config
- show debugging

Note: The log messages are sorted and displayed in reverse chronological order.

Format `show tech-support [bgp|bgp-ipv6|ospf|ospfv3]`
Mode Privileged EXEC

length *value*

Use this command to set the pagination length to value number of lines for the sessions specified by configuring on different Line Config modes (telnet/ssh/console) and is persistent.

Example: **Length** command on Line Console mode applies for Serial Console session.

Default `24`
Format `length value`
Mode Line Config

no length *value*

Use this command to set the pagination length to the default value number of lines.

Format `no length value`
Mode Line Config

terminal length

Use this command to set the pagination length to *value* number of lines for the current session. This command configuration takes an immediate effect on the current session and is nonpersistent.

Default 24 lines per page
Format `terminal length value`
Mode Privileged EXEC

no terminal length

Use this command to set the *value* to the length value configured on Line Config mode depending on the type of session.

Format `no terminal length value`
Mode Privileged EXEC

show terminal length

Use this command to display all the configured terminal length values.

Format `show terminal length`

Mode Privileged EXEC

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

```
(Routing) #show terminal length
Terminal Length:
---------------------
For Current Session…….. 24
For Serial Console…… 24
For Telnet Sessions……... 24
For SSH Sessions…….. 24
```

memory free low-watermark processor

Use this command to get notifications when the CPU free memory falls below the configured threshold. A notification is generated when the free memory falls below the threshold. Another notification is generated once the available free memory rises to 10 percent above the specified threshold. To prevent generation of excessive notifications when the CPU free memory fluctuates around the configured threshold, only one Rising or Falling memory notification is generated over a period of 60 seconds. The threshold is specified in kilobytes. The CPU free memory threshold configuration is saved across a switch reboot.

Format `memory free low-watermark processor` *`1-1034956`*

Mode Global Config

Parameter	*Description*
low-watermark	When CPU free memory falls below this threshold, a notification message is triggered. The range is 1 to the maximum available memory on the switch. The default is 0 (disabled).

clear mac-addr-table

Use this command to dynamically clear learned entries from the forwarding database. Using the following options, the user can specify the set of dynamically-learned forwarding database entries to clear.

Default No default value.

Format `clear mac-addr-table {all | vlan` *`vlanId`* `| interface` *`slot/port`* `|` *`macAddr`* `[`*`macMask`*`] }`

Mode Privileged EXEC

Parameter	*Description*
all	Clears dynamically learned forwarding database entries in the forwarding database table.
vlan *vlanId*	Clears dynamically learned forwarding database entries for this *vlanId*.
interface *slot/port*	Clears forwarding database entries learnt on for the specified interface.

Parameter	*Description*
macAddr *macMask*	Clears dynamically learned forwarding database entries that match the range specified by MAC address and MAC mask. When MAC mask is not entered, only specified MAC is removed from the forwarding database table.

Logging Commands

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.

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

no logging buffered

This command disables logging to 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 Global Config

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 Global Config

logging cli-command

This command enables the CLI command logging feature, which enables the DCSS software to log all CLI commands issued on the system. The commands are stored in a persistent log. Use the `show logging persistent` command to display the stored history of CLI commands.

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 [severitylevel]`
Mode Global Config

no logging console

This command disables logging to the console.

Format `no logging console`
Mode Global Config

logging host

This command configures the logging host parameters. You can configure up to eight hosts.

Default
- port: 514 (for UDP) and 6514 (for TLS)
- authentication mode: anonymous
- certificate index: 0
- level: critical (2)

Format `logging host {hostaddress|hostname} addresstype tls [anon|x509name] certificate-index {port severitylevel}`
Mode Global Config

Parameter	*Description*
hostaddress|hostname	The IP address of the logging host.
address-type	Indicates the type of address being passed: DNS or IPv4.

Parameter	*Description*
tls	Enables TLS security for the host.
anon|x509name	The type of authentication mode: anonymous or x509name.
certificate-index	The certificate number to be used for authentication. The valid range is 0–8. Index 0 is used to the default file.
port	A port number from 1 to 65535.
severitylevel	Specify this 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).

Example: The following shows examples of the command.

```
(Routing) (Config)# logging host google.com dns 214
(Routing) (Config)# logging host 10.130.64.88 ipv4 214 6
(Routing) (Config)# logging host 5.5.5.5 ipv4 tls anon 6514 debug
(Routing) (Config)# logging host 5.5.5.5 ipv4 tls x509name 3 6514 debug
```

logging host reconfigure

This command enables logging host reconfiguration.

Format `logging host reconfigure` *`hostindex`*

Mode Global Config

Parameter	*Description*
hostindex	Enter the Logging Host Index for which to change the IP address.

logging host remove

This command disables logging to host. See “show logging hosts” on page 115 for a list of host indexes.

Format `logging host remove` *`hostindex`*

Mode Global Config

logging persistent

Use this command to configure 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 Disable

Format `logging persistent` *`severity level`*

Mode Global Config

no logging persistent

Use this command to disable the persistent logging in the switch.

Format `no logging persistent`
Mode Global Config

logging protocol

Use this command to configure the logging protocol version number as 0 or 1. RFC 3164 uses version 0 and RFC 5424 uses version 1.

Default The default is version 0 (RFC 3164).
Format `logging protocol {0|1}`
Mode Global Config

logging syslog

This command enables syslog logging.

Default disabled
Format `logging syslog`
Mode Global Config

no logging syslog

This command disables syslog logging.

Format `no logging syslog`
Mode Global Config

logging syslog port

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

Default disabled
Format `logging syslog port` *`portid`*
Mode Global Config

no logging syslog port

This command disables syslog logging.

Format `no logging syslog port`

Mode Global Config

logging syslog source-interface

Use this command to specify the physical or logical interface to use as the Syslog client source interface. If configured, the address of source Interface is used for all Syslog communications between the Syslog server and the Syslog client. Otherwise there is no change in behavior. If the configured interface is down, the Syslog client falls back to normal behavior.

Format `logging syslog source-interface {slot/port|{loopback loopback-id}|{vlan vlan-id}}`

Mode Global Config

Parameter	*Description*
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

no logging syslog source-interface

Use this command to remove the configured global source interface (Source IP selection) for all Syslog communications between the Syslog client and the server.

Format `no logging syslog source-interface`

Mode Global Config

show logging

This command displays logging configuration information.

Format `show logging`

Mode Privileged EXEC

Term	*Definition*
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
Logging Client Source Interface	Shows the configured syslog source-interface (source IP address).
CLI Command Logging	Shows whether CLI Command logging is enabled.

Term	*Definition*
Logging Protocol	The logging protocol version number. • 0: RFC 3164 • 1: RFC 5424
Console Logging	Shows whether console logging is enabled.
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.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity at which the logging entries are retained after a system reboot.
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.

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

```
(Routing) #show logging

Logging Client Local Port           : 514
Logging Client Source Interface     : (not configured)
CLI Command Logging                 : disabled
Logging Protocol                    : 1
Console Logging                     : enabled
Console Logging Severity Filter     : error
Buffered Logging                    : enabled
Persistent Logging                  : disabled
Persistent Logging Severity Filter  : alert

Syslog Logging                      : disabled

Log Messages Received               : 1010
Log Messages Dropped                : 0
Log Messages Relayed                : 0
```

show logging buffered

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

Format `show logging buffered`

Mode Privileged EXEC

Parameter	*Definition*
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

Term	*Definition*
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.
Status	Status field provides the current status of snmp row status. (Active, Not in Service, Not Ready).
Mode	The type of security: UDP or TLS.
Auth	The type of authentication mode: anonymous or x509name.
Cert #	The certificate number to be used for authentication. The valid range is 0–8. Index 0 is used to the default file.

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

```
(Routing) #show logging hosts
Index  IP Address/Hostname  Severity   Port   Status    Mode
----- --------------------- ---------- ------ --------- -----
1     1.1.1.17              critical   514    Active    udp
2     10.130.191.90         debug      10514  Active    tls
3     5.5.5.5               debug      333    Active    tls

Auth     Cert#
-------- -----

x509name 6
x509name 4
```

show logging persistent

Use the **show logging persistent** command to display persistent log entries. If `log-files` is specified, the persistent log files the system are displayed.

Format `show logging persistent [log-files]`

Mode Privileged EXEC

Parameter	*Description*
Persistent Logging	If persistent logging is enabled or disabled.
Persistent Log Count	The number of persistent log entries.
Persistent Log Files	The list of persistent log files in the system. Only displayed if `log-files` is specified.

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

```
(Switching) #show logging persistent

Persistent Logging    : disabled
Persistent Log Count  : 0

(Switching) #show logging persistent log-files

Persistent Log Files:

slog0.txt
slog1.txt
slog2.txt
olog0.txt
olog1.txt
olog2.txt
```

show logging traplogs

This command displays SNMP trap events and statistics.

Format `show logging traplogs`

Mode Privileged EXEC

Parameter	*Definition*
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.

Parameter	*Definition*
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.

clear logging buffered

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

Format `clear logging buffered`
Mode Privileged EXEC

Email Alerting and Mail Server Commands

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 [severitylevel]`
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 e-mailed immediately in a single e-mail 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 {severitylevel | 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.

Format `logging email message-type {urgent |non-urgent |both} to-addr` *`to-email-addr`*
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` *`to-email-addr`*
Mode Global Config

logging email from-addr

This command configures the email address of the sender (the switch).

Default switch@adtran.com
Format `logging email from-addr` *`from-email-addr`*
Mode Global Config

no logging email from-addr

This command removes the configured email source address.

Format `no logging email from-addr` *`from-email-addr`*
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` *`subject`*

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 30–1440 minutes.

Default 30 minutes

Format `logging email logtime` *`minutes`*

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` *severitylevel*

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` *message-body*

Mode Global Config

show logging email config

This command displays information about the email alert configuration.

Format `show logging email config`

Mode Privileged EXEC

Parameter	*Definition*
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.

Parameter	*Definition*
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

Parameter	*Definition*
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 or DNS name format.

Format `mail-server {ip-address | hostname}`
Mode Global Config

no mail-server

This command removes the specified SMTP server from the configuration.

Format `no mail-server {ip-address | hostname}`
Mode Global Config

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 {tlsv1 | none}`
Mode Mail Server Config

port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, and for no security (i.e. 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 (Mail Server Config)

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

Default admin
Format `username name`
Mode Mail Server Config

password

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

Default admin

Format `password password`

Mode Mail Server Config

show mail-server config

This command displays information about the email alert configuration.

Format `show mail-server {ip-address | hostname | all} config`

Mode Privileged EXEC

Parameter	*Definition*
No of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4 address or DNS hostname 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.

System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

clear config

This command resets the configuration of the switch to the configuration present in the `factory-defaults` configuration file, if this file is present, without powering off the switch. If the `factory-defaults` configuration file is not present, then DCSS compile time defaults are applied on the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter `y`, you automatically reset the 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 an interface on a VLAN based on the argument. If a virtual router is specified, the statistics for the ports on the virtual router are cleared. If no router is specified, the information for the default router will be displayed.

Format `clear counters {`*`slot/port`* `| all [vrf` *`vrf-name`*`] | vlan` *`id`*`}`

Mode Privileged EXEC

clear ip access-list counters

This command clears the counters of the specified IP ACL and the IP ACL rule.

Format `clear ip access-list counters` *`acl-ID`* `|` *`acl-name rule-id`*

Mode Privileged EXEC

clear ipv6 access-list counters

This command clears the counters of the specified IP ACL and the IP ACL rule.

Format `clear ipv6 access-list counters` *`acl-name rule-id`*

Mode Privileged EXEC

clear mac access-list counters

This command clears the counters of the specified MAC ACL and MAC ACL rule.

Format `clear mac access-list counters` *`acl-name rule-id`*

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 configuration changes before logging out.

Format `logout`

Modes
- Privileged EXEC
- User EXEC

ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI interface.

Default
- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format `ping [vrf vrf-name] {ip-address| hostname | {ipv6 {interface {unit/slot/port | vlan 1-4093 | loopback loopback-id | network | serviceport | tunnel tunnel-id } link-local-address} | ip6addr | hostname} [count count] [interval 1-60] [size size] [source ip-address | ip6addr | {unit/slot/port | vlan 1-4093 | serviceport | network}]`

Modes
- Privileged EXEC
- User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	*Description*
vrf-name	The name of the virtual router in which to initiate the ping. If no virtual router is specified, the ping is initiated in the default router instance.
address	IPv4 or IPv6 addresses to ping.
count	Use the `count` 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.

Parameter	*Description*
interval	Use the `interval` parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the `size` parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the *source* parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.
hostname	Use the *hostname* parameter to resolve to an IPv4 or IPv6 address. The *ipv6* keyword is specified to resolve the hostname to IPv6 address. The IPv4 address is resolved if no keyword is specified.
ipv6	The optional keyword *ipv6* can be used before the *ipv6-address* or *hostname* argument. Using the *ipv6* optional keyword before *hostname* tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.
interface	Use the *interface* keyword to ping a link-local IPv6 address over an interface.
link-local-address	The link-local IPv6 address to ping over an interface.

The following are examples of the CLI command.

Example: ping success:

```
(Routing) #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: ping failure:

In Case of Unreachable Destination:

```
(Routing) # 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
```

In Case Of Request TimedOut:

```
(Routing) # 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`

Modes
- 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.

If ONIE is installed, the `os` parameter is added to the reload command. This parameter enables the user to boot back into ONIE.

Format `reload [warm | configuration [`*`scriptname`*`]]`

Mode Privileged EXEC

Parameter	*Description*
warm	When the Warm Reload feature is present, the reload command adds the `warm` option. This option reduces the time it takes to reboot a Linux switch, thereby reducing the traffic disruption in the network during a switch reboot. For a typical Linux Enterprise switch, the traffic disruption is reduced from about two minutes for a cold reboot to about 20 seconds for a warm reboot. ***Note:*** The Warm Reload starts only the application process. The Warm Reload does not restart the boot code, the Linux kernel and the root file system. Since the Warm Reload does not restart all components, some code upgrades require that customers perform a cold reboot. ***Note:*** Warm resets can only be initiated by the administrator and do not occur automatically.
configuration	Gracefully reloads the configuration. If no configuration file is specified, the startup-config file is loaded.
scriptname	The configuration file to load. The scriptname must include the extension.

copy

The `copy` 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 using FTP, TFTP, Xmodem, Ymodem, or Zmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

Format `copy` *`source destination`* `{verify | noverify}`

Mode Privileged EXEC

Replace the *source* and *destination* parameters with the options in Table 9 on page 130. For the *url* source or destination, use one of the following values:
{xmodem | tftp://*ipaddr*|*hostname* | *ip6address*|*hostname/filepath/filename* [noval]| sftp|scp://*username@ipaddr* | *ipv6address/filepath/filename* | ftp://*user@ipaddress* | *hostname/filepath/filename*}

verify | *noverify* is only available if the image/configuration verify options feature is enabled (see "file verify" on page 133). verify specifies that digital signature verification will be performed for the specified downloaded image or configuration file. noverify specifies that no verification will be performed.

The keyword **ias-users** supports the downloading of the IAS user database file. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and its attributes available in the downloaded file. In the command **copy *url* ias-users**, for *url* one of the following is used for IAS users file:

{ { tftp://<ipaddr | hostname> | <ipv6address | hostname> /<filepath>/<filename> } | { sftp | scp://<username>@<ipaddress>/<filepath>/<filename>} }

Note: The maximum length for the file path is 160 characters, and the maximum length for the file name is 31 characters.

For FTP, 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.

To copy OpenFlow SSL certificates to the switch using TFTP or XMODEM, using only the following options pertinent to the OpenFlow SSL certificates.

Format copy [<mode/file>] nvram:{openflow-ssl-ca-cert | openflow-ssl-cert | openflow-ssl-priv-key}

Mode Privileged EXEC

\

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.

Table 9: Copy Parameters

Source	*Destination*	*Description*
nvram:application: *sourcefilename*	*url*	Filename of source application file.
nvram:backup-config	nvram:startup-config	Copies the backup configuration to the startup configuration.
nvram:clibanner	*url*	Copies the CLI banner to a server.

Table 9: Copy Parameters (Cont.)

Source	*Destination*	*Description*
`nvram: core-dump`	`tftp://<ipaddress|hostname>/<filepath>/<filename>| ftp://<user>@<ipaddr|hostname>/<path>/<filename> | scp://<user>@<ipaddr|hostname>/<path>/<filename> | sftp://<user>@<ipaddr|hostname>/<path>/<filename>}`	Uploads the core dump file on the local system to an external TFTP/FTP/SCP/SFTP server.
`nvram:crash-log`	`url`	Copies the crash log to a server.
`nvram:errorlog`	*`url`*	Copies the error log file to a server.
`nvram:factory-defaults`	*`url`*	Uploads factory defaults file.
`nvram:fastpath.cfg`	*`url`*	Uploads the binary config file to a server.
`nvram:log`	*`url`*	Copies the log file to a server.
`nvram:operational-log`	`url`	Copies the operational log file to a server.
`nvram:script` *`scriptname`*	*`url`*	Copies a specified configuration script file to a server.
`nvram:startup-config`	`nvram:backup-config`	Copies the startup configuration to the backup configuration.
`nvram:startup-config`	*`url`*	Copies the startup configuration to a server.
`nvram:startup-log`	`url`	Copies the startup log to a server.
`nvram: tech-support`	*`url`*	Uploads the system and configuration information for technical support.
`nvram:traplog`	*`url`*	Copies the trap log file to a server.
`system:image`	`url`	Saves the system image to a server.
`system:running-config`	`nvram:startup-config`	Saves the running configuration to NVRAM.
`system:running-config`	`nvram:factory-defaults`	Saves the running configuration to NVRAM to the `factory-defaults` file.
`url`	`nvram:application` *`destfilename`*	Destination file name for the application file.
`url`	`nvram: application` *`destfilename`*	Downloads an application to the system.
`url`	`nvram: backup-config`	Downloads the backup configuration to the
`url`	`nvram:ca-root` *`index`*	Downloads the CA certificate file to /mnt/fastpath directory and uses the index number name the downloaded file to CA*index*.pem
`url`	`nvram:clibanner`	Downloads the CLI banner to the system.
`url`	`nvram:client-key` *`index`*	Downloads the client key file to the /mnt/fastpath directory and uses the index number name the downloaded file to CA*index*.key.
`url`	`nvram:client-ssl-cert` *`1-8`*	Downloads the client certificate to the /mnt/fastpath directory and uses the index number to name the downloaded file to CA*index*.pem.

Table 9: Copy Parameters (Cont.)

Source	*Destination*	*Description*
url	nvram:fastpath.cfg	Downloads the binary config file to the system.
url	nvram:script *destfilename*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
url	nvram:script *destfilename* noval	When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows:
(Routing) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval		
url	nvram:sshkey-dsa	Downloads an SSH key file. For more information, see "Secure Shell Commands" on page 51.
url	nvram:sshkey-rsa1	Downloads an SSH key file.
url	nvram:sshkey-rsa2	Downloads an SSH key file.
url	nvram:openflow-ssl-ca-cert	Downloads Openflow CA Certificate.
url	nvram:openflow-ssl-cert	Downloads Openflow Switch Certificate.
url	nvram:openflow-ssl-priv-key	Downloads Openflow Private Key.
url	nvram:startup-config	Downloads the startup configuration file to the system.
url	ias-users	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.
url	nvram:tech-support-cmds	Downloads the file containing list of commands to be displayed using the show tech-support command.
url	{active | backup}	Download an image from the remote server to either image.
{active | backup}	*url*	Upload either image to the remote server.
active	backup	Copy the active image to the backup image.
backup	active	Copy the backup image to the active image.

Example: The following shows an example of downloading and applying ias users file.

```
(Routing) #copy tftp://10.131.17.104/aaa_users.txt ias-users

Mode..................................... TFTP
Set Server IP............................ 10.131.17.104
Path..................................... ./
Filename................................. aaa_users.txt
Data Type................................ IAS Users

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
```

```
Validating and updating the users to the IAS users database.

Updated IAS users database successfully.

(Routing) #
```

file verify

This command enables digital signature verification while an image and/or configuration file is downloaded to the switch.

Format `file verify {all | image | none | script}`
Mode Global Config

Parameter	*Description*
All	Verifies the digital signature of both image and configuration files.
Image	Verifies the digital signature of image files only.
None	Disables digital signature verification for both images and configuration files.
Script	Verifies the digital signature of configuration files.

no file verify

Resets the configured digital signature verification value to the factory default value.

Format `no file verify`
Mode Global Config

write memory

Use this command to save 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`. Use the `confirm` keyword to directly save the configuration to NVRAM without prompting for a confirmation.

Format `write memory [confirm]`
Mode Privileged EXEC

Simple Network Time Protocol Commands

This section describes the commands you use to automatically configure the system time and date by using Simple Network Time Protocol (SNTP).

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 10.

Default 6
Format `sntp broadcast client poll-interval` *poll-interval*
Mode Global Config

no sntp broadcast client poll-interval

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

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

sntp client mode

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

Default disabled
Format `sntp client mode` *[broadcast | unicast]*
Mode Global Config

no sntp client mode

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

Format `no sntp client mode`
Mode Global Config

sntp client port

This command sets the SNTP client port ID to a 0, 123, or a value between 1025 and 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 OS.

Default 0

Format `sntp client port portid`
Mode Global Config

no sntp client port

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

Format `no sntp client port`
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 10.

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

no sntp unicast client poll-interval

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

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

sntp unicast client poll-timeout

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

Default 5
Format `sntp unicast client poll-timeout poll-timeout`
Mode Global Config

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.

Default 1
Format `sntp unicast client poll-retry poll-retry`
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 server

This command configures an SNTP server (a maximum of three). The server address is an IPv4/IPv6 address. The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

Format `sntp server {ipaddress | ipv6address | hostname} [priority [version [portid]]]`
Mode Global Config

no sntp server

This command deletes an server from the configured SNTP servers.

Format `no sntp server remove {ipaddress | ipv6address | hostname}`
Mode Global Config

sntp source-interface

Use this command to specify the physical or logical interface to use as the SNTP client source interface. If configured, the address of source Interface is used for all SNTP communications between the SNTP server and the SNTP client. Otherwise there is no change in behavior. If the configured interface is down, the SNTP client falls back to its default behavior.

Format `sntp source-interface {slot/port | loopback loopback-id | vlan vlan-id}`
Mode Global Config

Parameter	*Description*
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.

Parameter	*Description*
vlan-id	Specifies the VLAN to use as the source interface.

no sntp source-interface

Use this command to reset the SNTP source interface to the default settings.

Format `no sntp source-interface`

Mode Global Config

show sntp

This command is used to display SNTP settings and status.

Format `show sntp`

Mode Privileged EXEC

Parameter	*Definition*
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.

show sntp client

This command is used to display SNTP client settings.

Format `show sntp client`

Mode Privileged EXEC

Parameter	*Definition*
Client Supported Modes	Supported SNTP Modes (Broadcast or Unicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP Client Port. The field displays the value 0 if it is 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 OS.
Client Mode	Configured SNTP Client Mode.

show sntp server

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

Format `show sntp server`

Mode Privileged EXEC

Parameter	*Definition*
Server Host Address	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4 or 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:

Parameter	*Definition*
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server (IPv4 or 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.
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.

show sntp source-interface

Use this command to display the SNTP client source interface configured on the switch.

Format `show sntp source-interface`

Mode Privileged EXEC

Field	*Description*
SNTP Client Source Interface	The interface ID of the physical or logical interface configured as the SNTP client source interface.
SNTP Client Source IPv4 Address	The IP address of the interface configured as the SNTP client source interface.

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

```
(Routing) #show sntp source-interface

SNTP Client Source Interface.................. 0/2
SNTP Client Source IPv4 Address............... 192.168.2.20          [Up]
```

Time Zone Commands

clock set

This command sets the system time and date.

Note: System time and date cannot be set when SNTP is enabled. If SNTP is enabled after you configure the system time and date, the SNTP clock takes precedence over the user-configured system time and date. If the platform supports real-time clock (RTC), the set time and date can be retained after a save and reload. Otherwise, the configured clock will not be retained across reloads.

Format `clock set` *`hh:mm:ss`*
`clock set` *`mm/dd/yyyy`*

Mode Global Config

Parameter	*Description*
hh	Hours in 24-hour format. The range is 0 to 23.
mm	Minutes, the range is 0 to 59.
ss	Seconds, the range is 0 to 59.
mm	Month, in 2-character numeric format. The range is 01 to 12.
dd	Day, in 2-character numeric format. The range is 01 to 31.
yyyy	Year, in 4-character numeric format. The range is 2010 to 2079.

Example: The following shows an example of the command.

```
(Routing)(Config)# clock set 03:17:00
(Routing) (Config)# clock set 11/01/2011
```

clock summer-time date

This command sets the Daylight Saving Time (DST), also known as summertime, offset to UTC. You have to specify the start year and end year along with the month, day, and time. If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Format `clock summer-time date {`*`date month year hh:mm date month year hh:mm`*`}[offset` *`offset`*`] [zone` *`acronym`*`]`

Mode Global Config

Parameter	*Description*
date	Day of the month. The range is 1 to 31.
month	Month. The range is the first three letters by name (for example, Jan).
year	Year. The range is 2000 to 2097.
hh:mm	Time in 24-hour format in hours and minutes. hh range is 0 to 23, mm range is 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the time zone to be displayed when summertime is in effect. The range is up to four characters.

Example: The following shows examples of the command.

```
(Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
```

(Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18 offset 120 zone INDA

clock summer-time recurring

This command sets the summertime offset to UTC recursively every year. This means that summertime will affect every year from the time of configuration. You have to specify the start and end parameters which include the month, day, and time. If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Format `clock summer-time recurring {`*`week day month hh:mm week day month hh:mm`*`}[offset `*`offset`*`] [zone `*`acronym`*`]`

Mode Global Config

Parameter	*Description*
EU	The system clock uses the standard recurring summer time settings used in countries in the European Union.
USA	The system clock uses the standard recurring daylight saving time settings used in the United States.
week	Week of the month. Range is 1 to 5, first, last.
day	Day of the week. The range is the first three letters by name; sun, for example.
month	Month. The range is the first three letters by name; jan for example.
hh:mm	Time in 24-hour format in hours and minutes. hh range is 0 to 23, mm range is 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the time zone to be displayed when summertime is in effect. The range is up to four characters.

Example: The following shows examples of the command.

```
(Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18
(Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18 offset 120 zone INDA
```

no clock summer-time

This command resets the summertime configuration.

Format `no clock summer-time`

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no clock summer-time
```

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 zero (0) or \0 as appropriate.`

Format `clock timezone {`*`hours`*`} [minutes `*`minutes`*`] [zone `*`acronym`*`]`

Mode Global Config

Parameter	*Description*
hours	Hours difference from UTC. The range is –12 to 13.
minutes	Minutes difference from UTC. The range is zero (0) to 59.
acronym	The acronym for the time zone. The range is up to four characters.

Example: The following shows an example of the command.

```
(Routing) (Config)# clock timezone 5 minutes 30 zone INDA
```

no clock timezone

`This command resets the time zone settings.`

Format no clock timezone

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no clock timezone
```

show clock

`This command displays the time and date from the system clock.`

Format `show clock`

Mode Privileged EXEC

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

```
(Routing) # show clock
```

```
15:02:09 (UTC+0:00) Nov 1 2011
No time source
```

Example: With the configuration above, the following output appears:

```
(Routing) # show clock

10:55:40 INDA(UTC+7:30) Nov 1 2011
No time source
```

show clock detail

This command displays the detailed system time along with the time zone and the summertime configuration.

Format	show clock detail
Mode	Privileged EXEC

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

```
(Routing) # show clock detail

15:05:24 (UTC+0:00) Nov 1 2011
No time source

 Time zone:
 Acronym not configured
 Offset is UTC+0:00

 Summertime:
 Summer-time is disabled
```

Example: With the configuration above, the following output appears:

```
(Routing) # show clock detail

10:57:57 INDA(UTC+7:30) Nov 1 2011
No time source

 Time zone:
 Acronym is INDA
 Offset is UTC+5:30

 Summertime:
 Acronym is INDA
 Recurring every year
 Begins on second Sunday of Nov at 03:18
 Ends on second Monday of Nov at 03:18
 Offset is 120 minutes
```

DNS Client Commands

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 DCSS.

ip domain lookup

Use this command to enable the DNS client.

Default enabled

Format `ip domain lookup`

Mode Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format `no ip domain lookup`

Mode Global Config

ip domain name

Use this command to define a default domain name that DCSS 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` *`name`*

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

Use this command to remove the default domain name configured using the `ip domain name` command.

Format `no ip domain name`

Mode Global Config

ip domain list

Use this command to define 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 none

Format `ip domain list` *`name`*

Mode Global Config

no ip domain list

Use this command to delete a name from a list.

Format `no ip domain list` *`name`*

Mode Global Config

ip name server

Use this command to configure 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 address of the server. The preference of the servers is determined by the order they were entered.

Format `ip name-server` *`server-address1`* [*`server-address2...server-address8`*]

Mode Global Config

no ip name server

Use this command to remove a name server.

Format `no ip name-server` [*`server-address1...server-address8`*]

Mode Global Config

ip name source-interface

Use this command to specify the physical or logical interface to use as the DNS client source interface. If configured, the address of source Interface is used for all DNS communications between the DNS server and the DNS client. Otherwise there is no change in behavior. If the configured interface is down, the DNS client falls back to its default behavior.

Format `ip name source-interface {`*`slot/port`* | `loopback` *`loopback-id`* | `tunnel` *`tunnel-id`* | `vlan` *`vlan-id`*`}`

Mode Global Config

Parameter	*Description*
slot/port	Specifies the port to use as the source interface.

Parameter	*Description*
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

no ip name source-interface

Use this command to reset the DNS source interface to the default settings.

Format `no ip name source-interface`
Mode Global Config

ip host

Use this command to define static host name-to-address mapping in the host cache. The parameter *name* is host name and *ip address* is the IP address of the host. The hostname can include 1–255 alphanumeric characters, periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default none
Format `ip host name ipaddress`
Mode Global Config

no ip host

Use this command to remove the name-to-address mapping.

Format `no ip host name`
Mode Global Config

ip domain retry

Use this command to specify 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 number`
Mode Global Config

no ip domain retry

Use this command to return to the default.

Format `no ip domain retry` *`number`*

Mode Global Config

ip domain timeout

Use this command to specify 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.

Default 3

Format `ip domain timeout` *`seconds`*

Mode Global Config

no ip domain timeout

Use this command to return to the default setting.

Format `no ip domain timeout` *`seconds`*

Mode Global Config

clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears IPv4 entries.

Format `clear host {`*`name`* `| all}`

Mode Privileged EXEC

Parameter	*Description*
name	A particular host entry to remove. The parameter *`name`* ranges from 1-255 characters.
all	Removes all entries.

show hosts

Use this command to display 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 1-255 characters. This command displays IPv4 entries.

Format `show hosts [name]`

Mode Privileged EXEC
User EXEC

Parameter	*Description*
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.
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 example shows CLI display output for the command.

```
(Switching) 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
```

IP Address Conflict Commands

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 `ip address-conflict-detect run`

Mode
- Global Config
- Virtual Router Config

show ip address-conflict

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

Format `show ip address-conflict`

Modes Privileged EXEC

Parameter	*Definition*
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 for the specified virtual router. If no router is specified, the command is executed for the default router.

Format `clear ip address-conflict-detect [vrf vrf-name]`

Modes Privileged EXEC

Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their DCSS product.

Caution! The output of “debug” commands can be long and may adversely affect system performance.

capture start

Use the command **capture start** to manually start capturing CPU packets for packet trace.

The packet capture operates in three modes:

- capture file
- remote capture
- capture line

The command is not persistent across a reboot cycle.

Format `capture start [{all | receive | transmit}]`
Mode Privileged EXEC

Parameter	*Description*
all	Capture all traffic.
receive	Capture only received traffic.
transmit	Capture only transmitted traffic.

capture stop

Use the command **capture stop** to manually stop capturing CPU packets for packet trace.

Format `capture stop`
Mode Privileged EXEC

capture file|remote|line

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format `capture {file|remote|line}`
Mode Global Config

Parameter	*Description*
file	In the capture file mode, the captured packets are stored in a file on NVRAM. The maximum file size defaults to 524288 bytes. The switch can transfer the file to a TFTP server via TFTP, SFTP, SCP via CLI, and SNMP. The file is formatted in pcap format, is named cpuPktCapture.pcap, and can be examined using network analyzer tools such as Wireshark® or Ethereal®. Starting a file capture automatically terminates any remote capture sessions and line capturing. After the packet capture is activated, the capture proceeds until the capture file reaches its maximum size, or until the capture is stopped manually using the CLI command **capture stop**.
remote	In the remote capture mode, the captured packets are redirected in real time to an external PC running the Wireshark tool for Microsoft® Windows®. A packet capture server runs on the switch side and sends the captured packets via a TCP connection to the Wireshark tool. The remote capture can be enabled or disabled using the CLI. There should be a Windows PC with the Wireshark tool to display the captured file. When using the remote capture mode, the switch does not store any captured data locally on its file system. You can configure the IP port number for connecting Wireshark to the switch. The default port number is 2002. If a firewall is installed between the Wireshark PC and the switch, then these ports must be allowed to pass through the firewall. You must configure the firewall to allow the Wireshark PC to initiate TCP connections to the switch. If the client successfully connects to the switch, the CPU packets are sent to the client PC, then Wireshark receives the packets and displays them. This continues until the session is terminated by either end. Starting a remote capture session automatically terminates the file capture and line capturing.
line	In the capture line mode, the captured packets are saved into the RAM and can be displayed on the CLI. Starting a line capture automatically terminates any remote capture session and capturing into a file. There is a maximum 128 packets of maximum 128 bytes that can be captured and displayed in Line mode.

capture remote port

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *id* parameter is a TCP port number from 1024– 49151.

Format `capture remote port id`

Mode Global Config

capture file size

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *max-file-size* parameter is the maximum size the pcap file can reach, which is 2–512 KB.

Format `capture file size max file size`

Mode Global Config

capture line wrap

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity.

Format `capture line wrap`
Mode Global Config

no capture line wrap

This command disables wrapping of captured packets and configures capture packet to stop when the captured packet capacity is full.

Format `no capture line wrap`
Mode Global Config

show capture packets

Use this command to display packets captured and saved to RAM. It is possible to capture and save into RAM, packets that are received or transmitted through the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Format `show capture packets`
Mode Privileged EXEC

cpu-traffic direction interface

Use this command to associate CPU filters to an interface or list of interfaces. The interfaces can be a physical or logical LAG. The statistics counters are updated only for the configured interfaces. The traces can also be obtained for the configured interfaces.

Note: The offset should consider the VLAN tag headers as the packet to the CPU is always a tagged packet.

Default None
Format `cpu-traffic direction {tx|rx|both} interface` *`interface-range`*
Mode Global Config

no cpu-traffic direction interface

Use this command to remove all interfaces from the CPU filters.

Format `no cpu-traffic direction {tx|rx|both} interface interface-range`

Mode Global Config

cpu-traffic direction match cust-filter

Use this command to configure a custom filter. The statistics and/or traces for configured filters are obtained for the packet matching configured data at the specific offset. If the mask is not specified then the default mask is 0xFF. There can be three different offsets specified as match conditions. Each time a custom filter is configured, the switch overrides the previous configuration.

Note: The offset should consider the VLAN tag headers as the packet to the CPU is always a tagged packet.

Default None

Format `cpu-traffic direction {tx|rx|both} match cust-filter offset1 data1 [mask1 mask1] offset2 data2 [mask2 mask2] offset3 data3 [mask3 mask3]`

Mode Global Config

no cpu-traffic direction match cust-filter

Use this command to remove the configured custom filter.

Format `no cpu-traffic direction {tx|rx|both} match cust-filter offset1 data1 [mask1 mask1] offset2 data2 [mask2 mask2] offset3 data3 [mask3 mask3]`

Mode Global Config

cpu-traffic direction match srcip

Use this command to configure the source IP address-specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured source IP/Mask.

Default None

Format `cpu-traffic direction {tx|rx|both} match srcip ipaddress [mask mask]`

Mode Global Config

no cpu-traffic direction match srcip

Use this command to disable the configured source IP address filter.

Format `no cpu-traffic direction {tx|rx|both} match srcip ipaddress [mask mask]`

Mode Global Config

cpu-traffic direction match dstip

Use this command to configure the destination IP address-specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured destination IP/Mask.

Default None

Format `cpu-traffic direction {tx|rx|both} match dstip ipaddress [mask mask]`

Mode Global Config

no cpu-traffic direction match dstip

Use this command to disable the configured destination IP address filter.

Format `no cpu-traffic direction {tx|rx|both} match dstip ipaddress [mask mask]`

Mode Global Config

cpu-traffic direction match tcp

Use this command to configure the source or destination TCP port-specific filter. The statistics and/or traces for configured filters are obtained for the packet matching configured source/destination TCP port.

Default None

Format `cpu-traffic direction {tx|rx|both} match {srctcp|dsttcp} port [mask mask]`

Mode Global Config

no cpu-traffic direction match tcp

Use this command to remove the configured source/destination TCP port filter.

Format `no cpu-traffic direction {tx|rx|both} match {srctcp|dsttcp} port [mask mask]`

Mode Global Config

cpu-traffic direction match udp

Use this command to configure the source or destination UDP port-specific filter. The statistics and/or traces for configured filters are obtained for the packet matching configured source/destination UDP port.

Default None

Format `cpu-traffic direction {tx|rx|both} match {srcudp|dstudp} port [mask mask]`

Mode Global Config

no cpu-traffic direction match udp

Use this command to remove the configured source/destination UDP port filter.

Format `no cpu-traffic direction {tx|rx|both} match {srcudp|dstudp} port [mask mask]`
Mode Global Config

cpu-traffic mode

Use this command to configure CPU-traffic mode. The packets in the RX/TX direction are matched when the mode is enabled.

Default Disabled
Format `cpu-traffic mode`
Mode Global Config

no cpu-traffic mode

Use this command to disable CPU-traffic mode.

Format `no cpu-traffic mode`
Mode Global Config

cpu-traffic trace

Use this command to configure CPU packet tracing. The packet can be received by multiple components. If the feature is enabled and tracing configured, the packets are traced per the defined filter. If dump-pkt is enabled, the first 64 bytes of the packet are displayed along wtih the trace statistics.

Default Disabled
Format `cpu-traffic trace {dump-pkt}`
Mode Global Config

no cpu-traffic trace

Use this command to disable CPU packet tracing and dump-pkt (if configured).

Format `no cpu-traffic trace {dump-pkt}`
Mode Global Config

show cpu-traffic

Use this command to display the current configuration parameters.

Default None

Format `show cpu-traffic`

Mode Privileged EXEC

Example:

```
(Routing) #show cpu-traffic

Admin Mode..................................... Disable
Packet Trace................................... Disable
Packet Dump.................................... Disable

Direction TX:
Filter Options................................. N/A
Interface...................................... N/A
Src TCP parameters............................. 0 0
Dst TCP parameters............................. 0 0
Src UDP parameters............................. 0 0
Dst UDP parameters............................. 0 0
Src IP parameters.............................. 0.0.0.0 0.0.0.0
Dst IP parameters.............................. 0.0.0.0 0.0.0.0
Src MAC parameters............................. 00:00:00:00:00:00 00:00:00:00:00:00
Dst MAC parameters............................. 00:00:00:00:00:00 00:00:00:00:00:00
Custom filter parameters1...................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters2...................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters3...................... Offset=0x0 Value=0x0 Mask=0x0

Direction RX:
Filter Options................................. N/A
Interface...................................... N/A
Src TCP parameters............................. 0 0
Dst TCP parameters............................. 0 0
Src UDP parameters............................. 0 0
Dst UDP parameters............................. 0 0
Src IP parameters.............................. 0.0.0.0 0.0.0.0
Dst IP parameters.............................. 0.0.0.0 0.0.0.0
Src MAC parameters............................. 00:00:00:00:00:00 00:00:00:00:00:00
Dst MAC parameters............................. 00:00:00:00:00:00 00:00:00:00:00:00
Custom filter parameters1...................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters2...................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters3...................... Offset=0x0 Value=0x0 Mask=0x0
```

show cpu-traffic interface

Use this command to display per interface statistics for configured filters. The statistics can be displayed for a specific filter (e.g., stp, udld, arp etc). If no filter is specified, statistics are displayed for all configured filters. Similarly, source/destination IP, TCP, UDP or MAC along with custom filter can be used as command option to get statistics.

Default None

Format `show cpu-traffic interface {all | slot/port | cpu } filter`

Mode Privileged EXEC

show cpu-traffic summary

Use this command to display summary statistics for configured filters for all interfaces.

Default None

Format `show cpu-traffic summary`

Mode Privileged EXEC

Example:

```
(Routing) #show cpu-traffic summary

Filter       Received   Transmitted
------------ ---------- -----------
STP          0          0
LACPDU       0          0
ARP          0          0
UDLD         0          0
LLDP         0          0
IP           0          0
OSPF         0          0
BGP          0          0
DHCP         0          0
BCAST        0          0
MCAST        0          0
UCAST        0          0
SRCIP        0          0
DSTIP        0          0
SRCMAC       0          0
DSTMAC       0          0
CUSTOM       0          0
SRCTCP       0          0
DSTTCP       0          0
SRCUDP       0          0
```

show cpu-traffic trace

Use this command to display traced information. The trace information can be displayed either for all available packets or for specific filter (e.g., stp, udld, arp etc). Similarly, source/destination IP or MAC along with custom filter can be used as command option to get specific traces from history. If enabled, packet dump information is displayed along with packet trace statistics. By default, packet dump buffer size is set to store first 64 bytes of packet.

Default None

Format `show cpu-traffic trace` *`filter`*

Mode Privileged EXEC

Example:

```
(Routing) #show cpu-traffic summary
Packet #1: IP; DHCP; UCAST; SRCMAC=00:10:10:10:10:10;
<08:06:10> Sysnet received in sysNetNotifyPduReceive()
```

```
<08:06:10> Packet delivered to IP via ipMapRecvIP()
<08:06:10> Freed
0000 00 10 18 82 18 b3 00 10 10 10 10 10 81 00 00 01    ................
0010 08 00 45 10 01 21 00 00 00 00 40 11 79 bd 00 00    ..E..!....@.y...
0020 00 00 ff ff ff ff 00 44 00 43 01 0d 48 10 03 01    .......D.C..H...
0030 06 00 18 85 4a 83 00 00 80 00 00 00 00 00 00 00    ....J...........
```

clear cpu-traffic

Use this command to clear cpu-traffic statistics or trace information on all interfaces.

Default None

Format `clear cpu-traffic {counters | traces}`

Mode Global Config

debug arp

Use this command to enable ARP debug protocol messages. Optionally, a virtual router can be specified in which to execute the command.

Default disabled

Format `debug arp [vrf vrf-name]`

Mode Privileged EXEC

no debug arp

Use this command to disable ARP debug protocol messages.

Format `no debug arp`

Mode Privileged EXEC

debug auto-voip

Use this command to enable Auto VOIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Default disabled

Format `debug auto-voip [H323|SCCP|SIP|oui]`

Mode Privileged EXEC

no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format `no debug auto-voip`

Mode Privileged EXEC

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.

Note: The debug console command is used to direct debug data to a login session. The severity level of messages appearing in the session is still decided by the console logging severity filter specified with the `logging console` command.

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 crashlog

Use this command to view information contained in the crash log file that the system maintains when it experiences an unexpected reset. The crash log file contains the following information:

- Call stack information in both primitive and verbose forms
- Log Status
- Buffered logging
- Event logging
- Persistent logging
- System Information (output of sysapiMbufDump)
- Message Queue Debug Information
- Memory Debug Information
- Memory Debug Status
- OS Information (output of osapiShowTasks)
- /proc information (meminfo, cpuinfo, interrupts, version and net/sockstat)

Default disabled

Format `debug crashlog {[kernel] crashlog-number [upload url] | proc | verbose | deleteall}`

Mode Privileged EXEC

Parameter	*Description*
kernel	View the crash log file for the kernel
crashlog-number	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4.”deb
upload *url*	To upload the crash log (or crash dump) to a TFTP server, use the `upload` keyword and specify the required TFTP server information.
proc	View the application process crashlog.
verbose	Enable the verbose crashlog.
deleteall	Delete all crash log files on the system.
data	Crash log data recorder.
crashdump-number	Specifies the crash dump number to view. The valid range is 0–2.
download *url*	To download a crash dump to the switch, use the `download` keyword and specify the required TFTP server information.
component-id	The ID of the component that caused the crash.
item-number	The item number.
additional-parameter	Additional parameters to include.

debug crashlog kernel

Use this command to display the dmesg log from the specified kdump slot.

Default disabled

Format `debug crashlog kernel crashlog-number`
Mode Privileged EXEC

debug crashlog kernel upload

Use this command to upload the specified kernel dump to the TFTP server.

Default disabled
Format `debug crashlog kernel crashlog-number upload tftpaddress`
Mode Privileged EXEC

debug dcbx packet

Use this command to enable debug tracing for DCBX packets that are transmitted or received.

Default disabled
Format `debug dcbx packet {receive | transmit}`
Mode Privileged EXEC

debug debug-config

Use this command to download or upload the debug-config.ini file. The debug-config. ini file executes CLI commands (including devshell and drivshell commands) on specific predefined events. The debug config file is created manually and downloaded to the switch.

Default disabled
Format `debug debug-config {download <url> | upload <url>}`
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

This command disables the display of “debug” trace output for DHCPv4 client activity.

Format `no debug dhcp packet [transmit | receive]`

Mode Privileged EXEC

debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default disabled

Format `debug lacp packet`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %%
 Pkt TX - Intf: slot/port(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key:
0x36
```

no debug lacp packet

This command disables tracing of LACP packets.

Format `no debug lacp packet`

Mode Privileged EXEC

debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/ service port for switching packages. For routing packages, pings are traced on the routing ports as well. If specified, pings can be traced on the virtual router.

Default disabled

Format `debug ping packet [vrf vrf-name]`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128) 20 % Pkt TX - Intf: 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: 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:

Parameter	*Definition*
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. Format used is slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
SRC_IP	The source IP address in the IP header in the packet.

Parameter	*Definition*
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 bpdu

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

Default disabled
Format `debug spanning-tree bpdu`
Mode Privileged EXEC

no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format `no debug spanning-tree bpdu`
Mode Privileged EXEC

debug spanning-tree bpdu receive

This command enables tracing of spanning tree BPDUs received by the switch. 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 bpdu receive`
Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX - Intf: 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:

Parameter	*Definition*
RX	A packet received by the device.

Parameter	*Definition*
Intf	The interface that the packet came in on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	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. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default disabled

Format `debug spanning-tree bpdu transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt TX - Intf: 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:

Parameter	*Definition*
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	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 transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format `no debug spanning-tree bpdu transmit`
Mode Privileged EXEC

debug telnetd start

Use this command to start the debug telnet daemon. The debug telnet daemon gives access to a Linux shell prompt. The telnet user ID is “root”. If the telnet daemon is already running when this command is issued, the command stops and restarts the telnet daemon.

Format `debug telnetd start [password][port]`
Mode Privileged EXEC

Parameter	*Description*
password	The optional telnet password. If no password is specified, the default password lvl7dbg is used.
port	The optional telnet port number. If no telnet port is specified, the default port 2323 is used.

debug telnetd stop

Use this command to stop the telnet daemon previously started by the debug telnetd start command. If the daemon is not running when this command is issued, the command has no effect.

Format `debug telnetd stop`
Mode Privileged EXEC

debug transfer

This command enables debugging for file transfers.

Format `debug transfer`
Mode Privileged EXEC

no debug transfer

This command disables debugging for file transfers.

Format `no debug transfer`
Mode Privileged EXEC

debug udld events

This command enables debugging for the UDLD events.

Default `Disabled`
Format `debug udld events`
Mode Privileged EXEC

debug udld packet receive

This command enables debugging on the received UDLD PDUs.

Default `Disabled`
Format `debug udld packet receive`
Mode Privileged EXEC

debug udld packet transmit

This command enables debugging on the transmitted UDLD PDUs.

Default `Disabled`
Format `debug udld packet transmit`
Mode Privileged EXEC

show debugging

Use the `show debugging` command to display enabled packet tracing configurations.

Format `show debugging`
Mode Privileged EXEC

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

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

(Routing)# show debugging
Arp packet tracing enabled.\
```

exception core-file

Use this command to configure a prefix for a core-file name. The core file name is generated with the prefix as follows:

If `hostname` is selected:
`file-name-prefix_hostname_Time_Stamp``.bin`

If `hostname` is not selected:
`file-name-prefix_MAC_Address_Time_Stamp``.bin`

If `hostname` is configured the core file name takes the `hostname`, otherwise the core-file names uses the MAC address when generating a core dump file. The prefix length is 15 characters.

Note: This command is only available on selected Linux-based platforms.

Default	Core
Format	`exception core-file {`*`file-name-prefix`* `| [hostname] | [time-stamp]}`
Mode	Global Config

no exception core-file

Use this command to reset the exception core file prefix configuration to its factory default value. The hostname and time-stamp are disabled.

Note: This command is only available on selected Linux-based platforms.

Default	Core
Format	`no exception core-file`
Mode	Global Config

exception dump active-port

Note: This command is only available on selected Linux- based platforms.

This command specifies the interface enabled for the core dump. It is the only port used to upload the core dump.

Default	None
Format	`exception dump active-port` *`slot/port`*
Mode	Global Config

no exception dump active-port

This command resets the interface enabled for the core dump to the default.

Default None
Format `no exception dump active-port`
Mode Global Config

exception dump filepath

Use this command to configure a file-path to dump core file to a TFTP or FTP server, NFS mount or USB device subdirectory.

Note: This command is only available on selected Linux-based platforms.

Default None
Format `exception dump filepath` *`dir`*
Mode Global Config

no exception dump filepath

Use this command to reset the exception dump filepath configuration to its factory default value.

Note: This command is only available on selected Linux-based platforms.

Default None
Format `exception dump  filepath`
Mode Global Config

exception dump nfs

Use this command to configure an NFS mount point in order to dump core file to the NFS file system.

Note: This command is only available on selected Linux-based platforms.

Default None
Format `exception dump nfs` *`ip-address/dir`*
Mode Global Config

no exception dump nfs

Use this command to reset the exception dump NFS mount point configuration to its factory default value.

Note: This command is only available on selected Linux-based platforms.

Default	None
Format	`no exception dump nfs`
Mode	Global Config

exception dump tftp-server

Use this command to configure the IP address of a remote TFTP server in order to dump core files to an external server.

Note: This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump tftp-server {`*`ip-address`*`}`
Mode	Global Config

no exception dump tftp-server

Use this command to reset the exception dump remote server configuration to its factory default value.

Note: This command is only available on selected Linux-based platforms.

Default	None
Format	`no exception dump tftp-server`
Mode	Global Config

exception kernel-dump

Use this command to enable kernel crash core dump (kdump) functionality. This command requires reboot if the command was not enabled since the last reboot.

Default None
Format `exception kernel-dump`
Mode Global Config

no exception kernel-dump

Use this command to disable kernel crash core dump (kdump) functionality. If a crash log number is specified, the specified slot is deleted.

Default None
Format `no exception kernel-dump` *`crashlog-number`*
Mode Global Config

exception kernel-dump path

Use this command to set the path where the kernel crash core dump (kdump) entries are stored.

Default None
Format `exception kernel-dump path` *`path`*
Mode Global Config

no exception kernel-dump path

Use this command to return the path where the kernel crash core dump (kdump) entries are stored to the default value.

Default None
Format `no exception kernel-dump path`
Mode Global Config

exception protocol

Use this command to specify the protocol used to store the core dump file.

Note: This command is only available on selected Linux-based platforms.

Default None
Format `exception protocol {nfs | tftp | ftp | local | usb | none}`
Mode Global Config

no exception protocol

Use this command to reset the exception protocol configuration to its factory default value.

Note: This command is only available on selected Linux-based platforms.

exception switch-chip-register

This command enables or disables the switch-chip-register dump in case of an exception. The switch-chip-register dump is taken only for a master unit and not for member units

Note: This command is only available on selected Linux-based platforms.

Default	Disable
Format	`exception switch-chip-register {enable | disable}`
Mode	Global Config

exception dump ftp-server

This command configures the IP address of remote FTP server to dump core files to an external server. If the username and password are not configured, the switch uses anonymous FTP. (The FTP server should be configured to accept anonymous FTP.)

Default	None
Format	`exception dump ftp-server` *`ip-address`* `[{username` *`user-name`* `password` *`password`*`}]`
Mode	Global Config

no exception dump ftp-server

This command resets exception dump remote FTP server configuration to its factory default value. This command also resets the FTP username and password to empty string.

Default	None
Format	`no exception dump ftp-server`
Mode	Global Config

exception dump compression

This command enables compression mode.

Default Enabled
Format `exception dump compression`
Mode Global Config

no exception dump compression

This command disables compression mode.

Default None
Format `no exception compression`
Mode Global Config

exception nmi

This command enables or disables taking core dump in case of NMI occurs.

Default Disable
Format `exception nmi {enable | disable}`
Mode Global Config

show exception kernel-dump

Use this command to display the current kernel dump settings and slots available to view.

Format `show exception kernel-dump`
Mode Privileged Exec

show exception kernel-dump list

Use this command to display the currently captured dumps.

Format `show exception kernel-dump list`
Mode Privileged Exec

show exception kernel-dump log

Use this command to display the dmesg log from a specified kdump slot.

Format `show exception kernel-dump log` *`crashlog-number`*
Mode Privileged Exec

mbuf

Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format `mbuf {falling-threshold | rising threshold | severity}`

Mode Global Config

Field	*Description*
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level at which Mbuf logs messages. The range is 1 to 7. The default is 5 (L7_LOG_SEVERITY_NOTICE).

write core

Use the *write core* command to generate a core dump file on demand. The `write core test` command is helpful when testing the core dump setup. For example, if the TFTP protocol is configured, `write core test` communicates with the TFTP server and informs the user if the TFTP server can be contacted. Similarly, if protocol is configured as `nfs`, this command mounts and unmounts the file system and informs the user of the status.

Note: `write core` reloads the switch which is useful when the device malfunctions, but has not crashed.

For the `write core test` command, the destination file name is used for the TFTP test. Optionally, you can specify the destination file name when the protocol is configured as TFTP.

Note: This command is only available on selected Linux-based platforms.

Default None

Format `write core [test [dest_file_name]]`

Mode Privileged EXEC

debug exception

The command displays core dump features support.

Default None
Format `debug exception`
Mode Privileged EXEC

show exception

Use this command to display the configuration parameters for generating a core dump file.

Note: This command is only available on selected Linux-based platforms.

Default None
Format `show exception`
Mode Privileged EXEC

Example: The following shows an example of this command.

```
show exception

Coredump file name                core
Coredump filename uses hostname   False
Coredump filename uses time-stamp TRUE
TFTP Server Address               TFTP server configuration
FTP Server IP                     FTP server configuration
FTP user name                     FTP user name
FTP password                      FTP password
NFS Mount point                   NFS mount point configuration
File path                         Remote file path
Core File name prefix             Core file prefix configuration.
Hostname                          Core file name contains hostname if enabled.
Timestamp                         Core file name contains timestamp if enabled.
Switch Chip Register Dump         Switch chip register dump configuration
Compression mode                  TRUE/FALSE
Active network port               0/28
```

show exception core-dump-file

This command displays core dump files existing on the local file system.

Default None
Format `show exception core-dump-file`
Mode Privileged EXEC, Config Mode

show exception log

This command displays core dump traces on the local file system.

Default None
Format `show exception log [previous]`
Mode Privileged EXEC, Config Mode

show mbuf total

Use this command to display the memory buffer (MBUF) Utilization Monitoring parameters.

Format `show mbuf total`
Mode Privileged EXEC

Field	*Description*
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level.

show msg-queue

Use this command to display the message queues.

Default None
Format `show msg-queue`
Mode Priveleged EXEC mode

debug packet-trace

Use this command to enable traces for the packet trace feature.

Default None
Format `debug packet-trace`
Mode Privileged Exec

packet-trace eth

Use this command to specify the ethernet packet fields for a packets for which a trace profile is required. If the optional vlan parameter is not specified, the PVID/internal VLAN associated with the ingress port (specified in the show packet-trace command) is used in the VLAN tag.

Default	None
Format	`packet-trace eth src-mac` *`src-mac`* `dst-mac` *`dst-mac`* `vlan` *`vlan`*
Mode	Privileged Exec

packet-trace ipv4

Use this command to specify the IPv4 packet header fields.

Default	None
Format	`packet-trace ipv4 src-ip` *`src-ip`* `dst-ip` *`dst-ip`* `tos` *`tos`*
Mode	Privileged Exec

packet-trace l4

Use this command to specify TCP packet fields.

Default	None
Format	`packet-trace l4 src-port` *`src-port`* `dst-port` *`dst-port`*
Mode	Privileged Exec

show packet-trace ecmp

Use this command for getting a summary (link utilization percentage) for all complete packets present in the PCAP file (uploaded onto the system using the copy command).

Default	None
Format	`show packet-trace ecmp` *`prefix/prefix-length`* `port` *`slot/port`* `pcap summary`
Mode	Privileged Exec

show packet-trace lag

Use this command for getting a summary (link utilization percentage) for all complete packets present in the PCAP file (uploaded onto the system using the copy command).

Default	None
Format	`show packet-trace lag` *`lag-id`* `port` *`slot/port`* `pcap summary`
Mode	Privileged Exec

Example:

```
(Routing)#show packet-trace lag 1 port 0/1 pcap summary

LAG   ............................... 3/1
Link State..................................... Up
```

```
Admin Mode..................................... Enabled
Type........................................... Static
Port-channel Min-links......................... 1
Load Balance Option............................ 3
(Src/Dest MAC, VLAN, EType, incoming port)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/3   actor/long    10G Full  True
        partner/long
0/2   actor/long    10G Full  True
        partner/long

LAG 1 member port link utilization %:
-------------------------------------
Total number of valid packets in pcap file: 20
Member port 0/3 utilization: 20%
Member port 0/4 utilization: 80%
```

show packet-trace packet-data

Use this command to dump all the configured packet header fields.

Default By default, all packet fields are set to 0.

Format `show packet-trace trace-data`

Mode Privileged Exec

Example:

```
DUT#show packet-trace packet-data

L2 Header fields:
-----------------------
Src MAC: 00 00 00 0a 0b 0c
Dst MAC: 00 00 00 0d 0e 0f
VLAN: 10

L3 Header fields:
-------------------------
IPv4:
Src IP: 10.0.10.1
Dst IP: 10.0.10.10
TOS: 0

IPv6:
Src IP: 4001::1/8
Dst IP: 5001::1/8
Traffic Class: 0

L4 header fields:
-----------------------
Src Port: 80
Dst Port: 80
```

show packet-trace port

Use this command for getting detailed information for the maximum packets in the PCAP file.

Default None

Format `show packet-trace port slot/port pcap detailed maxpkts`

Mode Privileged Exec

Example:

```
DUT#show packet-trace port 0/1 pcap detailed 5

            Packet fields:
src-Mac      --------------     00:00:00:00:00:0a
dst-mac      --------------     00:00:00:00:00:0b
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG                Destination member port
---------         ---------------------------------
Lag 1                     0/4


Packet fields:
src-Mac      --------------     00:00:00:00:00:0c
dst-mac      --------------     00:00:00:00:00:0d
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG                Destination member port
---------         ---------------------------------
Lag 1                     0/3


Packet fields:
src-Mac      --------------     00:00:00:00:00:0e
dst-mac      --------------     00:00:00:00:00:0f
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG                Destination member port
---------         ---------------------------------
Lag 1                     0/2

Packet fields:
src-Mac      --------------     00:00:00:00:00:1a
dst-mac      --------------     00:00:00:00:00:1b
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG                Destination member port
```

```
---------         ---------------------------------
Lag 1                     0/4

Packet fields:
src-Mac      --------------     00:00:00:00:00:1c
dst-mac      --------------     00:00:00:00:00:1d
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG               Destination member port
---------         ---------------------------------
Lag 1                     0/3
```

show packet-trace port eth

Use this command to retrieve the trace profile for an ethernet packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information.

Default None

Format `show packet-trace port slot/port eth`

Mode Privileged Exec

Example:

```
(Routing)# show packet-trace port 0/1 eth

LAG               Destination member port
---------         ---------------------------------
Lag 1                              0/3

LAG   ............................... 3/1
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Port-channel Min-links......................... 1
Load Balance Option............................ 3
(Src/Dest MAC, VLAN, EType, incoming port)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/3   actor/long    10G Full  True
        partner/long
0/2   actor/long    10G Full  True
        partner/long
```

show packet-trace port ipv4

Use this command to retrieve the trace profile for an IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for an IP packet, both the Ethernet and IP packet fields need to be configured.

Default None

Format `show packet-trace port slot/port ipv4`

Mode Privileged Exec

Example:

```
(Routing)# show packet-trace port 0/1 ipv4
ECMP               Egress port            Next Hop IP
-----------      ----------------         -----------------
10.0.0.2/16             0/4                 3.3.3.3

ECMP routes to 10.0.0.2/16:
-------------------------------
via 3.3.3.3 on interface 0/4
via 2.2.2.2 on interface 0/5
```

show packet-trace port tcpv4

Use this command to retrieve the trace profile for a TCP-IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also corresponding member/link information. Note that in order to get the trace profile for a TCP packet, the ethernet, IP and L4 packet fields need to be configured.

Default None

Format `show packet-trace port slot/port tcpv4`

Mode Privileged Exec

show packet-trace port udpv4

Use this command to retrieve the trace profile for a UDP-IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for a UDP packet, the ethernet, IP and L4 packet fields need to be configured.

Default None

Format `show packet-trace port slot/port udpv4`

Mode Privileged Exec

clear packet-trace packet-data

Use this command to clear the configured packet header fields.

Format `clear packet-trace packet-data`
Mode Privileged Exec

watchdog clear

This command clears the watchdog settings and history and resets the timeout interval to the default value.

Format `watchdog clear`
Mode Privileged EXEC

watchdog disable

This command disables watchdog services. Watchdog is automatically changed (that is, no reboot is required).

Default Disabled
Format `watchdog disable`
Mode Privileged EXEC

watchdog enable

This command enables watchdog services. Watchdog services give DCSS the ability to recover when it is no longer executing properly. When a recovery is attempted, debug information is saved and the switch is reset.

Default Disabled
Format `watchdog enable`
Mode Privileged EXEC

Cable Test Command

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.

If the port has an active link while the cable test is run, the link can go down for the duration of the test.

cablestatus

This command returns the status of the specified port.

Format `cablestatus` *`slot/port`*

Mode Privileged EXEC

Parameter	*Description*
Cable Status	One of the following statuses is returned: • **Normal**: The cable is working correctly. • **Open**: The cable is disconnected or there is a faulty connector. • **Short**: There is an electrical short in the cable. • **Cable Test Failed**: The cable status could not be determined. The cable may in fact be working. • **Crosstalk:** There is crosstalk present on the cable. • **No Cable:** There is no cable present.
Cable Length	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.

Port Locator Commands

The port locator commands identify ports that have network cabling errors and/or cabling complications (mis-wiring) by providing a command that blinks a single interface's LED or the LEDs of multiple interfaces and turns off all other interface LEDs so that the mis-wired interface can be easily identified. The LEDs blink at the rate of one second on and one second off. The LED of interfaces that are linked up will have their LEDs solidly lit only if port locator is not enabled on that interface. Traffic present on any interface will not cause the LED to blink to indicate traffic. A port–locator enabled interface will blink and not light solid if the link is up. In other words, port locator has precedence over link status.

If an interface has two LEDs, one for link and a second for activity, only the link LED is used for the port locator function. The activity LED is turned off while the port locator feature is active. If an interface has one LED for link and activity, the LED will not blink if activity is present on the interface while the port locator feature is active.

Out-of-band port LEDs are not affected by this feature. This feature is configurable on physical ports, LAGs, diagnostically disabled ports, and pluggable module ports.

port-locator disable

This command globally disables the port locator function and restores all port LEDs to normal operation.

Format `port-locator disable`

Mode
- Privileged EXEC
- Interface Config

Example:

```
(Routing)(Config)# port-locator disable
```

port-locator enable

This command turns on the LED for the interface or interfaces.

Format `port-locator enable`

Mode Interface Config

Example:

```
(Routing)(Interface 0/1,0/3,0/5,0/7)#port-locator enable

(Routing)(Interface 0/54,0/55,0/56,0/57)#port-locator enable

Error! Interface 0/55  is in Detach state
Error! Interface 0/56  is in Detach state
Error! Interface 0/57  is in Detach state
```

show port- locator

This command displays which port or ports currently have locator mode enabled. LAG interfaces are also displayed if port-locator was enabled on a LAG.

Format `show port-locator`

Mode Privileged EXEC

Example:

```
(Routing)#show port-locator

          Locator
Intf      Mode
--------- --------
0/1       Enable
0/2       Disable
0/3       Enable
0/4       Disable
0/5       Enable
0/6       Disable
0/7       Enable
0/8       Disable
0/9       Enable
```

Example: Below interface 3/1 is a LAG interface, members are 0/1 and 0/45.

```
(Routing)#show port-locator  | include enable

0/1       enable
0/45      enable
3/1       enable
```

SFP Transceiver Commands

These commands show details for the SFP transceivers. Transceivers that are compliant with the SFF-8472(SFP+) and SFF-8436(QSFP+) standards are supported.

show fiber-ports optical-transceiver

This command displays the diagnostic information of the SFP. The values are derived from the SFP's A2 (Diagnostics) table using the I2c interface.

Format `show fiber-ports optical-transceiver {all|`*`slot/port`*`}`

Mode Privileged EXEC

Parameter	*Description*
Temp	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured optical output power relative to 1mW.
Input Power	Measured optical power received relative to 1mW.
TX Fault	Transmitter fault.
LOS	Loss of signal.

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

```
(Routing) #show fiber-ports optical-transceiver all

                                    Output    Input
Port      Temp  Voltage  Current     Power    Power   TX     LOS
           [C]   [Volt]     [mA]     [dBm]    [dBm]   Fault
--------  ----  -------  -------   -------  -------   -----  ---
0/49      39.3    3.256      5.0    -2.234   -2.465   No     No
0/50      33.9    3.260      5.3    -2.374  -40.000   No     Yes
0/51      32.2    3.256      5.6    -2.300   -2.897   No     No


(Routing) #show fiber-ports optical-transceiver 0/49

                                    Output    Input
Port      Temp  Voltage  Current     Power    Power   TX     LOS
           [C]   [Volt]     [mA]     [dBm]    [dBm]   Fault
--------  ----  -------  -------   -------  -------   -----  ---
0/49      39.3    3.256      5.0    -2.234   -2.465   No     No
```

show fiber-ports optical-transceiver-info

This command displays the SFP vendor-related information. The values are derived from the SFP's A0 table using the I2c interface.

Format `show fiber-ports optical-transceiver-info {all|slot/port}`

Mode Privileged EXEC

Parameter	*Description*
Vendor Name	The vendor name is the full name of the corporation, an abbreviation for the name of the corporation, the SCSI company code for the corporation, or the stock exchange symbol for the corporation. The name is 1 to 16 ASCII characters in length.
Link Length 50um	This value specifies the link length that is supported by the transceiver while operating in compliance with applicable standards using 50 micron multimode OM2 [500 MHz * km at 850nm] fiber. A value of zero means that the transceiver does not support 50 micron multimode fiber or that the length information must be determined from the transceiver technology.
Link Length 62.5um	This value specifies the link length that is supported by the transceiver while operating in compliance with applicable standards using 62.5 micron multimode OM1 [200 MHz * km at 850nm, 500 MHz * km at 1310nm] fiber. A value of zero means that the transceiver does not support 62.5 micron multimode fiber or that the length information must be determined from the transceiver technology.
Serial Number	The vendor serial number for the transceiver. The serial number is 1 to 16 ASCII characters in length. A value of all zeros in the field indicates that the vendor serial number is unspecified.
Part Number	The vendor part number or product name. A value of all zeros in the 16-byte field indicates that the vendor part number is unspecified.
Nominal Bit Rate	The nominal bit (signaling) rate, specified in units of 100 MBd, rounded off to the nearest 100 MBd. The bit rate includes those bits necessary to encode and delimit the signal, as well as those bits carrying data information. A value of zero indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate depends on the encoding of the data, as defined by the encoding value.
Rev	The vendor's product revision number. A blank value in this field indicates that the vendor revision is unspecified.

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

```
(Switching) #show fiber-ports optical-transceiver-info all

                        Link Link                                  Nominal
                      Length Length                                    Bit
                        50um 62.5um                                  Rate
Port     Vendor Name     [m] [m]  Serial Number    Part Number     [Mbps] Rev
-------- --------------- --- ---- ---------------- ---------------- ------ ----
0/49     NETGEAR           8    3 A7N2018414       AXM761            10300 10
0/51     NETGEAR           8    3 A7N2018472       AXM761            10300 10
0/52     NETGEAR           8    3 A7N2018501       AXM761            10300 10


(Switching) #show fiber-ports optical-transceiver-info 0/49

                        Link Link                                  Nominal
                      Length Length                                    Bit
                        50um 62.5um                                  Rate
Port     Vendor Name     [m] [m]  Serial Number    Part Number     [Mbps] Rev
-------- --------------- --- ---- ---------------- ---------------- ------ ----
0/49     NETGEAR           8    3 A7N2018414       AXM761            10300 10
```

Section 7: Switching Commands

This section describes the following switching commands available in the DCSS CLI:

Note: 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.

Port Configuration Commands

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(startrange)-slot/port(endrange)}`

Mode Global Config

Example: The following example enters Interface Config mode for port 0/1:

```
(Routing) #configure
(Routing) (config)#interface 0/1
(Routing) (interface 0/1)#
```

Example: The following example enters Interface Config mode for ports 0/1 through 0/4:

```
(Routing)#configure
(Routing) (config)#interface 0/1-0/4
(Routing) (interface 0/1-0/4)#
```

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

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format `description` *`description`*

Mode Interface Config

media-type

Use this command to change between fiber and copper mode on the Combo port.

- Combo Port: A port or an interface that can operate in either copper or in fiber mode.
- Copper and Fiber port: A port that uses copper a medium for communication (for example, RJ45 ports). A fiber port uses the fiber optics as a medium for communication (for example, example SFP ports).

Default Auto-select, SFP preferred

Format `media-type {auto-select | rj45 | sfp }`

Mode Interface Config

The following modes are supported by the `media-type` command.

- Auto-select, SFP preferred: The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the fiber link takes precedence and the fiber link is up.
- Auto-select, RJ45 preferred: The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the copper link takes precedence and the copper link is up.
- SFP: Only the fiber medium works. The copper medium is always down.
- RJ45: Only the copper medium works. The fiber medium is always down.

no media-type

Use this command to revert the `media-type` configuration and configure the default value on the interface.

Format `no media-type`
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 DCSS implementation, the MTU size is a valid integer between 1504–12270 for tagged packets and a valid integer between 1500–12270 for untagged packets.

Note: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see “ip mtu” on page 271.

Default 1500 (untagged)
Format `mtu` *`1500-12270`*
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 `shutdown all`
Mode Global Config

no shutdown all

This command enables all ports.

Format `no shutdown all`
Mode Global Config

speed

Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. The duplex parameter allows you to set the advertised speed for both half as well as full duplex mode.

Use the `auto` keyword to enable auto-negotiation on the port. Use the command without the `auto` keyword to ensure auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is disabled, the speed and duplex mode must be set.

Default Auto-negotiation is enabled.

Format
```
speed auto {10|100|1000|2.5G|10G|20G|25G|40G|50G|100G}
[10|100|1000|2.5G|10G|20G|25G|40G|50G|100G] [half-duplex|full-duplex]

speed {10|100|1000|2.5G|10G|20G|25G|40G|50G|100G} {half-duplex|full-duplex}
```

Mode Interface Config

speed all

This command sets the speed and duplex setting for all interfaces if auto-negotiation is disabled. If auto-negotiation is enabled, an error message is returned. Use the `no auto-negotiate` command to disable.'

Default Auto-negotiation is enabled. Adv. is 10h, 10f, 100h, 100f, 1000f.

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

Mode Global Config

show interface media-type

Use this command to display the media-type configuration of the interface.

Format
```
show interface media-type
```

Mode Privileged EXEC

The following information is displayed for the command.

Term	*Definition*
Port	The slot/port.
Configured Media Type	The media type for the interface. auto-select—The media type is automatically selected. The preferred media type is displayed. RJ45—RJ45 SFP—SFP
Active	Displays the current operational state of the combo port.

Example: The following command shows the command output:

```
(Routing) #show interface media-type
```

```
Port       Configured Media Type        Active
---------  ---------------------------  ------
0/21       SFP                          RJ45
0/22       auto-select, SFP preferred   Down
0/23       auto-select, SFP preferred   RJ45
0/24       auto-select, SFP preferred   Down
```

show port

This command displays port information.

Format `show port {intf-range | all}`

Mode Privileged EXEC

Parameter	*Definition*
Interface	slot/port
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • **Mirror** — this port is a monitoring port. • **PC Mbr**— this port is a member of a port-channel (LAG). • **Probe** — this port is a probe port.
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	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	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.

Example: The following command shows an example of the command output for all ports.

```
(Routing) #show port all

                Admin     Physical   Physical   Link   Link    LACP   Actor
Intf      Type  Mode      Mode       Status     Status Trap    Mode   Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------ --------
0/1             Enable    Auto       100 Full   Up     Enable  Enable long
0/2             Enable    Auto       100 Full   Up     Enable  Enable long
0/3             Enable    Auto                  Down   Enable  Enable long
0/4             Enable    Auto       100 Full   Up     Enable  Enable long
0/5             Enable    Auto       100 Full   Up     Enable  Enable long
0/6             Enable    Auto       100 Full   Up     Enable  Enable long
0/7             Enable    Auto       100 Full   Up     Enable  Enable long
0/8             Enable    Auto       100 Full   Up     Enable  Enable long
1/1             Enable                          Down   Disable N/A    N/A
```

```
1/2             Enable                          Down   Disable N/A    N/A
1/3             Enable                          Down   Disable N/A    N/A
1/4             Enable                          Down   Disable N/A    N/A
1/5             Enable                          Down   Disable N/A    N/A
1/6             Enable                          Down   Disable N/A    N/A
```

Example: The following command shows an example of the command output for a range of ports.

```
(Routing) #show port 0/1-1/6

                Admin     Physical   Physical   Link   Link    LACP   Actor
Intf      Type  Mode      Mode       Status     Status Trap    Mode   Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------ --------
0/1             Enable    Auto       100 Full   Up     Enable  Enable long
0/2             Enable    Auto       100 Full   Up     Enable  Enable long
0/3             Enable    Auto                  Down   Enable  Enable long
0/4             Enable    Auto       100 Full   Up     Enable  Enable long
0/5             Enable    Auto       100 Full   Up     Enable  Enable long
0/6             Enable    Auto       100 Full   Up     Enable  Enable long
0/7             Enable    Auto       100 Full   Up     Enable  Enable long
0/8             Enable    Auto       100 Full   Up     Enable  Enable long
1/1             Enable                          Down   Disable N/A    N/A
1/2             Enable                          Down   Disable N/A    N/A
1/3             Enable                          Down   Disable N/A    N/A
1/4             Enable                          Down   Disable N/A    N/A
1/5             Enable                          Down   Disable N/A    N/A
1/6             Enable                          Down   Disable N/A    N/A
```

show port description

This command displays the interface description.

Format `show port description {slot/port | lag lag-id}`

Mode Privileged EXEC

Parameter	*Definition*
Interface	The slot/port or LAG with the information to view.
ifIndex	The interface index number associated with the port.
Description	The alpha-numeric description of the interface created by the command “description” on page 188.
MAC address	The MAC address of the port. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Bit Offset Val	The bit offset value.

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

```
(Switching) #show port description 0/1

Interface...........0/1
ifIndex.............1
Description.........
MAC address.........00:10:18:82:0C:10
Bit Offset Val......1
```

hardware profile portmode

Use the `hardware profile portmode` command to configure a 40G QSFP port in either 4x10G mode or 1x40G mode. When the command is successfully executed, the following message is displayed on the screen:

```
This command will not take effect until the switch is rebooted.
```

This command can only be executed on the 40G interface. Entering the command on any other type of interface will give an error.

This command will take effect only after rebooting the switch.

Note: This command does not operate in interface range mode.

Default The default mode for QSFP 40G ports on platform BCM956846k_02 is:
- Front panel 40G ports 1–12 are configured in 4x10G mode.
- Front panel 40G ports 13–16 are configured in 1x40G mode.

Format `hardware profile portmode {1x40g | 4x10g}`

Mode Interface Config

Parameter	*Definition*
1x40g	Configure the port as a single 40G port using four lanes.
4x10g	Configure the port as four 10G ports, each on a separate lane. This mode requires the use of a suitable 4x10G to 1x40G pigtail cable.

no hardware profile portmode

Use the no form of the `hardware profile portmode` command to return the port to the 1x40G mode.

Format `no hardware profile portmode`

Mode Interface Config

show interfaces hardware profile

Use the `show interfaces hardware profile` command in Privileged EXEC mode to display the hardware profile information for the 40G ports. The command displays the 40G interface and the corresponding 10G interfaces. Because any hardware profile configuration is only effective with the next boot of the switch, the configured mode may be different than the operational mode of the interface. Therefore, this command also displays the configured mode and the operational mode of the interface.

The user can optionally specify an interface or all 40G interfaces to display.

Format `show interfaces hardware profile [interface]`

Mode Privileged EXEC

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

Note: The port mappings can vary from platform to platform. This example is only for illustration, and may not represent the actual port mappings on all platforms.

```
(Routing) #show interfaces hardware profile

                                Configured  Oper
40G Interface  10G Interfaces   Mode        Mode
-------------  --------------  ----------  -------
0/1            0/17-20         1x40G       4x10G
0/2            0/21-24         1x40G       1x40G


(Routing) #show interfaces hardware profile 0/1

                                Configured  Oper
40G Interface  10G Interfaces   Mode        Mode
-------------  --------------  ----------  -------
0/1               0/17-20       1x40G       4x10G
```

Spanning Tree Protocol Commands

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

Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

Default	Enabled
Format	`spanning-tree auto-edge`
Mode	Interface Config

no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree auto-edge`
Mode	Interface Config

spanning-tree backbonefast

Use this command to enable the detection of indirect link failures and accelerate spanning tree convergence on PVSTP configured switches.

Backbonefast accelerates finding an alternate path when an indirect link to the root port goes down.

Backbonefast can be configured even if the switch is configured for MST(RSTP) or PVST mode. It only has an effect when the switch is configured for the PVST mode.

If a backbonefast-enabled switch receives an inferior BPDU from its designated switch on a root or blocked port, it sets the maximum aging time on the interfaces on which it received the inferior BPDU if there are alternate paths to the designated switch. This allows a blocked port to immediately move to the listening state where the port can be transitioned to the forwarding state in the normal manner.

On receipt of an inferior BPDU from a designated bridge, backbonefast enabled switches send a Root Link Query (RLQ) request to all non-designated ports except the port from which it received the inferior BPDU. This check validates that the switch can receive packets from the root on ports where it expects to receive BPDUs. The port from which the original inferior BPDU was received is excluded because it has already encountered a failure. Designated ports are excluded as they do not lead to the root.

On receipt of an RLQ response, if the answer is negative, the receiving port has lost connection to the root and its BPDU is immediately aged out. If all nondesignated ports have already received a negative answer, the whole bridge has lost the root and can start the STP calculation from scratch.

If the answer confirms the switch can access the root bridge on a port, it can immediately age out the port on which it initially received the inferior BPDU.

A bridge that sends an RLQ puts its bridge ID in the PDU. This ensures that it does not flood the response on designated ports.

A bridge that receives an RLQ and has connectivity to the root forwards the query toward the root through its root port.

A bridge that receives a RLQ request and does not have connectivity to the root (switch bridge ID is different from the root bridge ID in the query) or is the root bridge immediately answers the query with its root bridge ID.

RLQ responses are flooded on designated ports.

Default	NA
Format	`spanning-tree backbonefast`
Mode	Global Config

no spanning-tree backbonefast

This command disables backbonefast.

Note: Per VLAN Rapid Spanning Tree Protocol (PVRSTP) embeds support for FastBackbone and FastUplink. Even if FastUplink and FastBackbone are configured, they are effective only in PVSTP mode.

Format `no spanning-tree backbonefast`
Mode Global Config

spanning-tree cost

Use this command to configure the external path cost for port used by a MST instance. When the `auto` keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a *`cost`* value from 1–200000000.

Default auto
Format `spanning-tree cost {`*`cost`* `| auto}`
Mode Interface Config

no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Format `no spanning-tree auto-edge`
Mode Interface Config

spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

Default disabled
Format `spanning-tree bpdufilter`
Mode Interface Config

no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default disabled
Format `no spanning-tree bpdufilter`
Mode Interface Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default disabled
Format `spanning-tree bpdufilter`
Mode Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default disabled
Format `no spanning-tree bpdufilter default`
Mode Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on an interface or range of interfaces.

Default disabled
Format `spanning-tree bpduflood`
Mode Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface or range of interfaces.

Default disabled
Format `no spanning-tree bpduflood`
Mode Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default disabled
Format `spanning-tree bpduguard`
Mode Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default disabled
Format `no spanning-tree bpduguard`
Mode Global Config

spanning-tree bpdumigrationcheck

Use this command to force 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 name`

Mode Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format `no spanning-tree configuration name`

Mode Global Config

spanning-tree configuration revision

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

Default 0

Format `spanning-tree configuration revision 0-65535`

Mode Global Config

no spanning-tree configuration revision

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

Format `no spanning-tree configuration revision`

Mode Global 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 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 “(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 guard

This command selects whether loop guard or root guard is enabled on an interface or range of interfaces. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default none
Format `spanning-tree guard {none | root | loop}`
Mode Interface Config

no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format `no spanning-tree guard`
Mode Interface 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 x (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 parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

Default 20

Format `spanning-tree max-hops 1-127`

Mode Global Config

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 mode

This command configures global spanning tree mode per VLAN spanning tree. On a switch, only one mode can be enabled at a time.

When PVSTP or rapid PVSTP (PVRSTP) is enabled, MSTP/RSTP/STP is operationally disabled. To reenable MSTP/RSTP/STP, disable PVSTP/RVPVSTP. By default, DCSS has MSTP enabled. In PVSTP or PVRSTP mode, BPDUs contain per-VLAN information instead of the common spanning-tree information (MST/RSTP).

PVSTP maintains independent spanning tree information about each configured VLAN. PVSTP uses IEEE 802.1Q trunking and allows a trunked VLAN to maintain blocked or forwarding state per port on a per-VLAN basis. This allows a trunk port to be forwarded on some VLANs and blocked on other VLANs.

PVRSTP is based on the IEEE 8012.1w standard. It supports fast convergence IEEE 802.1D. RVPVSTP is compatible with IEEE 802.1D spanning tree. PVRSTP sends BPDUs on all ports, instead of only the root bridge sending BPDUs, and supports the discarding, learning, and forwarding states.

When the mode is changed to PVRSTP, version 0 STP BPDUs are no longer transmitted and version 2 PVRSTP BPDUs that carry per-VLAN information are transmitted on the VLANs enabled for spanning-tree. If a version 0 BPDU is seen, RVPVSTP reverts to sending version 0 BPDUs.

Per VLAN Rapid Spanning Tree Protocol (PVRSTP) embeds support for PVSTP FastBackbone and FastUplink. There is no provision to enable or disable these features in PVRSTP.

Default Disabled

Format `spanning-tree mode {pvst|rapid-pvst}`

Mode Global Config

no spanning-tree mode

This command globally configures the switch to the default DCSS spanning-tree mode, MSTP.

Format `no spanning-tree mode { pvst | rapid-pvst }`
Mode Global Configuration

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.
Default enabled
Format `spanning-tree port mode`
Mode Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.
Format `no spanning-tree port mode`
Mode Interface Config

spanning-tree port mode all

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

spanning-tree port-priority

Use this command to change the priority value of the port to allow the operator to select the relative importance of the port in the forwarding process. Set this value to a lower number to prefer a port for forwarding of frames.

All LAN ports have 128 as priority value by default. PVSTP/PVRSTP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.

The application uses the port priority value when the LAN port is configured as an edge port.

Default enabled
Format `spanning-tree port-priority` *`0-240`*
Mode Interface Config

spanning-tree transmit

This command sets the Bridge Transmit Hold Count parameter. The valid hold count range is 1–10.

Default 6
Format `spanning-tree transmit hold-count`
Mode Global Config

Parameter	*Description*
hold-count	The Bridge Tx hold-count parameter. The value in an integer between 1 and 10.

spanning-tree tcnguard

Use this command to enable TCN guard on the interface. When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

Default Enabled
Format `spanning-tree tcnguard`
Mode Interface Config

no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Format `no spanning-tree tcnguard`
Mode Interface Config

spanning-tree uplinkfast

This command configures the rate at which gratuitous frames are sent (in packets per second) after switchover to an alternate port on PVSTP configured switches and enables uplinkfast on PVSTP switches. The range is 0-32000; the default is 150. This command has the effect of accelerating spanning-tree convergence after switchover to an alternate port.

Uplinkfast can be configured even if the switch is configured for MST(RSTP) mode, but it only has an effect when the switch is configured for PVST mode. Enabling FastUplink increases the priority by 3000. Path costs less than 3000 have an additional 3000 added when uplinkfast is enabled. This reduces the probability that the switch will become the root switch.

Uplinkfast immediately changes to an alternate root port on detecting a root port failure and changes the new root port directly to the fowarding state. A TCN is sent for this event.

After a switchover to an alternate port (new root port), uplinkfast multicasts a gratuitous frame on the new root port on behalf of each attached machine so that the rest of the network knows to use the secondary link to reach that machine.

PVRSTP embeds support for backbonefast and uplinkfast. There is no provision to enable or disable these features in PVRSTP configured switches.

Default 150
Format spanning-tree uplinkfast [max-update-rate *packets*]
Mode Global Config

no spanning-tree uplinkfast

This command disables uplinkfast on PVSTP configured switches. All switch priorities and path costs that have not been modified from their default values are set to their default values.

Format no spanning-tree uplinkfast [max-update-rate]
Mode Global Config

spanning-tree vlan

Use this command to enable/disable spanning tree on a VLAN.

Default None
Format spanning-tree vlan *vlan-list*
Mode Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.

spanning-tree vlan cost

Use this command to set the path cost for a port in a VLAN. The valid values are in the range of 1 to 200000000 or auto. If auto is selected, the path cost value is set based on the link speed.

Default None
Format spanning-tree vlan *vlan-id* cost {auto |*1-200000000*}
Mode Interface Config

spanning-tree vlan forward-time

Use this command to configure the spanning tree forward delay time for a VLAN or a set of VLANs. The default is 15 seconds.

Set this value to a lower number to accelerate the transition to forwarding. The network operator should take into account the end-to-end BPDU propagation delay, the maximum frame lifetime, the maximum transmission halt delay, and the message age overestimate values specific to their network when configuring this parameter.

Default `15 seconds`

Format `spanning-tree vlan vlan-list forward-time 4-30`

Mode Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.
forward-time	The spanning tree forward delay time. The range is 4-30 seconds.

spanning-tree vlan hello-time

Use this command to configure the spanning tree hello time for a specified VLAN or a range of VLANs. The default is 2 seconds. Set this value to a lower number to accelerate the discovery of topology changes.

Default `2 seconds`

Format `spanning-tree vlan vlan-list hello-time 1-10`

Mode Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.
hello-time	The spanning tree forward hello time. The range is 1-10 seconds.

spanning-tree vlan max-age

Use this command to configure the spanning tree maximum age time for a set of VLANs. The default is 20 seconds.

Set this value to a lower number to accelerate the discovery of topology changes. The network operator must take into account the end-to-end BPDU propagation delay and message age overestimate for their specific topology when configuring this value.

The default setting of 20 seconds is suitable for a network of diameter 7, lost message value of 3, transit delay of 1, hello interval of 2 seconds, overestimate per bridge of 1 second, and a BPDU delay of 1 second. For a network of diameter 4, a setting of 16 seconds is appropriate if all other timers remain at their default values.

Default `20 seconds`

Format `spanning-tree vlan vlan-list max-age 6-40`

Mode Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.

Parameter	*Description*
hello-time	The spanning tree forward hello time. The range is 1-10 seconds.

spanning-tree vlan port-priority

Use this command to change the VLAN port priority value of the VLAN port to allow the operator to select the relative importance of the VLAN port in the forwarding selection process when the port is configured as a point-to-point link type. Set this value to a lower number to prefer a port for forwarding of frames.

Default None

Format spanning-tree vlan *vlan-id* port-priority *priority*

Mode Interface Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.
priority	The VLAN port priority. The range is 0-255.

spanning-tree vlan root

Use this command to configure the switch to become the root bridge or standby root bridge by modifying the bridge priority from the default value of 32768 to a lower value calculated to ensure the bridge is the root (or standby) bridge.

The logic takes care of setting the bridge priority to a value lower (primary) or next lower (secondary) than the lowest bridge priority for the specified VLAN or a range of VLANs.

Default 32768

Format spanning-tree vlan *vlan-list* root {primary|secondary}

Mode Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.

spanning-tree vlan priority

Use this command to configure the bridge priority of a VLAN. The default value is 32768.

If the value configured is not among the specifed values, it will be rounded off to the nearest valid value.

Default 32768

Format spanning-tree vlan *vlan-list* priority *priority*

Mode Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.
priority	The VLAN bridge priority. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format `show spanning-tree`

Mode
- Privileged EXEC
- User EXEC

Parameter	*Definition*
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Root Port Max Age	Derived value.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
Bridge Max Hops	Bridge max-hops count for the device.
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

show spanning-tree active

Use this command to display the spanning tree values on active ports for the modes (xSTP and PV(R)STP).

Format `show spanning-tree active`

Mode
- Privileged EXEC
- User EXEC

Example: Example 1

```
(Routing)#show spanning-tree active

Spanning Tree: Enabled (BPDU Flooding: Disabled) Portfast BPDU Filtering: Disabled
Mode: rstp
CST Regional Root:        80:00:00:01:85:48:F0:0F
Regional Root Path Cost:  0


###### MST 0 Vlan Mapped:   3
ROOT ID
              Priority        32768
              Address         00:00:EE:EE:EE:EE
              This Switch is the Root.
              Hello Time: 2s Max Age: 20s Forward Delay: 15s
Interfaces

Name      State    Prio.Nbr  Cost      Sts            Role  RestrictedPort
--------- -------- --------- --------- -------------- ----- --------------
0/49      Enabled  128.49    2000      Forwarding     Desg  No
3/1       Enabled  96.66     5000      Forwarding     Desg  No
3/2       Enabled  96.67     5000      Forwarding     Desg  No
3/10      Enabled  96.75     0         Forwarding     Desg  No
```

Example: Example 2

```
(Routing)#show spanning-tree active

Spanning-tree enabled protocol rpvst

VLAN    1
 RootID    Priority        32769
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface State     Prio.Nbr  Cost    Status         Role
--------- --------- --------- ------- -------------- -----------
0/49      Enabled   128.49    2000    Forwarding     Designated
3/1       Enabled   128.66    5000    Forwarding     Designated
3/2       Enabled   128.67    5000    Forwarding     Designated
3/10      Enabled   128.75    0       Forwarding     Designated
```

```
VLAN    3
 RootID    Priority        32771
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32771 (priority 32768 sys-id-ext 3)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
3/1       Enabled   128.66    5000    Forwarding    Designated
3/2       Enabled   128.67    5000    Forwarding    Designated
3/10      Enabled   128.75    0       Forwarding    Designated
```

Example: Example 3

```
(Routing)#show spanning-tree active

Spanning-tree enabled protocol rpvst

VLAN    1
 RootID    Priority        32769
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            10(3/10   )
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
0/49      Enabled   128.49    2000    Discarding    Alternate
3/1       Enabled   128.66    5000    Forwarding    Disabled
3/2       Enabled   128.67    5000    Forwarding    Disabled
3/10      Enabled   128.75    0       Forwarding    Root

VLAN    3
 RootID    Priority        32771
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            10(3/10   )
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32771 (priority 32768 sys-id-ext 3)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
3/1       Enabled   128.66    5000    Forwarding    Disabled
3/2       Enabled   128.67    5000    Forwarding    Disabled
```

```
3/10      Enabled   128.75    0       Forwarding    Root
```

show spanning-tree backbonefast

This command displays spanning tree information for backbonefast.

Format `show spanning-tree backbonefast`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Transitions via Backbonefast	The number of backbonefast transitions.
Inferior BPDUs received (all VLANs)	The number of inferior BPDUs received on all VLANs.
RLQ request PDUs received (all VLANs)	The number of root link query (RLQ) requests PDUs received on all VLANs.
RLQ response PDUs received (all VLANs)	The number of RLQ response PDUs received on all VLANs.
RLQ request PDUs sent (all VLANs)	The number of RLQ request PDUs sent on all VLANs.
RLQ response PDUs sent (all VLANs)	The number of RLQ response PDUs sent on all VLANs.

Example: The following example shows output from the command.

```
(Routing)#show spanning-tree backbonefast

Backbonefast Statistics
-----------------------
Transitions via Backbonefast (all VLANs)         : 0
Inferior BPDUs received (all VLANs)              : 0
RLQ request PDUs received (all VLANs)            : 0
RLQ response PDUs received (all VLANs)           : 0
RLQ request PDUs sent (all VLANs)                : 0
RLQ response PDUs sent (all VLANs)               : 0
```

show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format `show spanning-tree brief`

Mode
- Privileged EXEC
- User EXEC

Parameter	*Definition*
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.

Parameter	*Definition*
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* | lag *lag-id*} is the desired switch port or LAG to view. The following details are displayed on execution of the command.

Format show spanning-tree interface {*slot/port* | lag *lag-id*}

Mode
- Privileged EXEC
- User EXEC

Parameter	*Definition*
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Guard Effect	Enabled or disabled.
Root Guard	Enabled or disabled.
Loop Guard	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.
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 summary

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

Format `show spanning-tree summary`

Mode
- Privileged EXEC
- User EXEC

Parameter	*Definition*
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 uplinkfast

This command displays spanning tree information for uplinkfast.

Format `show spanning-tree uplinkfast`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Uplinkfast transitions (all VLANs)	The number of uplinkfast transitions on all VLANs.
Proxy multicast addresses transmitted (all VLANs)	The number of proxy multicast addresses transmitted on all VLANs.

Example: The following example shows output from the command.

```
(Routing) #show spanning-tree uplinkfast

Uplinkfast is enabled.
BPDU update rate : 150 packets/sec

Uplinkfast Statistics
---------------------
Uplinkfast transitions (all VLANs)..... 0
Proxy multicast addresses transmitted (all VLANs).. 0
```

show spanning-tree vlan

This command displays spanning tree information per VLAN and also lists out the port roles and states along with port cost. The *vlan-list* parameter is a list of VLANs or VLAN-ranges separated by commas and with no embedded blank spaces. VLAN ranges are of the form “X-Y” where X and Y are valid VLAN identifiers and X< Y. The *vlanid* corresponds to an existing VLAN ID.

Format `show spanning-tree vlan {vlanid | vlan-list}`

Mode
- Privileged EXEC
- User EXEC

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

```
(Routing) show spanning-tree vlan 1

VLAN    1
          Spanning-tree enabled protocol rpvst
          RootID    Priority        32769
           Address         00:0C:29:D3:80:EA
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 15 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:0C:29:D3:80:EA
           Hello Time 2 Sec Max Age 15 sec Forward Delay 15 sec
           Aging Time 300
Interface  Role        Sts            Cost         Prio.Nbr
---------  ----------  -------------  ---------    --------
1/0/1      Designated  Forwarding     3000        128.1
1/0/2      Designated  Forwarding     3000        128.2
1/0/3      Disabled    Disabled       3000        128.3
1/0/4      Designated  Forwarding     3000        128.4
1/0/5      Designated  Forwarding     3000        128.5
1/0/6      Designated  Forwarding     3000        128.6
1/0/7      Designated  Forwarding     3000        128.7
1/0/8      Designated  Forwarding     3000        128.8
0/1/1      Disabled    Disabled       3000        128.1026
0/1/2      Disabled    Disabled       3000        128.1027
0/1/3      Disabled    Disabled       3000        128.1028
0/1/4      Disabled    Disabled       3000        128.1029
0/1/5      Disabled    Disabled       3000        128.1030
0/1/6      Disabled    Disabled       3000        128.1031
```

VLAN Commands

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.

Format `vlan database`

Mode Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

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.

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). VLAN range is 1-4093.

Format `vlan` *`1-4093`*

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 1-4093.

Format `no vlan 1-`*`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. ID range is 1-4093.

Default

- VLAN ID 1 - default
- other VLANS - blank string

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 1-4093`

Mode VLAN 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 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 `vlan tagging 1-4093`

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 `no vlan tagging 1-4093`

Mode
- Interface Config

show vlan

This command displays information about the configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and the ports which belong to a private VLAN.

Format `show vlan {vlanid|private-vlan [type]}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Primary	Primary VLAN identifier. The range of the VLAN ID is 1 to 4093.
Secondary	Secondary VLAN identifier.
Type	Secondary VLAN type (community, isolated, or primary).
Ports	Ports which are associated with a private VLAN.
VLAN ID	The 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 Default (VLAN ID = 1) or static (one that is configured and permanently defined), or 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	The physical port, or LAG interface associated with the rest of the data in the row.
Current	The degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. • **Tagged** - Transmit traffic for this VLAN as tagged frames. • **Untagged** - Transmit traffic for this VLAN as untagged frames.

show vlan internal usage

This command displays information about the VLAN ID allocation on the switch.

Format `show vlan internal usage`

Mode
- Privileged EXEC
- User EXEC

Parameter	*Definition*
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

Parameter	*Definition*
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1-4093.
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 Default (VLAN ID = 1) or static (one that is configured and permanently defined).

show vlan port

This command displays VLAN port information.

Format `show vlan port {`*`slot/port`* `| all}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	*`slot/port`* It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID Configured	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.
Port VLAN ID Current	The current VLAN ID that this port assigns to untagged frames or priority tagged frames received on this port. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering Configured	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.
Ingress Filtering Current	Shows the current ingress filtering configuration.
GVRP	May be enabled or disabled.

Term	*Definition*
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.
Protected Port	Specifies if this is a protected port. If False, it is not a protected port; If true, it is.
Switchport mode	The current switchport mode for the port.
Operating parameters	The operating parameters for the port, including the VLAN, name, egress rule, and type.
Static configuration	The static configuration for the port, including the VLAN, name, and egress rule.
Forbidden VLANs	The forbidden VLAN configuration for the port, including the VLAN and name.

Switch Ports

This section describes the commands used for switch port mode.

switchport mode

Use this command to configure the mode of a switch port as access, trunk or general.

In Trunk mode, the port becomes a member of all VLANs on switch unless specified in the allowed list in the `switchport trunk allowed vlan` command. The PVID of the port is set to the Native VLAN as specified in the `switchport trunk native vlan` command. It means that trunk ports accept both tagged and untagged packets, where untagged packets are processed on the native VLAN and tagged packets are processed on the VLAN ID contained in the packet. MAC learning is performed on both tagged and untagged packets. Tagged packets received with a VLAN ID of which the port is not a member are discarded and MAC learning is not performed. The Trunk ports always transmit packets untagged on native VLAN.

In Access mode, the port becomes a member of only one VLAN. The port sends and receives untagged traffic. It can also receive tagged traffic.The ingress filtering is enabled on port. It means that when the VLAN ID of received packet is not identical to Access VLAN ID, the packet is discarded.

In General mode, the user can perform custom configuration of VLAN membership, PVID, tagging, ingress filtering etc. This is legacy DCSS behavior of switch port configuration. Legacy DCSS CLI commands are used to configure port in general mode.

Default	General mode
Format	`switchport mode {access | trunk | general}`
Mode	Interface Config

no switchport mode

This command resets the switch port mode to its default value.

Format	`no switchport mode`
Mode	Interface Config

switchport trunk allowed vlan

Use this command to configure the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. The default is all.

The VLANs list can be modified using the add or remove options or replaced with another list using the vlan-list, all, or except options. If all is choosen, all VLANs are added to the list of allowed vlan. The except option provides an exclusion list.

Trunk ports accept tagged packets, where tagged packets are processed on the VLAN ID contained in the packet, if this VLAN is in the allowed VLAN list. Tagged packets received with a VLAN ID to which the port is not a member are discarded and MAC learning is not performed. If a VLAN is added to the system after a port is set to the Trunk mode and it is in the allowed VLAN list, this VLAN is assigned to this port automatically.

Default All

Format `switchport trunk allowed vlan {vlan-list | all | {add vlan-list} | {remove vlan-list} | {except vlan-list }}`

Mode Interface Config

Parameter	*Description*
all	Specifies all VLANs from 1 to 4093. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
add	Adds the defined list of VLANs to those currently set instead of replacing the list.
remove	Removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4093; extended-range VLAN IDs of the form X-Y or X,Y,Z are valid in this command.
except	Lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)
vlan-list	Either a single VLAN number from 1 to 4093 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

no switchport trunk allowed vlan

This command resets the list of allowed VLANs on the trunk port to its default value.

Format `no switchport trunk allowed vlan`

Mode Interface Config

switchport trunk native vlan

Use this command to configure the Trunk port Native VLAN (PVID) parameter. Any ingress untagged packets on the port are tagged with the value of Native VLAN. Native VLAN must be in the allowed VLAN list for tagging of received untagged packets. Otherwise, untagged packets are discarded. Packets marked with Native VLAN are transmitted untagged from Trunk port. The default is 1.

Default 1 (Default VLAN)

Format `switchport trunk native vlan vlan-id`

Mode Interface Config

no switchport trunk native vlan

Use this command to reset the switch port trunk mode native VLAN to its default value.

Format `no switchport trunk native vlan`
Mode Interface Config

switchport access vlan

Use this command to configure the VLAN on the Access port. Only one VLAN can be assigned to the Access port. Access ports are members of VLAN 1 by default. Access ports may be assigned to a VLAN other than VLAN 1. Removing the Access VLAN on the switch makes the Access port a member of VLAN 1. Configuring an Access port to be a member of a VLAN that does not exist results in an error and does not change the configuration.

Default 1 (Default VLAN)
Format `switchport access vlan` *`vlan-id`*
Mode Interface Config

no switchport access vlan

This command resets the switch port access mode VALN to its default value.

Format `no switchport access vlan`
Mode Interface Config

show interfaces switchport

Use this command to display the switchport status for all interfaces or a specified interface.

Format `show interfaces switchport` *`slot/port`*
Mode Privileged EXEC

Example:

```
(Routing) #show interfaces switchport 1/0/1

Port: 1/0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False
```

```
(Routing) #show interfaces switchport

Port: 1/0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False
```

show interfaces switchport

Use this command to display the Switchport configuration for a selected mode per interface. If the interface is not specified, the configuration for all interfaces is displayed.

Format `show interfaces switchport {access | trunk | general} [slot/port]`

Mode Privileged EXEC

Example:

```
Switching) # show interfaces switchport access 1/0/1

Intf      PVID
--------- ----
1/0/1      1


(Switching) # show interfaces switchport trunk 1/0/6

Intf      PVID  Allowed Vlans List
--------- ----- -------------------
1/0/6     1     All


(Switching) # show interfaces switchport general 1/0/5

Intf      PVID  Ingress     Acceptable  Untagged  Tagged   Forbidden  Dynamic
                Filtering   Frame Type  Vlans     Vlans    Vlans     Vlans
--------- ----- ----------- ----------  --------- --------- --------- ---------
1/0/5     1     Enabled     Admit All   7         10-50,55  9,100-200 88,96



(Switching) # show interfaces switchport general

Intf      PVID  Ingress     Acceptable  Untagged  Tagged   Forbidden  Dynamic
                Filtering   Frame Type  Vlans     Vlans    Vlans     Vlans
```

```
--------- ----- ---------- ----------  --------- --------- --------- ---------
1/0/1     1     Enabled    Admit All   1,4-7     30-40,55  3,100-200 88,96
1/0/2     1     Disabled   Admit All   1         30-40,55  none      none
..
```

Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which is 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, 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 "speed" on page 191.

Format `port-channel` *name*
Mode Global 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 enabled, which means the port-channel is static. 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 enabled
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

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch. Instead of *`slot/port`*, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format `show port-channel`

Mode
- Privileged EXEC

Term	*Definition*
Logical Interface	The valid slot/port number.
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.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • **Static** - The port-channel is statically maintained. • **Dynamic** - The port-channel is dynamically maintained.
Local Preference Mode	Indicates whether the local preference mode is **enabled** or **disabled**.
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	This field lists ports that are actively participating in the port-channel (LAG).

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

```
(Switch) #show port-channel 3/1


Local Interface.............................. 3/1
Channel Name................................. ch1
Link State................................... Up
Admin Mode................................... Enabled
Type......................................... Static
Load Balance Option.......................... 3
(Src/Dest MAC, VLAN, EType, incoming port)
Local Preference Mode........................ Enabled

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
```

```
0/1     actor/long     Auto       True
        partner/long
0/2     actor/long     Auto       True
        partner/long
0/3     actor/long     Auto       False
        partner/long
0/4     actor/long     Auto       False
        partner/long
```

show port-channel counters

Use this command to display port-channel counters for the specified port.

Format `show port-channel slot/port counters`

Mode Privileged EXEC

Term	*Definition*
Local Interface	The valid slot/port number.
Channel Name	The name of this port-channel (LAG).
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Port Channel Flap Count	The number of times the port-channel was inactive.
Mbr Ports	The slot/port for the port member.
Mbr Flap Counters	The number of times a port member is inactive, either because the link is down, or the admin state is disabled.

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

```
(Switch) #show port-channel 0/3/1 counters


Local Interface.............................. 3/1
Channel Name................................. ch1
Link State................................... Down
Admin Mode................................... Enabled
Port Channel Flap Count...................... 0

Mbr    Mbr Flap
Ports  Counters
------ ---------
0/1    0
0/2    0
0/3    1
0/4    0
0/5    0
0/6    0
0/7    0
0/8    0
```

clear port-channel counters

Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

Format `clear port-channel {lag-intf-num | slot/port} counters`

Mode Privileged EXEC

clear port-channel all counters

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Format `clear port-channel all counters`

Mode Privileged EXEC

DHCP L2 Relay Agent Commands

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

dhcp l2relay

This command enables the DHCP Layer 2 Relay agent for an interface a range of interfaces in, or all interfaces. The subsequent commands mentioned in this section can only be used when the DHCP L2 relay is enabled.

Format `dhcp l2relay`

Mode
- Global Config
- Interface Config

no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

Format `no dhcp l2relay`

Mode
- Global Config
- Interface Config

dhcp l2relay circuit-id subscription-name

This command sets the Option-82 Circuit ID for a given service subscription identified by *`subscription-string`* on a given interface. The *`subscription-string`* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is enabled using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 circuit-id as the incoming interface number.

Default disabled

Format `dhcp l2relay circuit-id subscription-name subscription-string`

Mode Interface Config

no dhcp l2relay circuit-id subscription-name

This command resets the Option-82 Circuit ID for a given service subscription identified by *`subscription-string`* on a given interface. The *`subscription-string`* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is disabled using this command, all Client DHCP requests that fall under this service subscription are no longer added with Option-82 circuit-id.

Format `no dhcp l2relay circuit-id subscription-name` *`subscription-string`*

Mode Interface Config

dhcp l2relay circuit-id vlan

This parameter sets the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format `dhcp l2relay circuit-id vlan vlan-list`

Mode Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Format `no dhcp l2relay circuit-id vlan vlan-list`

Mode Global Config

dhcp l2relay remote-id subscription-name

This command sets the Option-82 Remote-ID string for a given service subscription identified by *subscription-string* on a given interface or range of interfaces. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. The *remoteid-string* is a character string. When remote-id string is set using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 Remote-id as the configured remote-id string.

Default empty string

Format `dhcp l2relay remote-id remoteid-string subscription-name subscription-string`

Mode Interface Config

no dhcp l2relay remote-id subscription-name

This command resets the Option-82 Remote-ID string for a given service subscription identified by *subscription-string* on a given interface. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When remote-id string is reset using this command, the Client DHCP requests that fall under this service subscription are not added with Option-82 Remote-id.

Format `no dhcp l2relay remote-id remoteid-string subscription-name subscription-string`

Mode Interface Config

dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format `dhcp l2relay remote-id remote-id-string vlan vlan-list`

Mode Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay remote-id vlan

This parameter clears the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format `no dhcp l2relay remote-id vlan vlan-list`

Mode Global Config

dhcp l2relay subscription-name

This command enables relaying DHCP packets on an interface or range of interfaces that fall under the specified service subscription. The *subscription-string* is a character string that needs to be matched with configured DOT1AD subscription string for correct operation.

Default disabled (i.e. no DHCP packets are relayed)

Format `dhcp l2relay subscription-name subscription-string`

Mode Interface Config

no dhcp l2relay subscription-name

This command disables relaying DHCP packets that fall under the specified service subscription. The *subscription-string* is a character string that needs to be matched with configured DOT1AD subscription string for correct operation.

Format `no dhcp l2relay subscription-name subscription-string`

Mode Interface Config

dhcp l2relay trust

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

Default untrusted

Format `dhcp l2relay trust`
Mode Interface Config

no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format `no dhcp l2relay trust`
Mode Interface Config

dhcp l2relay vlan

Use this command to enable the DHCP L2 Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default `disable`
Format `dhcp l2relay vlan` *`vlan-list`*
Mode Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay vlan

Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Format `no dhcp l2relay vlan` *`vlan-list`*
Mode Global Config

show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Format `show dhcp l2relay all`
Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay all

DHCP L2 Relay is Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
```

```
 0/4        Disabled     trusted

VLAN Id    L2 Relay  CircuitId  RemoteId
--------- ----------  ----------- ------------
3           Disabled    Enabled    --NULL--
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    adtran
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

show dhcp l2relay circuit-id vlan

This command displays DHCP circuit-id vlan configuration.

Format `show dhcp l2relay circuit-id vlan` *`vlan-list`*

Mode Privileged EXEC

Parameter	*Description*
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Format `show dhcp l2relay interface {all | ` *`interface-num`*`}`

Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay interface all

DHCP L2 Relay is  Enabled.

Interface  L2RelayMode   TrustMode
----------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted
```

show dhcp l2relay remote-id vlan

This command displays DHCP Remote-id vlan configuration.

Format `show dhcp l2relay remote-id vlan` *`vlan-list`*

Mode Privileged EXEC

Parameter	*Description*
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Format `show dhcp l2relay stats interface {all | interface-num}`

Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay stats interface all

DHCP L2 Relay is  Enabled.

Interface  UntrustedServer    UntrustedClient  TrustedServer     TrustedClient
            MsgsWithOpt82    MsgsWithOpt82    MsgsWithoutOpt82  MsgsWithoutOpt82
---------  --------------- -----------------  ----------------- --------------
 0/1           0                0                0                0
 0/2           0                0                3                7
 0/3           0                0                0                0
 0/4           0                12               0                0
 0/5           0                0                0                0
 0/6           3                0                0               0
 0/7           0                0                0                0
 0/8           0                0                0                0
 0/9           0                0                0                0
```

show dhcp l2relay subscription interface

This command displays DHCP L2 Relay configuration specific to a service subscription on an interface.

Format `show dhcp l2relay subscription interface {all|interface-num}`

Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay subscription interface all
Interface   SubscriptionName    L2Relay mode  Circuit-Id mode  Remote-Id mode
----------  ----------------   -------------- ---------------  ----------------
  0/1            sub1             Enabled       Disabled         --NULL--
  0/2            sub3             Enabled       Disabled         EnterpriseSwitch
  0/2            sub22            Disabled      Enabled          --NULL--
  0/4            sub4             Enabled       Enabled          --NULL--
```

show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format `show dhcp l2relay agent-option vlan` *`vlan-range`*

Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay agent-option vlan 5-10

DHCP L2 Relay is  Enabled.

VLAN Id    L2 Relay      CircuitId  RemoteId
--------- ----------  ----------- ------------
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    adtran
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

show dhcp l2relay vlan

This command displays DHCP vlan configuration.

Format `show dhcp l2relay vlan` *vlan-list*

Mode Privileged EXEC

Parameter	*Description*
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

clear dhcp l2relay statistics interface

Use this command to reset the DHCP L2 relay counters to zero. Specify the port with the counters to clear, or use the `all` keyword to clear the counters on all ports.

Format `clear dhcp l2relay statistics interface {`*slot/port* | *all*`}`

Mode Privileged EXEC

DHCP Client Commands

DCSS can include vendor and configuration information in DHCP client requests sent to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

dhcp client vendor-id-option

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the DCSS switch.

Format `dhcp client vendor-id-option` *`string`*
Mode Global Config

no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the DCSS switch.

Format `no dhcp client vendor-id-option`
Mode Global Config

dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the DCSS switch.

Format `dhcp client vendor-id-option-string` *`string`*
Mode Global Config

no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format `no dhcp client vendor-id-option-string`
Mode Global Config

show dhcp client vendor-id-option

This command displays the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in DHCP requests.

Format `show dhcp client vendor-id-option`
Mode Privileged EXEC

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

```
(Switching) #show dhcp client vendor-id-option

DHCP Client Vendor Identifier Option.........Enabled
DHCP Client Vendor Identifier Option String...DCSSClient.
```

LLDP (802.1AB) Commands

This section describes the command 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

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default disabled

Format `lldp transmit`

Mode Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format `no lldp transmit`

Mode Interface Config

lldp receive

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default disabled

Format `lldp receive`

Mode Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format `no lldp receive`

Mode Interface Config

lldp timers

Use this command to set 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 1-32768 seconds. The *hold-value* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The *reinit-seconds* is the delay before reinitialization, and the range is 1-0 seconds.

Default
- interval—30 seconds
- hold—4
- reinit—2 seconds

Format `lldp timers [interval interval-seconds] [hold hold-value] [reinit reinit-seconds]`

Mode Global Config

no lldp timers

Use this command to return 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

Use this command to specify 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. To configure the system name, see “snmp-server” on page 58. 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 [sys-desc] [sys-name] [sys-cap] [port-desc]`

Mode Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format `no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Mode Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. This command can be used to configure a single interface or a range of interfaces.

Format `lldp transmit-mgmt`
Mode Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format `no lldp transmit-mgmt`
Mode Interface Config

lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default disabled
Format `lldp notification`
Mode Interface Config

no lldp notification

Use this command to disable notifications.

Default disabled
Format `no lldp notification`
Mode Interface Config

lldp notification-interval

Use this command to configure 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 5-3600 seconds.

Default 5
Format `lldp notification-interval` *`interval`*
Mode Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format `no lldp notification-interval`
Mode Global Config

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format `clear lldp statistics`
Mode Privileged EXEC

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format `clear lldp remote-data`
Mode Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format `show lldp`
Mode Privileged EXEC

Parameter	*Definition*
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 reinitialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display 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

Parameter	*Definition*
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.
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

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format `show lldp statistics {`*slot/port* `| all}`

Mode Privileged EXEC

Parameter	*Definition*
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:

Term	*Definition*
Interface	The interface in *slot/port* format.
TX Total	Total number of LLDP packets transmitted on the port.
RX 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.

Term	*Definition*
TLV MED	The total number of LLDP-MED TLVs received on the interface.
TLV 802.1	The total number of LLDP TLVs received on the interface which are of type 802.1.
TLV 802.3	The total number of LLDP TLVs received on the interface which are of type 802.3.

show lldp remote-device

Use this command to display 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

Parameter	*Definition*
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 example shows CLI display output for the command.

```
(Switching) #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

Use this command to display 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

Parameter	*Definition*
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.
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 alpha-numeric 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 example shows CLI display output for the command.

```
(Switching) #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

Use this command to display 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

Parameter	*Definition*
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

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format `show lldp local-device detail slot/port`

Mode Privileged EXEC

Parameter	*Definition*
Interface	The interface that sends the LLDPDU.
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 alpha-numeric 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

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

Use this command to enable 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

Use this command to disable MED.

Format `no lldp med`
Mode Interface Config

lldp med confignotification

Use this command to configure 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

Use this command to disable notifications.

Format `no lldp med confignotification`
Mode Interface Config

lldp med transmit-tlv

Use this command to specify 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	*Definition*
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

Use this command to remove a TLV.

Format `no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`

Mode Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports.

Format `lldp med all`

Mode Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format `lldp med confignotification all`

Mode Global Config

lldp med faststartrepeatcount

Use this command to set 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` *`[count]`*

Mode Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format `no lldp med faststartrepeatcount`

Mode Global Config

lldp med transmit-tlv all

Use this command to specify 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 [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`

Mode Global Config

Parameter	*Definition*
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

Use this command to remove a TLV.

Format `no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`

Mode Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format `show lldp med`

Mode Privileged EXEC

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

```
(Routing) #show lldp med
LLDP MED Global Configuration
```

```
Fast Start Repeat Count: 3
Device Class: Network Connectivity

(Routing) #
```

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. 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 example shows CLI display output for the command.

```
(Routing) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
0/1      Down    Disabled  Disabled  Disabled     0,1
0/2      Up      Disabled  Disabled  Disabled     0,1
0/3      Down    Disabled  Disabled  Disabled     0,1
0/4      Down    Disabled  Disabled  Disabled     0,1
0/5      Down    Disabled  Disabled  Disabled     0,1
0/6      Down    Disabled  Disabled  Disabled     0,1
0/7      Down    Disabled  Disabled  Disabled     0,1
0/8      Down    Disabled  Disabled  Disabled     0,1
0/9      Down    Disabled  Disabled  Disabled     0,1
0/10     Down    Disabled  Disabled  Disabled     0,1
0/11     Down    Disabled  Disabled  Disabled     0,1
0/12     Down    Disabled  Disabled  Disabled     0,1
0/13     Down    Disabled  Disabled  Disabled     0,1
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
(Routing) #show lldp med interface 0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
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

(Routing) #
```

show lldp med local-device detail

Use this command to display 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 example shows CLI display output for the command.

```
(Routing) #show lldp med local-device detail 0/8
LLDP MED Local Device Detail

Interface: 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

Use this command to display 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

Parameter	*Definition*
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.
Device Class	Device classification of the remote device.

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

```
(Routing) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Remote ID  Device Class
---------  ---------  ------------
0/8           1          Class I
0/9           2          Not Defined
0/10          3          Class II
0/11          4          Class III
0/12          5          Network Con
```

show lldp med remote-device detail

Use this command to display 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 example shows CLI display output for the command.

```
(Routing) #show lldp med remote-device detail 0/8

LLDP MED Remote Device Detail

Local Interface: 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
```

Section 8: IPv4 Routing Commands

This section describes the following routing commands available in the DCSS CLI:

Note: 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.

Address Resolution Protocol Commands

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

arp

This command creates an ARP entry in the specified virtual router instance (vrf vrf-name). If a virtual router is not specified, the static ARP entry is created in the default router. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device. The interface parameter specifies the next hop interface.

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

Format `arp [vrf vrf-name] ipaddress macaddr interface {slot/port | vlan id}`
Mode Global Config

no arp

This command deletes an ARP entry in the specified virtual router. The value for *arpentry* is the IP address of the interface. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device. The interface parameter specifies the next hop interface.

Format `no arp [vrf vrf-name] ipaddress interface {slot/port | vlan id}`
Mode Global Config

arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

Format `arp cachesize platform specific integer value`
Mode Global Config

no arp cachesize

This command configures the default ARP cache size.

Format `no arp cachesize`
Mode Global Config

arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out. When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host may be lost until the router receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option applies only to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Default disabled
Format `arp dynamicrenew`
Mode Privileged EXEC

no arp dynamicrenew

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

Format `no arp dynamicrenew`
Mode Privileged EXEC

arp purge

This command causes the specified IP address to be removed from the ARP cache in the specified virtual router. If no router is specified, the ARP entry is deleted in the default router. Only entries of type dynamic or gateway are affected by this command.

Format `arp purge [vrf vrf-name] ipaddress interface {slot/port | vlan id}`
Mode Privileged EXEC

Parameter	*Description*
ipaddress	The IP address to remove from the ARP cache.
vrf-name	The virtual router from which IP addresses will be removed.
interface	The interface from which IP addresses will be removed.

resptime

This command configures the ARP request response timeout.

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

Default 1
Format `arp resptime 1-10`
Mode Global Config

no arp resptime

This command configures the default ARP request response timeout.

Format `no arp resptime`
Mode Global Config

arp retries

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

The value for *retries* is an integer, which represents the maximum number of request for retries. The range for *retries* is an integer between 0-10 retries.

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

no arp retries

This command configures the default ARP count of maximum request for retries.
Format `no arp retries`
Mode Global Config

arp timeout

This command configures the ARP entry ageout time.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for *seconds* is between 15-21600 seconds.
Default 1200
Format `arp timeout 15-21600`
Mode Global Config

no arp timeout

This command configures the default ARP entry ageout time.

Format `no arp timeout`

Mode Global Config

clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache for the virtual router. If no router is specified, the cache for the default router is cleared. If the *gateway* keyword is specified, the dynamic entries of type gateway are purged as well.

Format `clear arp-cache [vrf vrf-name] [gateway]`

Mode Privileged EXEC

clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, `ping` from the remote system to the DUT. Issue the `show arp switch` command to see the ARP entries. Then issue the `clear arp-switch` command and check the `show arp switch` entries. There will be no more arp entries.

Format `clear arp-switch`

Mode Privileged EXEC

show arp

This command displays the Address Resolution Protocol (ARP) cache for a specified virtual router instance. If a virtual router is not specified, the ARP cache for the default router is displayed. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the `show arp` results in conjunction with the `show arp switch` results.

Format `show arp [vrf vrf-name]`

Mode Privileged EXEC

Parameter	*Definition*
Age Time (seconds)	The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.

Parameter	*Definition*
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Parameter	*Definition*
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing *slot/port* associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

show arp brief

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

Format `show arp brief`

Mode Privileged EXEC

Parameter	*Definition*
Age Time (seconds)	The time it takes for an ARP entry to age out. This value is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format `show arp switch`

Mode Privileged EXEC

Parameter	*Definition*
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing *slot/port* associated with the device's ARP entry.

IP Routing Commands

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

routing

This command enables IPv4 routing for an interface or range of interfaces. You can view the current value for this function with the `show ip brief` command. The value is labeled as “Routing Mode.”

Default	disabled
Format	`routing`
Mode	Interface Config

no routing

This command disables routing for an interface.

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

Format	`no routing`
Mode	Interface Config

ip routing

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

Format	`ip routing`
Mode	• Global Config • Virtual Router Config

no ip routing

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

Format	`no ip routing`
Mode	Global Config

ip address

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface. The command supports RFC 3021 and accepts using 31-bit prefixes on IPv4 point-to-point links. This command adds the label IP address in the command "show ip interface" on page 274.

Note: The 31-bit subnet mask is only supported on routing interfaces. The feature is not supported on network port and service port interfaces because DCSS acts as a host, not a router, on these management interfaces.

Parameter	*Description*
ipaddr	The IP address of the interface.
subnetmask	A 4-digit dotted-decimal number which represents the subnet mask of the interface.
masklen	Implements RFC 3021. Using the **/** notation of the subnet mask, this is an integer that indicates the length of the subnet mask. Range is 5 to 32 bits.

Format `ip address ipaddr {subnetmask | /masklen} [secondary]`

Mode Interface Config

Example: The following example of the command shows the configuration of the subnet mask with an IP address in the dotted decimal format on interface vlan 100.

```
(Routing) (Interface vlan 300)#ip address 192.168.10.1 255.255.255.254

(Routing) (Interface vlan 300)#
```

Example: The next example of the command shows the configuration of the subnet mask with an IP address in the **/** notation on interface vlan 100.

```
(Routing) (Config)#interface vlan 30

(Routing) (Interface vlan 30)#ip address 192.168.10.1 /31
```

no ip address

This command deletes an IP address from an interface. The value for *ipaddr* is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for *subnetmask* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command `no ip address`.

Format `no ip address [{ipaddr subnetmask [secondary]}]`

Mode Interface Config

ip address dhcp

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

To enable the DHCPv4 client on an in-band interface and send DHCP client messages with the client identifier option (DHCP Option 61), use the **ip address dhcp client-id** configuration command in interface configuration mode.

Default disabled

Format `ip address dhcp [client-id]`

Mode Interface Config

Example: In the following example, DHCPv4 is enabled on interface 0/1.

```
(router1) #config
(router1) (Config)#interface 0/1
(router1) (Interface 0/1)#ip address dhcp
```

no ip address dhcp

The **no ip address dhcp** command releases a leased address and disables DHCPv4 on an interface. The **no** form of the **ip address dhcp client-id** command removes the client-id option and also disables the DHCP client on the in-band interface.

Format `no ip address dhcp [client-id]`

Mode Interface Config

ip default-gateway

This command manually configures a default gateway for the switch. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

Format `ip default-gateway` *`ipaddr`*

Mode
- Global Config
- Virtual Router Config

no ip default-gateway

This command removes the default gateway address from the configuration.

Format `no ip default-gateway` *`ipaddr`*

Mode
- Interface Config
- Virtual Router Config

ip load-sharing

This command configures IP ECMP load balancing mode.

Default 6

Format `ip load-sharing mode {inner | outer}`

Mode Global Config

Parameter	*Description*
mode	Configures the load balancing or sharing mode for all EMCP groups. • 1: Based on a hash using the Source IP address of the packet. • 2: Based on a hash using the Destination IP address of the packet. • 3: Based on a hash using the Source and Destination IP addresses of the packet. • 4: Based on a hash using the Source IP address and the Source TCP/UDP Port field of the packet. • 5: Based on a hash using the Destination IP address and the Destination TCP/UDP Port field of the packet. • 6: Based on a hash using the Source and Destination IP address, and the Source and Destination TCP/UDP Port fields of the packet.
inner	Use the inner IP header for tunneled packets.
outer	Use the outer IP header for tunneled packets.

no ip load-sharing

Format `no ip load-sharing`

Mode Global Config

release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface.

Format `release dhcp {slot/port | vlan id}`

Mode Privileged EXEC

renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

Note: This command can be used on in-band ports as well as the service or network (out-of-band) port.

Format `renew dhcp {slot/port | vlan id}`
Mode Privileged EXEC

renew dhcp network-port

Use this command to renew an IP address on a network port.

Format `renew dhcp network-port`
Mode Privileged EXEC

renew dhcp service-port

Use this command to renew an IP address on a service port.

Format `renew dhcp service-port`
Mode Privileged EXEC

ip route

This command configures a static route in a specified virtual router instance (vrf *vrf-name*). The *ipaddr* parameter is a valid IP address, and *subnetmask* is a valid subnet mask. The *nexthopip* parameter is a valid IP address of the next hop router. Specifying `Null0` as nexthop parameter adds a static reject route. The optional *preference* parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

The description parameter allows a description of the route to be entered.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Default preference—1
Format `ip route [vrf vrf-name]ipaddr subnetmask { nexthopip | Null0 | interface {slot/port| vlan-id}} [preference] [description description]`
Mode Global Config

Example:

Subnetwork 9.0.0.0/24 is a connected subnetwork in global table and subnet 56.6.6.0/24 is reachable via a gateway 9.0.0.2 in the global table.

Subnet 8.0.0.0/24 is a connected subnetwork in virtual router *Red*.

Now we leak the 2 routes from global route table into the virtual router *Red* and leak the connected subnet 8.0.0.0/24 from *Red* to global table.

When leaking connected route in the global routing table to a virtual router, the /32 host route for the leaked host is added in the virtual router instance's route table.

Also we add a non-leaked static route for 66.6.6.0/24 subnetwork scoped to the domain of virtual router Red below.

```
(Router) (Config)#ip routing
(Router) (Config)#ip vrf Red
(Router) (Config)#interface 0/27
(Router) (Interface 0/27)#routing
(Router) (Interface 0/27)#ip vrf forwarding Red
(Router) (Interface 0/27)#ip address 8.0.0.1 /24

(Router) (Interface 0/27)#interface 0/26
(Router) (Interface 0/26)#routing
(Router) (Interface 0/26)#ip address 9.0.0.1 /24
(Router) (Interface 0/26)#exit

(Router) (Config)#ip route 56.6.6.0 /24 9.0.0.2

Routes leaked from global routing table to VRF's route table are :
(Router) (Config)#ip route vrf Red 9.0.0.2 255.255.255.255 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 56.6.6.0 255.255.255.0 9.0.0.2 0/26

Route leaked from VRF's route table to global routing table is :
(Router) (Config)#ip route 8.0.0.2 255.255.255.255 0/27

Route (non-leaked) internal to VRF's route table is :
(Router) (Config)#ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2
```

no ip route

This command deletes a single next hop to a destination static route. If you use the *nexthopip* parameter, the next hop is deleted. If you use the *preference* value, the preference value of the static route is reset to its default.

Format `no ip route` *ipaddr subnetmask [*{*nexthopip [preference]* | `Null0`}*]*

Mode Global Config

ip route default

This command configures the default route. The value for *nexthopip* is a valid IP address of the next hop router. The *preference* is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default preference—1

Format `ip route default` *nexthopip [preference]*

Mode Global Config

no ip route default

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

Format `no ip route default [{nexthopip | preference}]`
Mode Global Config

ip route distance

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

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

no ip route distance

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

Format `no ip route distance`
Mode Global Config

ip route net-prototype

This command adds net prototype IPv4 routes to the hardware.

Format `ip route net-prototype prefix/prefix-length nexthopip num-routes`
Mode Global Config

Parameter	*Description*
prefix/prefix-length	The destination network and mask for the route.
nexthopip	The next-hop ip address, It must belong to an active routing interface, but it does not need to be resolved.
num-routes	The number of routes need to added into hardware starting from the given prefix argument and within the given prefix-length.

no ip route net-prototype

This command deletes all the net prototype IPv4 routes added to the hardware.

Format `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*
Mode Global Config

ip netdirbcast

This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default disabled
Format `ip netdirbcast`
Mode Interface Config

no ip netdirbcast

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

Format `no ip netdirbcast`
Mode Interface Config

ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.

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

Note: The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see “mtu” on page 189) must take into account the size of the Ethernet header.

Default 1500 bytes
Format `ip mtu` *`68-9198`*
Mode Interface Config

no ip mtu

This command resets the ip mtu to the default value.

Format `no ip mtu`

Mode Interface Config

ip unnumbered gratuitous-arp accept

This command enables the configuration of static interface routes to the unnumbered peer dynamically on receiving gratuitous ARP.

Default Interface route installation for receiving gratuitous ARP is enabled by default.

Format `ip unnumbered gratuitous-arp accept`

Mode Interface Config

no ip unnumbered gratuitous-arp accept

This command disables interface route configuration on receiving gratuitous ARP.

Format `no ip unnumbered gratuitous-arp accept`

Mode Interface Config

ip unnumbered loopback

This command identifies unnumbered interfaces and specifies the numbered interface providing the borrowed address. The `interface` should be loopback interface number.

Default Interfaces are numbered by default.

Format `ip unnumbered loopback` *`interface`*

Mode Interface Config

Parameter	*Definition*
interface	The numbered interface providing the borrowed address. This interface cannot be unnumbered. The loopback interface is identified by its loopback interface number.

no ip unnumbered loopback

This command removes the unnumbered configuration.

Format `no ip unnumbered loopback`

Mode Interface Config

encapsulation

This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be `ethernet` or `snap`.

Default ethernet

Format `encapsulation {ethernet | snap}`

Mode Interface Config

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

show dhcp lease

This command displays a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. This command does not apply to service or network ports.

Format `show dhcp lease [interface {`*`slot/port`*` | vlan `*`id`*`}]`

Modes Privileged EXEC

Parameter	*Definition*
IP address, Subnet mask	The IP address and network mask leased from the DHCP server
DHCP Lease server	The IPv4 address of the DHCP server that leased the address.
State	State of the DHCPv4 Client on this interface
DHCP transaction ID	The transaction ID of the DHCPv4 Client
Lease	The time (in seconds) that the IP address was leased by the server
Renewal	The time (in seconds) when the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address
Rebind	The time (in seconds) when the DHCP Rebind process starts
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds

show ip brief

This command displays the summary information of the IP global configurations for the specified virtual router, including the ICMP rate limit configuration and the global ICMP Redirect configuration. If no router is specified, information related to the default router is displayed.

Format `show ip brief [vrf `*`vrf-name`*`]`

Modes
- Privileged EXEC
- User EXEC

Parameter	*Definition*
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. *Burst-interval* is from 0 to 2147483647 milliseconds. The default *burst-interval* is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.

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

```
(Routing) #show ip brief

Default Time to Live.......................... 64
Routing Mode.................................. Disabled
Maximum Next Hops............................. 4
Maximum Routes................................ 6000
ICMP Rate Limit Interval...................... 1000 msec
ICMP Rate Limit Burst Size.................... 100 messages
ICMP Echo Replies............................. Enabled
ICMP Redirects................................ Enabled
```

show ip interface

This command displays all pertinent information about the IP interface.

Format `show ip interface {slot/port | vlan vlan-id}`

Modes
- Privileged EXEC
- User EXEC

Parameter	*Definition*
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Unnumbered	For unnumbered interfaces, the IP address of the borrowed interface.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.

Parameter	*Definition*
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the **client-id** option on the in-band interface. See “ip address dhcp” on page 266.

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

```
(Routing) #show ip interface 0/1

Routing interface status..................... Up
Unnumbered - numbered interface.............. loopback 1
Unnumbered - gratuitous ARP accept........... Enable
Method....................................... N/A
Routing Mode................................. Enable
Administrative Mode.......................... Enable
Forward Net Directed Broadcasts.............. Disable
Active State................................. Active
Link Speed Data Rate......................... 1000 Full
MAC address.................................. 00:10:18:82:18:26
Encapsulation Type........................... Ethernet
IP MTU....................................... 1500
Bandwidth.................................... 1000000 kbps
Destination Unreachables..................... Enabled
ICMP Redirects............................... Enabled
Interface Suppress Status.................... Unsuppressed
Interface Name............................... rt1_0_1
```

Example: In the following example the DHCP client is enabled on a VLAN routing interface.

```
(Routing) #show ip interface vlan 10

Routing Interface Status..... Up
Method....................... DHCP
Routing Mode................. Enable
Administrative Mode.......... Enable
Forward Net Directed Broadcasts..... Disable
```

```
Active State.......................... Inactive
Link Speed Data Rate.................. 10 Half
MAC address........................... 00:10:18:82:16:0E
Encapsulation Type.................... Ethernet
IP MTU................................ 1500
Bandwidth............................. 10000 kbps
Destination Unreachables.............. Enabled
ICMP Redirects........................ Enabled
Interface Suppress Status............. Unsuppressed
DHCP Client Identifier................ 0dcss-0010.1882.160E-vl10
Interface Name........................... rt_v10
```

show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router, and indicates how each IP address was assigned for a specified virtual router instance. If a virtual router is not specified, the IP configuration settings cache for the default router is displayed.

Format `show ip interface [vrf vrf-name] brief`

Modes
- Privileged EXEC
- User EXEC

Parameter	*Definition*
Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format. Unnumbered interfaces show unnumbered and the corresponding numbered interface instead of the IP address.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Method	Indicates how each IP address was assigned. The field contains one of the following values: • **DHCP** - The address is leased from a DHCP server. • **Manual** - The address is manually configured.

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

```
(alpha1) #show ip interface brief

Interface    State  IP Address      IP Mask         Method
----------   -----  --------------- --------------- --------
0/17       Up     192.168.75.1    255.255.255.0   DHCP
0/19       Up     unnumbered
                      -->loopback 2                N/A
loopback 1   Down   0.0.0.0         0.0.0.0         None
loopback 2   Up     3.2.0.3         255.255.255.0   Manual
```

show ip load-sharing

This command displays the currently configured IP ECMP load balancing mode.

Format `show ip load-sharing`

Mode Privileged Exec

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

```
(Routing) #show ip load-sharing

ip load-sharing 6 inner
```

show ip protocols

This command lists a summary of the configuration and status for each unicast routing protocol running in the specified virtual router. The command lists routing protocols which are configured and enabled. If a protocol is selected on the command line, the display will be limited to that protocol. If no virtual router is specified, the configuration and status for the default router are displayed.

Format `show ip protocols [vrf vrf-name] [bgp | ospf]`

Mode Privileged EXEC

Parameter	*Description*
BGP Section:	
Routing Protocol	BGP.
Router ID	The router ID configured for BGP.
Local AS Number	The AS number that the local router is in.
BGP Admin Mode	Whether BGP is globally enabled or disabled.
Maximum Paths	The maximum number of next hops in an internal or external BGP route.
Always Compare MED	Whether BGP is configured to compare the MEDs for routes received from peers in different ASs.
Maximum AS Path Length	Limit on the length of AS paths that BGP accepts from its neighbors.
Fast Internal Failover	Whether BGP immediately brings down a iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast External Failover	Whether BGP immediately brings down an eBGP adjacency if the link to the neighbor goes down.
Distance	The default administrative distance (or route preference) for external, internal, and locally-originated BGP routes. The table that follows lists ranges of neighbor addresses that have been configured to override the default distance with a neighbor-specific distance. If a neighbor's address falls within one of these ranges, routes from that neighbor are assigned the configured distance. If a prefix list is configured, then the distance is only assigned to prefixes from the neighbor that are permitted by the prefix list.
Redistribution	A table showing information for each source protocol (connected, static, and ospf). For each of these sources the distribution list and route-map are shown, as well as the configured metric. Fields which are not configured are left blank. For ospf, an additional line shows the configured ospf match parameters.

Parameter	*Description*
Prefix List In	The global prefix list used to filter inbound routes from all neighbors.
Prefix List Out	The global prefix list used to filter outbound routes to all neighbors.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked “active.”
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
OSPFv2 Section:	
Routing Protocol	OSPFv2.
Router ID	The router ID configured for OSPFv2.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.
Routing for Networks	The address ranges configured with an OSPF network command.
Distance	The administrative distance (or “route preference”) for intra-area, inter-area, and external routes.
Default Route Advertise	Whether OSPF is configured to originate a default route.
Always	Whether default advertisement depends on having a default route in the common routing table.
Metric	The metric configured to be advertised with the default route.
Metric Type	The metric type for the default route.
Redist Source	A type of routes that OSPF is redistributing.
Metric	The metric to advertise for redistributed routes of this type.
Metric Type	The metric type to adveritse for redistributed routes of this type.
Subnets	Whether OSPF redistributes subnets of classful addresses, or only classful prefixes.
Dist List	A distribute list used to filter routes of this type. Only routes that pass the distribute list are redistributed.
Number of Active Areas	The number of OSPF areas with at least one interface running on this router. Also broken down by area type.
ABR Status	Whether the router is currently an area border router. A router is an area border router if it has interfaces that are up in more than one area.
ASBR Status	Whether the router is an autonomous system boundary router. The router is an ASBR if it is redistributing any routes or originating a default route.

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

```
(Router) #show ip protocols

Routing Protocol..... BGP
Router ID..... 6.6.6.6
Local AS Number..... 65001
BGP Admin Mode..... Enable
Maximum Paths..... Internal 32, External 32
Always compare MED ..... FALSE
Maximum AS Path Length ..... 75
Fast Internal Failover ..... Enable
Fast External Failover ..... Enable
```

```
Distance.............................. Ext 20 Int 200 Local 200
  Address         Wildcard        Distance    Pfx List
  -------         --------        --------    --------
  172.20.0.0      0.0.255.255           40        None
  172.21.0.0      0.0.255.255           45           1

Prefix List In........................ PfxList1
Prefix List Out....................... None

Redistributing:
Source        Metric  Dist List               Route Map
--------- ----------  ---------------------- --------------------------
connected             connected_list
static         32120                         static_routemap
ospf                                         ospf_map
  ospf match: int ext1 nssa-ext2
Networks Originated:
     10.1.1.0 255.255.255.0 (active)
     20.1.1.0 255.255.255.0

Neighbors:
172.20.1.100
   Filter List In..................... 1
   Filter List Out.................... 2
   Prefix List In..................... PfxList2
   Prefix List Out.................... PfxList3
   Route Map In....................... rmapUp
   Route Map Out...................... rmapDown
172.20.5.1
   Prefix List Out.................... PfxList12

Routing Protocol...................... OSPFv2
Router ID............................. 6.6.6.6
OSPF Admin Mode....................... Enable
Maximum Paths......................... 32
Routing for Networks.................. 172.24.0.0 0.0.255.255 area 0
                                       10.0.0.0 0.255.255.255 area 1
                                       192.168.75.0 0.0.0.255 area 2
Distance.............................. Intra 110 Inter 110 Ext 110

Default Route Advertise............... Disabled
Always................................ FALSE
Metric................................ Not configured
Metric Type........................... External Type 2

Redist
Source      Metric       Metric Type     Subnets    Dist List
---------  -------       -----------     -------    ---------
static     default                2         Yes         None
connected       10                2         Yes            1

Number of Active Areas................ 3 (3 normal, 0 stub, 0 nssa)
ABR Status............................ Yes
ASBR Status........................... Yes
```

show ip route

This command displays the routing table for the specified virtual router (vrf *vrf-name*). If no router is specified, the routing table for the defualt router is displayed. The *ip-address* specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The *mask* specifies the subnet mask for the given *ip-address*. When you use the *longer-prefixes* keyword, the *ip-address* and *mask* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the *protocol* parameter to specify the protocol that installed the routes. The value for *protocol* can be *ospf, bgp, connected*, or *static*. Use the *all* parameter to display all routes including best and non-best routes. If you do not use the *all* parameter, the command only displays the best route.

Note: If you use the *connected* keyword for *protocol*, the *all* option is not available because there are no best or non-best connected routes.

Format `show ip route [vrf vrf-name] [{ip-address [protocol] | {ip-address mask [longer-prefixes] [protocol] | protocol} [all] | all}]`

Modes
- Privileged EXEC
- User EXEC

Parameter	*Definition*
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The `show ip route` command displays the routing tables in the following format:

```
Code   IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface, Truncated
```

The columns for the routing table display the following information:

Parameter	*Definition*
Code	The codes for the routing protocols that created the routes.
Default Gateway	The IP address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be • Days:Hours:Minutes if days > = 1 • Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.

Parameter	*Definition*
T	A flag appended to a route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a **T** after the interface name.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF. Reject routes are supported in OSPFv2.

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

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2, S U - Unnumbered Peer
       L-Leaked Route, K - Kernel, P - Net Prototype

C      3.0.0.0/24 [0/1] directly connected,   0/3
S U    6.1.0.6/32 [0/0] via 0/1
S U    6.2.0.6/32 [0/0] via 0/2
C      12.1.0.0/24 [0/1] directly connected,   loopback 1
C      12.2.0.0/24 [0/1] directly connected,   loopback 2
C      12.3.0.0/24 [0/1] directly connected,   loopback 3
```

Example: The following shows an example of output that displays leaked routes.

Subnetwork 9.0.0.0/24 is a connected subnetwork in global table and subnet 56.6.6.0/24 is reachable via a gateway 9.0.0.2 in the global table. These two routes leak into the virtual router *Red* and leak the connected subnet 8.0.0.0/24 from *Red* to global table.

When leaking connected route in the global routing table to a virtual router, the /32 host route for the leaked host is added in the virtual router instance's route table. Leaking of non /32 connected routes into the virtual router table from global routing table is not supported.

This enables the nodes in subnet 8.0.0.0/24 to access shared services via the global routing table. Also we add a non-leaked static route for 66.6.6.0/24 subnetwork scoped to the domain of virtual router Red.

```
(Router) (Config)#ip route vrf Red 9.0.0.2 255.255.255.255 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 56.6.6.0 255.255.255.0 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2
(Router) (Config)#ip route 8.0.0.0 255.255.255.0 0/27

(Router) #show ip route vrf Red

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
   L – Leaked Route
```

```
C      8.0.0.0/24 [0/1] directly connected,   0/27
S L    9.0.0.2/32 [1/1] directly connected,   0/26
S L    56.6.6.0/24 [1/1] via 9.0.0.2,   02d:22h:15m,  0/26
S      66.6.6.0/24 [1/1] via 8.0.0.2,   01d:22h:15m,  0/27
(Router) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
   L – Leaked Route

C      9.0.0.0/24 [0/1] directly connected,   0/26
S L    8.0.0.0/24 [1/1] directly connected,   0/27
```

Example: The following example shows routes obtained from the kernel.

```
(Routing)#show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel

C      1.1.1.0/24 [0/1] directly connected,   0/9
S      12.12.12.0/24 [1/0] via 1.1.1.2,   0/9
S      13.13.13.0/24 [1/0] via 1.1.1.2,   0/9
K      25.25.25.0/24 [1/3] via 1.1.1.2,   0/9
```

The routes obtained from the kernel can be configured to be redistributed in the kernel. The CLI command below (in both IPv4 and Pv6) BGP Router mode has the kernel option kernel.

```
(7001) (Config)#router bgp 65401

(7001) (Config-router)#redistribute ?

<cr>                    Press enter to execute the command.
connected               Configure redistribution of Connected routes
kernel                  Configure redistribution of Kernel routes
ospf                    Configure redistribution of OSPF routes
rip                     Configure redistribution of RIP routes
static                  Configure redistribution of Static routes

(7001) (Config-router)#address-family ipv6

(7001) (config-router-af)#redistribute ?

<cr>                    Press enter to execute the command.
connected               Configure redistribution of Connected routes
kernel                  Configure redistribution of Kernel routes
ospf                    Configure redistribution of OSPF routes
static                  Configure redistribution of Static routes
```

Example: The following shows an example of the output that displays with a hardware failure.

```
(Router) (Config)#interface 0/1
(Router) (Interface 0/1)#routing
(Router) (Interface 0/1)#ip address 9.0.0.1 255.255.255.0
```

```
(Router) (Interface 0/1)#exit
(Router) (Config)#ip route net-prototype 56.6.6.0/24 9.0.0.2 1
(Router) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K – Kernel
      P – Net Prototype

C      9.0.0.0/24 [0/0] directly connected,   0/1
P      56.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
```

show ip route ecmp-groups

This command reports all current ECMP groups in the IPv4 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv4 address and outgoing interface of each next hop in each group.

Format `show ip route ecmp-groups`

Mode Privileged EXEC

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

```
(router) #show ip route ecmp-groups

ECMP Group 1 with 2 next hops (used by 1 route)
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34

ECMP Group 2 with 3 next hops (used by 1 route)
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34

ECMP Group 3 with 4 next hops (used by 1 route)
  172.20.31.100 on interface 2/31
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
```

show ip route hw-failure

Use this command to display the routes that failed to be added to the hardware due to hash errors or a table full condition.

Format `show ip route hw-failure`

Mode Privileged EXEC

Example: The following example displays the command output.

```
(Routing) (Config)#ip route net-prototype 66.6.6.0/24 9.0.0.2 4

(Routing) #show ip route connected

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K – Kernel
   P – Net Prototype

C      9.0.0.0/24 [0/0] directly connected,   0/1
C      8.0.0.0/24 [0/0] directly connected,   0/2

(Routing) #show ip route hw-failure

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K – Kernel
   P – Net Prototype

P      66.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.7.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.8.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.9.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
```

show ip route net-prototype

This command displays the net-prototype routes. The net-prototype routes are displayed with a P.

Format `show ip route net-prototype`

Modes Privileged EXEC

Example:

```
(Routing) #show ip route net-prototype

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K – Kernel
       P – Net Prototype

P      56.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1
P      56.6.7.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1
```

show ip route summary

Use this command to display the routing table summary. When the optional `all` keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

Format `show ip route summary [all]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by the BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.
OSPF Routes	Total number of routes installed by OSPF protocol.
Intra Area Routes	Total number of Intra Area routes installed by OSPF protocol.
Inter Area Routes	Total number of Inter Area routes installed by OSPF protocol.

Term	*Definition*
External Type-1 Routes	Total number of External Type-1 routes installed by OSPF protocol.
External Type-2 Routes	Total number of External Type-2 routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Net Prototype Routes	The number of net-prototype routes.
Total Routes	Total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination. The value in parentheses indicates the highest count of unique best routes since counters were last cleared.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Hardware Failed Route Adds	The number of routes failed be inserted into the hardware due to hash error or a table full condition.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes. The value in parentheses indicates the highest count of unique next hops since counters were last cleared.
Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups (High)	The number of next hop groups with multiple next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.

Term	*Definition*
Routes with n Next Hops	The current number of routes with each number of next hops.

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

```
(Routing) #show ip route summary
Connected Routes.............................. 7
Static Routes................................. 1
RIP Routes.................................... 20
BGP Routes.................................... 10
  External.................................... 0
  Internal.................................... 10
  Local....................................... 0
OSPF Routes................................... 1004
  Intra Area Routes........................... 4
  Inter Area Routes........................... 1000
  External Type-1 Routes...................... 0
  External Type-2 Routes...................... 0
Reject Routes................................. 0
Net Prototype Routes.......................... 10004
Total routes.................................. 1032

Best Routes (High)............................ 1032 (1032)
Alternate Routes.............................. 0
Route Adds.................................... 1010
Route Modifies................................ 1
Route Deletes................................. 10
Unresolved Route Adds......................... 0
Invalid Route Adds............................ 0
Failed Route Adds............................. 0
Hardware Failed Route Adds.................... 4
Reserved Locals............................... 0

Unique Next Hops (High)....................... 13 (13)
Next Hop Groups (High)........................ 13 (14)
ECMP Groups (High)............................ 2 (3)
ECMP Routes................................... 1001
Truncated ECMP Routes......................... 0
ECMP Retries.................................. 0
Routes with 1 Next Hop........................ 31
Routes with 2 Next Hops....................... 1
Routes with 4 Next Hops....................... 1000
```

clear ip route counters

The command resets to zero the IPv4 routing table counters reported in the command "show ip route summary" on page 285 for the specified virtual router. If no router is specified, the command is executed for the default router. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format `clear ip route counters`

Mode Privileged EXEC

show ip route preferences

This command displays detailed information about the route preferences for each type of route. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format `show ip route preferences`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Local	The local route preference value.
Static	The static route preference value.
BGP External	The BGP external route preference value.
OSPF Intra	The OSPF Intra route preference value.
OSPF Inter	The OSPF Inter route preference value.
OSPF External	The OSPF External route preference value.
RIP	The RIP route preference value.
BGP Internal	The BGP internal route preference value.
BGP Local	The BGP local route preference value.
Configured Default Gateway	The route preference value of the statically-configured default gateway
DHCP Default Gateway	The route preference value of the default gateway learned from the DHCP server.

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

```
(alpha-stack) #show ip route preferences

Local.......................................... 0
Static......................................... 1
BGP External................................... 20
OSPF Intra..................................... 110
OSPF Inter..................................... 110
OSPF External.................................. 110
RIP............................................ 120
```

```
BGP Internal................................. 200
BGP Local.................................... 200
Configured Default Gateway................... 253
DHCP Default Gateway......................... 254
```

show ip stats

This command displays IP statistical information. for a specified virtual router instance. If a virtual router is not specified, the IP statistical information for the default router is displayed.

Format `show ip stats [vrf vrf-name]`

Modes
- Privileged EXEC
- User EXEC

show routing heap summary

This command displays a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing applications.

Format `show routing heap summary`

Mode Privileged EXEC

Parameter	*Description*
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

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

```
(Router) #show routing heap summary

Heap Size ................................... 95053184
Memory In Use ............................... 56998
Memory on Free List ......................... 47
Memory Available in Heap .................... 94996170
In Use High Water Mark ...................... 57045
```

IP Event Dampening Commands

dampening

Use this command to enable IP event dampening on a routing interface.

Format `dampening [half-life period] [reuse-threshold suppress-threshold max-suppress-time [restart restart-penalty]]`

Mode Interface Config

Parameter	*Description*
Half-life period	The number of seconds it takes for the penalty to reduce by half. The configurable range is 1-30 seconds. Default value is 5 seconds.
Reuse Threshold	The value of the penalty at which the dampened interface is restored. The configurable range is 1-20,000. Default value is 1000.
Suppress Threshold	The value of the penalty at which the interface is dampened. The configurable range is 1-20,000. Default value is 2000.
Max Suppress Time	The maximum amount of time (in seconds) an interface can be in suppressed state after it stops flapping. The configurable range is 1-255 seconds. The default value is four times of half-life period. If half-period value is allowed to default, the maximum suppress time defaults to 20 seconds.
Restart Penalty	Penalty applied to the interface after the device reloads. The configurable range is 1-20,000. Default value is 2000.

no dampening

This command disables IP event dampening on a routing interface.

Format `no dampening`

Mode Interface Config

show dampening interface

This command summarizes the number of interfaces configured with dampening and the number of interfaces being suppressed.

Format `show dampening interface`

Mode Privileged EXEC

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

```
(Router)# show dampening interface
2 interfaces are configured with dampening.
1 interface is being suppressed.
```

show interface dampening

This command displays the status and configured parameters of the interfaces configured with dampening.

Format `show interface dampening`

Mode Privileged EXEC

Parameter	*Description*
Flaps	The number times the link state of an interface changed from UP to DOWN.
Penalty	Accumulated Penalty.
Supp	Indicates if the interface is suppressed or not.
ReuseTm	Number of seconds until the interface is allowed to come up again.
HalfL	Configured half-life period.
ReuseV	Configured reuse-threshold.
SuppV	Configured suppress threshold.
MaxSTm	Configured maximum suppress time in seconds.
MaxP	Maximum possible penalty.
Restart	Configured restart penalty.

Note:

1. The CLI command "clear counters" on page 125 resets the flap count to zero.
2. The interface CLI command "no shutdown" on page 189 resets the suppressed state to `False`.
3. Any change in the dampening configuration resets the current penalty, reuse time and suppressed state to their default values, meaning `0`, `0`, and `FALSE` respectively.

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

```
Router# show interface dampening

Interface 0/2
Flaps   Penalty   Supp   ReuseTm   HalfL   ReuseV   SuppV   MaxSTm   MaxP   Restart
   0          0     FALSE      0          5        1000       2000        20        16000      0
Interface 0/3
Flaps   Penalty   Supp   ReuseTm   HalfL   ReuseV   SuppV   MaxSTm   MaxP   Restart
   6       1865     TRUE      18          20      1000       2001        30         2828     1500
```

DHCP and BOOTP Relay Commands

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

bootpdhcprelay cidoptmode

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

Default disabled

Format `bootpdhcprelay cidoptmode`

Mode
- Global Config
- Virtual Router Config

no bootpdhcprelay cidoptmode

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

Format `no bootpdhcprelay cidoptmode`

Mode
- Global Config
- Virtual Router Config

bootpdhcprelay maxhopcount

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

Default 4

Format `bootpdhcprelay maxhopcount 1-16`

Mode
- Global Config
- Virtual Router Config

no bootpdhcprelay maxhopcount

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

Format `no bootpdhcprelay maxhopcount`

Mode
- Global Config
- Virtual Router Config

bootpdhcprelay minwaittime

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

Default 0

Format `bootpdhcprelay minwaittime` *`0-100`*

Mode
- Global Config
- Virtual Router Config

no bootpdhcprelay minwaittime

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

Format `no bootpdhcprelay minwaittime`

Mode
- Global Config
- Virtual Router Config

show bootpdhcprelay

This command displays the BootP/DHCP Relay information for the virtual router. If no router is specified, information for the default router is displayed.

Format `show bootpdhcprelay [vrf` *`vrf-name`*`]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.

show ip bootpdhcprelay

This command displays BootP/DHCP Relay information.

Format `show ip bootpdhcprelay`

Modes User EXEC

Parameter	*Definition*
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit Id option, which may be enabled or disabled.

Example: The following shows an example of the command.

```
(Routing) >show ip bootpdhcprelay

Maximum Hop Count.............................. 4
Minimum Wait Time(Seconds)..................... 0
Admin Mode..................................... Disable
Circuit Id Option Mode......................... Enable
```

Section 9: DCSS Log Messages

This section lists common log messages that are provided by DCSS, along with information regarding the cause of each message. There is no specific action that can be taken per message. When there is a problem being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem) will assist ADTRAN in determining the root cause of such a problem.

Note: This chapter is not a complete list of all syslog messages.

The Log Messages chapter includes the following sections:

Core

Table 10: BSP Log Messages

Component	*Message*	*Cause*
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting DCSS application.

Table 11: NIM Log Messages

Component	*Message*	*Cause*
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	There is no mapping between the USP and Interface number.
NIM	NIM: L7_DETACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: L7_DELETE out of order for interface unit x slot x port x	Interface creation out of order.

Table 11: NIM Log Messages (Cont.)

Component	*Message*	*Cause*
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system.
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent.
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase.
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase.
NIM	NIM: Component(x) failed on event(x) for interface	A component responded with a fail indication for an interface event.
NIM	NIM: Timeout event(x), interface remainingMask = xxxx	A component did not respond before the NIM timeout occurred.

Table 12: SIM Log Message

Component	*Message*	*Cause*
SIM	IP address conflict on service port/network port for IP address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx	This message appears when an address conflict is detected in the LAN for the service port/network port IP.

Table 13: System Log Messages

Component	*Message*	*Cause*
SYSTEM	Configuration file fastpath.cfg size is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file *file name* version *version num*	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.

Table 13: System Log Messages (Cont.)

Component	*Message*	*Cause*
SYSTEM	File *filename*: same version (*version num*) but the sizes (*version size* – *expected version size*) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	Migrating config file *filename* from version *version num* to *version num*	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.
SYSTEM	Building Defaults	Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.
SYSTEM	sysapiCfgFileGet failed size = *expected size of file* version = *expected version*	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

Utilities

Table 14: Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: slot/port	An interface changed link state.

Table 15: DHCP Filtering Log Messages

Component	Message	Cause
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	Unable to create semaphore used for dhcp filtering configuration structure.
DHCP Filtering	Failed to register with nv Store.	Unable to register save and restore functions for configuration save.
DHCP Filtering	Failed to register with NIM	Unable to register with NIM for interface callback functions.
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Error on trying to save configuration.

Table 16: NVStore Log Messages

Component	Message	Cause
NVStore	Building defaults for file XXX	A component's configuration file does not exist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	File XXX corrupted from file system. Checksum mismatch.	The calculated checksum of a component's configuration file in the file system did not match the checksum of the file in memory.
NVStore	Migrating config file XXX from version Y to Z	A configuration file version mismatch was detected so a configuration file migration has started.

Table 17: LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 18: SNTP Log Message

Component	Message	Cause
SNTP	SNTP: system clock synchronized on %s UTC	Indicates that SNTP has successfully synchronized the time of the box with the server.

Table 19: DHCPv4 Client Log Messages

Component	*Message*	*Cause*
DHCP4 Client	Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt	This message appears when a message is received from the DHCP Server that contains an un-supported Vendor Option.
DHCP4 Client	Failed to acquire an IP address on xxx; DHCP Server did not respond.	This message appears when the DHCP Client fails to lease an IP address from the DHCP Server.
DHCP4 Client	DNS name server entry add failed.	This message appears when the update of a DNS Domain name server info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	DNS domain name list entry addition failed.	This message appears when the update of a DNS Domain name list info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	Interface xxx Link State is Down. Connect the port and try again.	This message appears when the Network protocol is configured with DHCP without any active links in the Management VLAN.

Management

Table 20: SNMP Log Message

Component	*Message*	*Cause*
SNMP	EDB Callback: Unit Join: x.	A new unit has joined the stack.

Table 21: EmWeb Log Messages

Component	*Message*	*Cause*
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	A user attempted to connect via telnet when the maximum number of telnet sessions were already active.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	Handle table overflow	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	*ConnectionType* EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending: EWOULDBLOCK error sending data	Socket error on send.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

Table 22: CLI_UTIL Log Messages

Component	*Message*	*Cause*
CLI_UTIL	Telnet Send Failed errno = 0x%x	Failed to send text string to the telnet client.
CLI_UTIL	osapiFsDir failed	Failed to obtain the directory information from a volume's directory.

Table 23: SSHD Log Messages

Component	*Message*	*Cause*
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent.
SSHD	SSHD: Unknown UI event in message, event = XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it's an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue.

Table 24: SSLT Log Messages

Component	*Message*	*Cause*
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.
SSLT	SSLT: Msg Queue is full, event = XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSLcertificate from specified file. XXXX indicates the file from where the certificate is being read.
SSLT	SSLT: Error loading private key from file	Failed while loading private key for SSL connection.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Failed while setting cipher list.
SSLT	SSLT: Could not delete the SSL semaphores	Failed to delete SSL semaphores during cleanup.of all resources associated with the OpenSSL Locking semaphores.

Table 25: User_Manager Log Messages

Component	Message	Cause
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX indicates the username to be authenticated.
User_Manager	Access level for user XXXX could not be determined. Setting to Level 1.	Invalid access level specified for the user. The access level is set to Level 1. XXXX indicates the username.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Failed to migrate the config file. XXXX is the config file name. YYYY is the old version number and ZZZZ is the new version number.

Switching

Table 26: 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully.

Table 27: FDB Log Message

Component	Message	Cause
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Unable to set the age time in the hardware.

Table 28: Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 29: 802.1Q Log Messages

Component	*Message*	*Cause*
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan ids. i.e. 4094 - x.
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config.
802.1Q	dtl failure when adding ports to vlan id %d - portMask = %s	Failed to add the ports to VLAN entry in hardware.
802.1Q	dtl failure when deleting ports from vlan id %d - portMask = %s	Failed to delete the ports for a VLAN entry from the hardware.
802.1Q	dtl failure when adding ports to tagged list for vlan id %d - portMask = %s	Failed to add the port to the tagged list in hardware.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d - portMask = %s"	Failed to delete the port to the tagged list from the hardware.
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x"	Failed to receive the dot1q message from dot1q message queue.
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Failed to create VLAN ID, VLAN Database reached maximum values.
802.1Q	Attempt to create a vlan (%d) that already exists	Creation of the existing Dynamic VLAN ID from the CLI.
802.1Q	DTL call to create VLAN %d failed with rc %d"	Failed to create VLAN ID in hardware.
802.1Q	Problem unrolling data for VLAN %d	Failed to delete VLAN from the VLAN database after failure of VLAN hardware creation.
802.1Q	VLan %d does not exist	Failed to delete VLAN entry.
802.1Q	VLan %d requestor type %d does not exist	Failed to delete dynamic VLAN ID if the given requestor is not valid.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Failed to delete, as some unknown component has taken the ownership.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Failed to delete the VLAN ID as the given requestor and VLAN entry status are not same.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Failed to delete VLAN ID from the hardware.
802.1Q	Problem deleting data for VLAN %d	Failed to delete VLAN ID from the VLAN database.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Failed to modify the VLAN group filter
802.1Q	Cannot find vlan %d to convert it to static	Failed to convert Dynamic VLAN to static VLAN. VLAN ID not exists.

Table 29: 802.1Q Log Messages (Cont.)

Component	*Message*	*Cause*
802.1Q	Only Dynamically created vlans can be converted	Error while trying to convert the static created VLAN ID to static.
802.1Q	Cannot modify tagging of interface %s to non existence vlan %d"	Error for a given interface sets the tagging property for all the vlans in the vlan mask.
802.1Q	Error in updating data for VLAN %d in VLAN database	Failed to add VLAN entry into VLAN database.
802.1Q	DTL call to create VLAN %d failed with rc %d	Failed to add VLAN entry in hardware.
802.1Q	Not valid permission to delete the VLAN %d	Failed to delete static VLAN ID. Invalid requestor.
802.1Q	Attempt to set access vlan with an invalid vlan id %d	Invalid VLAN ID.
802.1Q	Attempt to set access vlan with (%d) that does not exist	VLAN ID not exists.
802.1Q	VLAN create currently underway for VLAN ID %d	Creating a VLAN which is already under process of creation.
802.1Q	VLAN ID %d is already exists as static VLAN	Trying to create already existing static VLAN ID.
802.1Q	Cannot put a message on dot1q msg Queue, Returns:%d	Failed to send Dot1q message on Dot1q message Queue.
802.1Q	Invalid dot1q Interface: %s	Failed to add VLAN to a member of port.
802.1Q	Cannot set membership for user interface %s on management vlan %d	Failed to add VLAN to a member of port.
802.1Q	Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s	Incorrect tagmode for VLAN tagging.
802.1Q	Cannot set tagging for interface %d on non existent vlan %d"	The VLAN ID does not exist.
802.1Q	Cannot set tagging for interface %d which is not a member of vlan %d	Failure in Setting the tagging configuration for a interface on a range of vlan.
802.1Q	VLAN create currently underway for VLAN ID %d"	Trying to create the VLAN ID which is already under process of creation.
802.1Q	VLAN ID %d already exists	Trying to create the VLAN ID which is already exists.
802.1Q	Failed to delete, Default VLAN %d cannot be deleted	Trying to delete Default VLAN ID.
802.1Q	Failed to delete, VLAN ID %d is not a static VLAN	Trying to delete Dynamic VLAN ID from CLI.
802.1Q	Requestor %d attempted to release internal vlan %d: owned by %d	–

Table 30: 802.1S Log Messages

Component	*Message*	*Cause*
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU.
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers.

Table 31: Port Mac Locking Log Message

Component	*Message*	*Cause*
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

QoS

Table 32: ACL Log Messages

Component	*Message*	*Cause*
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	ACL *name*, rule *x*: This rule is not being logged	The ACL configuration has resulted in a requirement for more logging rules than the platform supports. The specified rule is functioning normally except for the logging action.
ACL	aclLogTask: error logging ACL rule trap for correlator *number*	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL *number*: Forced truncation of one or more rules during config migration	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Routing

Table 33: DHCP Relay Log Messages

Component	*Message*	*Cause*
DHCP relay	REQUEST hops field more than config value	The DHCP relay agent has processed a DHCP request whose HOPS field is larger than the maximum value allowed. The relay agent will not forward a message with a hop count greater than 4.
DHCP relay	Request's seconds field less than the config value	The DHCP relay agent has processed a DHCP request whose SECS field is larger than the configured minimum wait time allowed.
DHCP relay	processDhcpPacket: invalid DHCP packet type: %u\n	The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent.

Table 34: ARP Log Message

Component	*Message*	*Cause*
ARP	IP address conflict on interface xxx for IP address yyy. Conflicting host MAC address is zzz.	When an address conflict is detected for any IP address on the switch upon reception of ARP packet from another host or router.

Technologies

Table 35: ADTRAN Error Messages

Component	*Message*	*Cause*
ADTRAN	Invalid USP unit = x, slot = x, port = x	A port was not able to be translated correctly during the receive.
ADTRAN	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
ADTRAN	Failed installing mirror action - rest of the policy applied successfully	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured.
ADTRAN	Policy x does not contain rule x	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy. Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy.
ADTRAN	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x	An issue installing the policy due to a possible duplicate hash.
ADTRAN	ACL x not found in internal table	Attempting to delete a non-existent ACL.
ADTRAN	ACL internal table overflow	Attempting to add an ACL to a full table.
ADTRAN	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it’s capabilities.
ADTRAN	USL: failed to put sync response on queue	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out.
ADTRAN	USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.
ADTRAN	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.
ADTRAN	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL.
ADTRAN	USL: failed to sync stg table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn’t exist.
ADTRAN	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
ADTRAN	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
ADTRAN	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.

Table 35: ADTRAN Error Messages (Cont.)

Component	*Message*	*Cause*
ADTRAN	USL: failed to sync trunk table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
ADTRAN	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
ADTRAN	USL: failed to sync dvlan data on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	USL: failed to sync policy table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	USL: failed to sync VLAN table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI.
ADTRAN	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
ADTRAN	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
ADTRAN	Unable to insert route R/P	Route R with prefix P could not be inserted in the hardware route table. A retry will be issued.
ADTRAN	Unable to Insert host H	Host H could not be inserted in hardware host table. A retry will be issued.
ADTRAN	USL: failed to sync L3 Intf table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	USL: failed to sync L3 Host table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	USL: failed to sync L3 Route table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	USL: failed to sync initiator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
ADTRAN	USL: failed to sync terminator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.