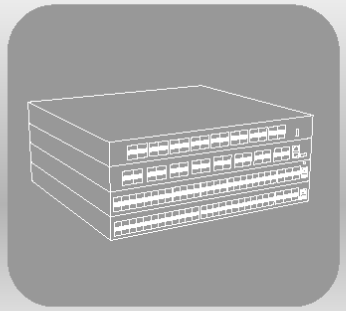
D-Link
Building Networks for People



CLI Reference Guide

Product Model : 5000 Series
Layer 2/3 Managed 10G/25G/40G/100G Data Center Switches
Release 1.00

Table of Contents

About This Guide

Objective and Audience

The Command Line Interface (CLI) used to view and configure D-LINK OS software is explained in this guide. The CLI can be accessed through the use of a direct connection to the serial port or by using telnet or SSH via a remote network connection.

The intended audience for this guide includes system administrators who use D-LINK OS software to configure and operate the systems they administer. The guide provides a comprehensive explanation of the configuration options for the D-LINK OS software.

It is assumed that readers of this guide will have an understanding of the D-LINK OS software base and will have read the appropriate specifications for the relevant networking device platform. It is further assumed that readers will have basic knowledge of Ethernet and networking concepts.

Acronyms and Abbreviations

The acronyms and abbreviations used in this guide are, in most cases, defined at their first use.

Acronym	**Expansion**
ACE	access control entry
ACL	access control list
AP	access point
API	application programming interface
APPL	application
ASIC	application-specific integrated circuit
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
C2W	WAN C2Wire
CAMP	Cooperative Asymmetric Multiprocessing
CAPI	card application program interface
CMOS	Complementary Metal Oxide Semiconductor
CPP	Control Plane Policing
CPU	central processing unit
CRC	cyclic redundancy check
CSG	Content Services Gateway
CWAN	Constellation WAN
CWPA	Constellation WAN port adapter
CWSLC	Constellation WAN SiByte Line Card1
CWTLC	Constellation WAN Toaster Line Card1
DBUS	data bus
DCM	Digital Clock Managers

Acronym	Expansion
DDR	dial-on-demand routing
DF	designated forwarder
DFC	Distributed Forwarding Card
DHCP	Dynamic Host Configuration Protocol
DIAG	diagnostic
DIP	Dual In-Line Package
dLFI	Distributed Link Fragmentation and Interleaving
dLFIoATM	Distributed Link Fragmentation and Interleaving over ATM
dLFIoFR	Distributed Link Fragmentation and Interleaving over Frame Relay
DMA	direct memory access
DOT1X	IEEE 802.1X
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
ECC	error checking and correction
EFC	Extended Flow Control
EM	Event Manager
EMD	Error Message Decoder
ENVM	environmental monitoring
EOBC	Ethernet out-of-band channel
EoMPLS	Ethernet over Multiprotocol Label Switching
EOU	Extensible Authentication Protocol over UDP
EPLD	Erasable Programmable Logic Device
ESF	Express Services Forwarding
FIB	Forwarding Information Base
FIFO	first-in, first-out
FM	Feature Manager
FPD	field-programmable device
FPGA	field-programmable gate array
GEMAC	Gigabit Ethernet Media Access Control
GEWAN	Gigabit Ethernet WAN
GSR	Gigabit Switch Router
HA	high availability
HSRP	Hot Standby Router Protocol
I/O	input/output
ICDM	Inter-CPU Data Mover

Acronym	Expansion
IDB	interface description block
IDPROM	identification programmable read-only memory
IGMP	Internet Group Management Protocol
IOS	Internet Operating System
IP	Internet Protocol
IPC	InterProcessor Communication
IPNAT	IP Network Address Translation
KPA	keepalive
L2	Layer 2
L3	Layer 3
L3MM	Layer 3 Mobility Manager
LAN	local-area network
LI	Lawful Intercept
LTL	Local Target Logic
MAC	Media Access Control
MCAST	Multicast
MD5	message digest 5
MET	Multicast Expansion Table
MFIB	Multicast Forwarding Information Base
MIB	Management Information Base
MII	media-independent interface
MLD	message loading device
MLS	Multilayer Switching
MLSM	multi-layer switching for multicast
MMI	Modem Management Interface
MMLS	Multicast Multilayer Switching
MN	mobile node
MPPE	Microsoft Point-to-Point Encryption
MRIB	Multicast Routing Information Base
MSFC	Multilayer Switch Feature Card
MTU	maximum transmission unit
NAT	Network Address Translation
OAL	Optimized ACL Logging
OIF	output interface
OIR	online insertion and removal

Acronym	Expansion
OSM	Optical Services Module
PBI	Programmable Binary Image
PCI	Peripheral Component Interconnect
PFC	Policy Feature Card
PFINIT	platform initialization
PFREDUN	platform redundancy
PIM	Protocol Independent Multicast
PIMSN	Protocol Independent Multicast Snooping
PISA	Programmable Intelligent Services Accelerator
PLIM	Physical Layer Interface Module
PM	port manager
PoS	Packet over SONET
POSLC	Packet over SONET Line Card1
PVLAN	private VLAN
PXF	Parallel Express Forwarding
QDR	Quad Data Rate
QinQ	IEEE 802.1Q in 802.1Q
QM	quality of service management
QoS	quality of service
RACL	router access control list
RADIUS	Remote Authentication Dial-In User Service
RF	redundancy feature
ROM	read-only memory
ROMMON	read-only memory monitor
RP	route processor
RPC	Remote Procedure Call
RPF	Reverse Path Forwarding
RPR	route processor redundancy
RTC	Real-Time Clock
SCP	Switch-Module Configuration Protocol
SIP	SPA Interface Processor
SMbus	system management bus
SMSC	short message service center
SP	switch processor
SPA	Shared Port Adapter

Acronym	Expansion
SPAN	Switched Port Analyzer
SRP	Spatial Reuse Protocol
SSA	Super Santa Ana ASIC
SSO	Stateful Switchover
SSP	State Synchronization Protocol Manager
SSRAM	synchronous static RAM
STAPL	Standard Test and Programming Language
SVI	switched virtual interface
SW	software
TBI	Ten Bit Interface
TCAM	ternary content addressable memory
TCP	Transmission Control Protocol
TFIB	Tag Forwarding Information Base
ToS	type of service
UDP	User Datagram Protocol
URLF	URL Filtering
VACL	VLAN access control list
VC	virtual circuit
VCD	virtual circuit descriptor
VLAN	Virtual LAN
VLOU	Virtual Logic Operation Unit
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPNSM	Virtual Private Network Services Module
VRF	VPN routing and forwarding
VSA	vendor-specific attribute
VTMS	Versatile Traffic Management and Shaping
VTP	VLAN Trunking Protocol
VTT	voltage termination
WAN	wide-area network
WCCP	Web Cache Communication Protocol

Guide Conventions

This guide makes use of the following conventions:

Convention	Description
Bold	Indicates user inputs and actions: for example, type **exit**, click **OK**, press **Alt+C**
`Monospace`	Indicates code: for example, `#include <iostream>` Indicates command-line commands and command outputs: for example, `(Routing)# show sysinfo`
`Monospace italic`	Indicates command variables: for example, `interface vlan vLan-id`
{ }	Indicates mutually exclusive command line parameters: for example, `network protocol {none I bootp I dhcp}`
[ ]	Indicates *optional* command-line parameters: for example, `write memory [confirm]`

1. About D-LINK OS Software

About D-LINK OS Software

The two primary purposes of the D-Link OS are as follows:

- To support the attached hardware in switching frames according to the Layer 2, 3, or 4 information contained in the frames.
- To provide network administrators with a complete device management portfolio.

Product Concept

The evolution of fast Ethernet and Gigabit Ethernet switching from high-end backbone applications to desktop switching applications is ongoing. At the same time, the cost of this technology continues to fall, even as its performance and feature sets continue to be enhanced. Relatedly, there is an increasing demand for devices that can switch Layers 2, 3, and 4, and D-LINK OS software offers a highly adaptable solution for these constantly increasing demands.

For each networking device on which the D-LINK OS software base runs, the exact functionality provided by the device will vary according to the platform used and the requirements of the D-LINK OS software.

The D-LINK OS software comes equipped with a comprehensive set of management functions that can be used to manage both the D-LINK OS software itself and the network. More specifically, the D-LINK OS software can be managed via either of the following methods:

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

Both of these D-LINK OS management options allow the user to control, configure, and otherwise manage the software locally or using in-band or out-of-band mechanisms. The management is standards-based, with a private MIB and specific configuration parameters allowing for control of functions not completely specified in the MIBs.

2. Using the Command-Line

The command-line interface (CLI) constitutes a text-based means by which to monitor and manage the system. The CLI can be accessed by the use of a direct serial connection or through the used of a remote logical connection via telnet or SSH.

Command Syntax

A command consists of one or more words. A given command may or may not be followed by one or more parameters, as parameters may be required or optional depending on the command being used.

For example, the commands `network` and `clear vlan` do not require parameters, whereas other commands, such as `network parms`, require that a value is included after the command. Such parameter values must be typed in a specific order, with any optional parameters following any required parameters. The following example illustrates the command syntax for the `network parms` command:

`network parms ipaddr netmask [gateway]`

- The term `network parms` is the name of the command itself.
- The terms `ipaddr` and `netmask` are parameters and are examples of required values that must be entered after the command itself are entered.
- The term `[gateway]` is an optional parameter, meaning that it is not required that a value be entered in place of the parameter.

Each command is listed by the command name in the *CLI Command Reference*, which also provides a brief description of each command.

The command keywords and the associated required and optional parameters are shown under Format.

The command mode used must be in to access the command is indicated under Mode.

The default value for a configurable setting on the device, if any, is indicated by Default.

Furthermore, the information that a given command shows is described by the `show` command.

Command Conventions

For a given command, the parameters used may include mandatory values, optional values, or keyword choices. Such parameters follow a prescribed order. Table 1 explains the conventions used in this guide to distinguish between value types.

Table 1: Parameter Conventions

Symbol	Example	Description
[] Brackets	`[value]`	Denotes an optional parameter.
Italic font in a parameter	*value* or *[value]*	Denotes a variable value. You must substitute the italicized text and brackets with an appropriate value, such as a name or number.
{} Braces	`{choice1 | choice2}`	Indicates a parameter selection option.
| Vertical bars	`choice1 | choice2`	Separates mutually exclusive choices.
[{}] Braces within brackets	`[{choicel | choice2}]`	Denotes a choice within an optional

Symbol	Example	Description
		element.

Common Parameter Values

The values for parameters might be names (strings) or numbers. Enclose the name value in double quotes in order to use spaces as part of a name parameter. For example, using the expression “System Name with Spaces” requires the system to accept the spaces, while the use of empty strings (“”) is not valid for user-defined strings. Table 2 explains common parameter values and value formatting.

Table 2: Parameter Descriptions

Parameter	Description

ipaddr	This parameter constitutes a valid IP address. The IP address can be entered 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)`
	Besides these formats, the CLI also accepts decimal, hexadecimal, and octal formats in the following input formats (where *n* consists of any valid hexadecimal, octal, or decimal number):
	`0xn (CLI assumes hexadecimal format.)`
	`0x (CLI assumes octal format with leading zeros.)`
	`n (CLI assumes decimal format.)`

Interface or `slot/port`	Used to indicate a valid slot and port number separated by a forward slash. For example, 0/1 denotes slot number 0 and port number 1.
Logical Interface	Indicates a logical slot and port number. This applies in the case of a port-channel (LAG). The logical slot/port can be used to configure the port-channel.
Character strings	Double quotation marks are used to identify character strings, e.g., “System Name with Spaces”. An empty string (“”) will not be considered valid.

Slot/Port Naming Convention

In referencing physical entities such as cards and ports, the D-LINK OS software uses a slot/port naming convention. This convention is also used by the software to identify certain logical entities, such as Port-Channel interfaces.

There are two uses for the slot number. With respect to physical ports, it indicates the card containing the ports. With respect to logical and CPU ports, it also indicates the type of interface or port.

Table 3: Types of Slot Numbers

Slot Type	Description
Physical slot numbers	Physical slot numbers start with zero, and are assinged up to the maximum number of physical slots.

Slot Type	Description
Logical slot numbers	Logical slots numbers are given immediately after physical slot numbers and identify port-channel (LAG) or router interfaces. The values for logical slot numbers are dependent upon the type of logical interface and can differ from platform to platform.
CPU slot numbers	The CPU slot numbers are given immediately after the logical slot numbers.

For a given slot, the port refers to the specific physical port or logical interface being managed on the slot.

Table 4: Types of Ports

Port Type	Description
Physical Ports	Starting from zero, the physical ports for each slot are numbered in sequence.
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces consist of logical interfaces that are used for bridging functions only. VLAN routing interfaces consist of logical interfaces that are used for routing functions only. Loopback interfaces consist of logical interfaces that are constantly up. Tunnel interfaces consist of logical point-to-point links in which encapsulated packets are carried.
CPU ports	CPU ports consist of ports that are handled by the driver and are physical entities that are located in physical slots.

Note: In the CLI itself, the `slot/port` format is not used for loopback interfaces. Use the loopback ID instead to specify a loopback interface.

Using the No Form of a Command

The `no` keyword is used to form the negative form of an existing command and is not a new or distinct command itself. A `no` form exists for almost every configuration command. in general, the `no` form of a command is used to reverse the action of the command or to reset a given value back to its default. For example, the `no` shutdown configuration command is used to reverse the shutdown of an interface. Alternatively, a given command can be used without the `no` keyword to reenable a previously disabled feature or to enable a feature that is disabled by default. The `no` form is only available for the configuration commands.

Executing Show Commands

Any mode (Global Config, VLAN Config, etc.) can be used to issue all show commands. These commands are used to obtain information about the system and its feature-specific configuration, status, and statistics.

CLI Output Filtering

In many cases, CLI show commands will cause a considerable amount of content to be displayed to the user. Such large amounts of content can be confusing and cumbersome to parse through to locate the desired information. However, by using the CLI Output Filtering feature, the user can, when executing CLI show display commands, optionally specify arguments in order to filter the CLI output so that only the desired information is displayed. The displayed information will thus be simplified, making it easier for the user to find the desired information.

The primary functions of the CLI Output Filtering feature are as follows:

- Pagination Control
  - For all **show** CLI commands, supports the enabling/disabling of paginated output. When disabled, the requested output is displayed in its entirety. When enabled, the requested output is displayed in a page-by-page manner such that the display does not scroll beyond the end of the screen until the user presses a key to continue. The options --More-- or (q)uit are displayed at the end of each page.
  - If pagination is enabled, pressing the return key will advance the display by a single line, pressing q or Q will cause the pagination to stop, and pressing any other key will advance the display by a whole page. No other configuring of these keys is possible.

Note: Although pagination is already supported by some D-LINK OS **show** commands, its implementation is unique per command rather than being generic to all commands.

- Output Filtering
  - “Grep”-like control used to modify the displayed output to show only the user-desired content.
    - Filter the displayed output to include only those lines containing a specified string match.
    - Filter the displayed output to omit only those lines containing a specified string match.
    - Filter the displayed output to include only those lines including and following a specified string match.
    - Filter the displayed output to include only a specified section of the content (e.g., “interface 0/1”) using a configurable end-of-section delimiter.
    - String matching should be case insensitive.
    - When enable, pagination also applies to filtered output.

Example

The following provides some examples of the extensions made to the CLI show.

```
show running-show config ?
<cr>                      Press enter to execute the command.
|                         Output filter options.
<scriptname>              Script file name for writing active configuration.
all                       Show all the running configuration on the switch.
interface                 Display the running config for specified interface on
                          the switch.
```

3. D-LINK OS Modules

The D-LINK OS software is composed of flexible modules that can be utilized in a variety of combinations in order to support advanced Layer 2/3/4 products. The installed modules determine the commands and command modes available on your switch. Additionally, please note that the output fields for some show commands might change depending upon the modules included in the D-LINK OS software.

The following modules are included in the D-LINK OS software suite:

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

Command Modes

Commands are grouped by the CLI into modes according to the command function, with specific D-LINK OS software commands being supported by each of the command modes. As such, the commands for a given mode are not available until the user switches to that particular mode, with the exception of the commands for the User EXEC mode. The User EXEC mode commands can also be executed in the Privileged EXEC mode.

To help the user identify the current mode, the command prompt changes for each different command mode. The command modes and the prompts for each mode are shown in Table 5.

Note: The installed sotware modules determine which command modes are available on your switch. For example, if a switch does not support the BGPV4 module, then the BGPv4 Router Command Mode will not be available.

Table 5: CLI Command Modes

Command Mode	Prompt	Mode Description
User EXEC	`Switch>`	Allows a limited set of commands used to view basic system information.
Privileged EXEC	`Switch#`	Allows the user to issue any EXEC command, to enter the VLAN mode, or to enter the Global Configuration mode.
Global Config	`Switch (Config)#`	Groups general setup commands and permits modifications to be made 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)#`
		Used to manage the operation of an interface by providing access to the router interface configuration commands.
		This mode can be used to set up a physical port for a specific logical connection operation.

Command Mode	Prompt	Mode Description

	`Switch (Interface Loopback id)#`
	`Switch (Interface tunnel id)#`
	`Switch (Interface slot/port (startrange - slot/port (endrange))#`
		This mode can also be used 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 is displayed as follows:
		(Routing) (Interface 0/2-0/4)#

Line Console	`Switch (config-line)#`	Includes commands that can be used to configure outbound telnet settings and console login/enable authentication, as well as to configure console interface settings.
Line SSH	`Switch (config-ssh)#`	Includes commands that can be used to configure SSH login/enable authentication.
Line Telnet	`Switch (config-telnet)#`	Includes commands that can be used to configure telnet login/enable authentication.
AAA IAS User Config	`Switch (config-IAS-User)#`	Includes commands that can be used to configure a password for a user in the IAS database.
Mail Server	`Switch (Mail-Server)#`	Includes commands that can be used to configure the e-mail server.
Class Map Config	`Switch (config-class-map)#`	Includes the commands for QoS class map configuration for IPv4.
Router OSPF Config	`Switch (config-router)#`	Includes the commands for OSPF configuration.
BGP Router Config	`Switch (config-router)#`	Includes the commands for BGP4 configuration.
IPv6 Address Family	`Switch (config-router-af)#`	Includes the commands for IPv6 address family configuration.
Radius Dynamic Authorization Config	`Switch (config-radius-da)#`	Includes the commands for Radius Dynamic Authorization.
MAC Access-list Config	`Switch (Config-mac-access-list)#`	Includes the commands for creating a MAC Access-List and allows the user to enter the mode containing the MAC Access-List configuration commands.
|Pv6 Access-list Config	`Switch (config-ipv6-acl)#`	Includes the commands for creating an IPv6 Access-List and allows the user to enter the mode containing the IPv6 Access-List configuration commands.
Management Access-list Config	`Switch (config-macal)#`	Includes the commands for creating a Management Access-List and allows the user to enter the mode containing the Management Access-List configuration commands.

Command Mode	Prompt	Mode Description
TACACS+ Config	`Switch (Tacacs)#`	Includes the commands for configuring the properties of the TACACS+ servers.
ARP Access-List Config Mode	`Switch (Config-arp-access-list)#`	Includes the commands used to add ARPACL rules in an ARP Access List.
Usergroup Configuration Mode	`Switch (config-usergroup)`	Includes the user group commands.
Taskgroup Configuration Mode	`Switch (config-taskgroup)`	Includes the task group commands.

Table 6 shows the input or inputs used to enter each mode. Alternatively, input the term exit to exit a given mode and return to the previous mode. However, press Ctrl+z to exit the Privileged EXEC mode.

Note: Entering Ctrl+z when in the Privileged EXEC mode will result in exiting to the User EXEC mode. Enter Logout if you wish to exit the User EXEC mode.

Table 6: CLI Mode Access and Exit

Command Mode	Access Method
User EXEC	The first level of access.
Privileged EXEC	Enter `enable` while in the User EXEC mode.
Global Config	Enter `configure` while in the Privileged EXEC mode.
VLAN Config	Enter vlan database while in the Privileged EXEC mode.

Interface Config	Enter one of the following terms while the Global Config mode:
	`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	Enter `line console` while in the Global Config mode.
Line SSH	Enter `line ssh` while in the Global Config mode.
Line Telnet	Enter `line telnet` while in the Global Config mode.
AAA IAS User Config	Enter while in the Global Config mode.
Mail Server Config	Enter `mail-server address` while in the Global Config mode.
Policy-Map Config	Enter `policy-map <policy-name> direction>` while in the Global Config mode.

Command Mode	Access Method
Policy-Class-Map Config	Enter `class <classname>` while in the Policy Map mode. **Note:** A given classname should be created using the `class-map` command.
Class-Map Config	Enter `class-map match-all <class-map-name>` while in the Global Config mode, and then use either the optional keyword `ipv4` or `ipv6` to specify the Layer 3 protocol for this class.
Router OSPF Config	Enter `router ospf` while in the Global Config mode.
BGP Router Config	Enter `router bgp asnumber` while in the Global Config mode.
Route Map Config	Enter `route-map` *`map-tag`* while in the Global Config mode.
IPv6 Address Family Config	Enter `address-family ipv6` while in the BGP Router Config mode,.
Peer Template Config	Enter `template peer name` while in the BGP Router Config mode to create a BGP peer template and to enter the Peer Template Configuration mode.
Peer Template Address Family Config	Enter `address-family {ipv4 | ipv6)` while in the Peer Template Config mode.
MAC Access-list Config	Enter `mac access-list extended name` while in the Global Config mode.
IPv6 Access-list Config	Enter `ipv6 access-list` *`name`* while in the Global Config mode.
Management Access-list Config	Enter `management access-list` *`name`* while in the Global Config mode.
TACACS+ Config	Enter `tacacs-server host ip-addr`, where `ip-addr` is the IP address of the TACACS+ server on your network, while in the Global Config mode.
ARP Access-List Config	Enter the `arp access-list` command while in the Global Config mode.
User-Group Configuration Mode	Enter the `usergroup <`*`usergroup-name`*`>` command while in the Global Config mode.
Task-Group Configuration Mode	Enter the `taskgroup <`*`taskgroup-name`*`>` command while in the Global Config mode.

Command Completion and Abbreviation

When the user types enough letters of a command to uniquely identify the command keyword, the command completion feature finishes spelling the command for the user. Once the user has entered enough letters, simply pressing the SPACEBAR or TAB key will complete the word.

Command abbreviation lets the user execute a command when the user has entered enough letters to uniquely identify the command. The user must, however, enter all of the required parameters and keywords before entering the command.

CLI Error Messages

If a command is entered by the user and the system cannot execute it, an error message will appear. Table 7 provides a list of the most common CLI error messages.

Table 7:CLI Error Messages

Message Text	Description
% Invalid input detected at '^' marker.	Indicates that an incorrect or unavailable command was entered. The carat (^) indicates the location of the invalid text. This message will also appear if any of the values or parameters is not recognized.
Command not found / Incomplete command. Use ? to list commands	Indicates that the required keywords or values were not entered.
Ambiguous command	Indicates that not enough letters were entered to uniquely identify the command.

CLI Line-Editing Conventions

Table 8 provides a list of the key combinations that can be used to edit commands or raise the speed of command entry. This list can be accessed from the CLI by entering help while in the User or Privileged EXEC modes.

Table 8: CLI Editing Conventions

Key Sequence	Description
DEL or Backspace	Deletes previous character.
Ctrl-A	Moves cursor to beginning of line.
Ctrl-E	Moves cursor to end of line.
Ctrl-F	Moves cursor forward one character.
Ctrl-B	Moves cursor backward one character.
Ctrl-D	Deletes current character.
Ctrl-U, X	Deletes text back to beginning of line.
Ctrl-K	Deletes text to end of line.
Ctrl-W	Deletes previous word.
Ctrl-T	Transposes previous character.
Ctrl-P	Takes user to previous line in history buffer.
Ctrl-R	Rewrites or pastes the current line.
Ctrl-N	Takes user to next line in history buffer.
Ctrl-Y	Prints last deleted character.
Ctrl-Q	Enables serial flow.
Ctrl-S	Disables serial flow.

Key Sequence	Description
Ctrl-Z	Returns user to root command prompt.
Tab, <SPACE>	Yields command-line completion.
Exit	Returns user to next lower command prompt.
?	Opens list of available commands, keywords, or parameters.

Using CLI Help

To display the commands available in the current mode, enter a question mark (?) at the command prompt.

```
(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.
```

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

```
(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.
```

In the event that the help output displays a parameter in angled brackets, you must replace the parameter with an appropriate value.

```
(Routing) #network parms ?

<ipaddr>            Enter the IP address.
```

In the event that there are no other command keywords or parameters, or in the event that any additional parameters are optional, the following message will appear in the output:

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

A question mark (?) may also be entered after the user types one or more characters of a word should the user wish to see a list of the available commands or parameters that begin with the letter(s)s, as shown in the following example:

```
(Routing) #show m?

Mac-addr-table      mac-address-t       monitor
```

Accessing the CLI

The CLI can be accessed through a direct console connection or through a telnet or SSH connection from a remote management host.

For the initial connection, a direct connection to the console port must be used. The system cannot be accessed remotely until it has been assigned an IP address, subnet mask, and default gateway. The network configuration information can be set manually, or the user can configure the system to allow these settings to be made from a BOOTP or DHCP server on the network. Please see “Network Interface Commands” for more information.

4. Management Commands

This section provides descriptions of the following management commands for the D-LINK OS CLI:

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

- Show commands, which are commands that display switch settings, statistics, and other information.
- Configuration commands, which are commands that can be used to configure the features and options of the switch. Please note that, for every configuration command, there is a corresponding show command that shows the configuration setting.
- Clear commands, which are commands clear some or all of the user-applied settings, returning the configurations to factory defaults.

Network Interface Commands

The commands used to configure a logical interface for management access are described in this section. Please see "network mgmt_vlan" for information on how to configure the management VLAN.

4-1 enable (Privileged EXEC access)

This command provides the user with access to the Privileged EXEC mode. From the Privileged EXEC mode, the network interface can be configured.

enable

Parameters

None

Default

The default is None.

Command Mode

User EXEC

4-2 do (Privileged EXEC) commands

This command causes Privileged EXEC mode commands to be executed from any of the configuration modes.

do *Priv Exec Mode Command*

Parameters

None

Default

The default is None.

Command Mode

- Global Config
- Interface Config
- VLAN Config
- Router Config

Example

The following provides an example of the **do** command that is used to execute the Privileged EXEC command **script list** while in the 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)#
```

4-3 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).

serviceport ip { *ipaddr netmask* **[***gateway***] | none}**

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

4-4 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.

serviceport protocol {none | bootp | dhcp}

Parameters

None

Default

The default is DHCP.

Command Mode

Privileged EXEC

4-5 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).

serviceport protocol dhcp [client-id]

Parameters

None

Default

The default is DHCP.

Command Mode

Privileged EXEC

Usage Guideline

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 command.

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

4-6 network parms

This command is used to set the IP address, subnet mask, and gateway of the device. It is required that the IP address and the gateway be located on the same subnet. The none option can be specified in order to clear the IPv4 address and mask, as well as the default gateway (i.e., each of the values will be reset to the default value on the switch).

network parms {*ipaddr netmask* **[***gateway***] I none)}**

Parameters

ipaddr	Enter the summary address designated for a range of addresses here.
netmask	Enter the IP subnet mask used for the summary route here.
gateway	(Optional) Enter the gateway address used for the summary route here.

Default

The default is None.

Command Mode

Privileged EXEC

4-7 network protocol

This command is used to specify the network configuration protocol to be utilized. If the user modifies this value, the change becomes effective immediately. If the ***bootp*** parameter is used, the switch sends requests to a BOOTP server on a periodic basis until a response is received. If the ***DHCP*** parameter is used, the switch sends requests to a DHCP server on a periodic basis until a response is received. If the ***none*** parameter is used, the network information for the switch must be configured manually.

network protocol {none | bootp | dhcp}

Parameters

none	No specified network information is set.
bootp	Specifies the static BOOTP server for packet requests.
dhcp	Specifies the DHCP server for packet requests.

Default

The default is DHCP.

Command Mode

Privileged EXEC

4-8 network protocol dhcp

This command is used to enable the DHCPv4 client on a Network port and, if used with the client identifier option (DHCP Option 61), sends DHCP client messages.

network protocol dhcp [client-id]

Parameters

client-id	(Optional) Specifies a DHCP client identifier in hexadecimal notation

Default

The default is None.

Command Mode

Global Config

Usage Guideline

The **no** form of the command **network protocol dhcp client-id** is not supported. Therefore, issue the command **network protocol dhcp** without the **client-id** option in order to remove the **client-id** option from the DHCP client messages. In addition, the user may use the command **network protocol none** to disable the DHCP client and client-id option on the interface.

Example

The following provides an example of the command.

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

4-9 show network

This command is used to show the configuration settings associated with the network interface of the switch. Please note that the network interface is the logical interface that is used to provide the switch with in-band connectivity via any of the switch's front panel ports. Also note that the configuration of the front panel ports through which traffic is switched or routed is not affected by the configuration parameters associated with the switch's network interface. Regardless of whether or not any member ports are up, the network interface is always considered to be up; as such, the **show network** command will always display the **Interface Status** as up.

show network

Parameters

None

Default

The default is None.

Command Mode

Global Config

Example

The following provides an example of a 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......................10.259.3.3
IPv6 Administrative Mode.............Enabled
Burned In MAC Address................00:05:64:2F:0D:E5
MAC Address Type.....................Burned In
Configured IPv4 Protocol.............None
Configured IPv6 Protocol.............None
IPv6 AutoConfig Mode.................Disabled
Management VLAN ID...................1
```

Display Parameters

Interface Status	Indicates the network interface status; it is always considered to be “up”.
IP Address	Indicates the IP address (default: 10.90.90.90/8) for the given interface.
Subnet Mask	Indicates the IP subnet/mask for the given interface.
Default Gateway	Indicates the default gateway for the given IP interface.
IPv6 Administrative Mode	Indicates whether the IPv6 Administrative Mode is enabled or disabled.
IPv6 Address/Length	Indicates the IPv6 address and length.
IPv6 Default Router	Indicates the IPv6 default router address.
Burned In MAC Address	Indicates the burned in MAC address utilized for in-band connectivity.

Configured IPv4 Protocol	Indicates the designated IPv4 network protocol (bootp | DHCP | none).
Configured IPv6 Protocol	Indicates the IPv6 network protocol being utilized. The options for this parameter are DHCP | none.
IPv6 Autoconfig Mode	Indicates whether the IPv6 Stateless address autoconfiguration is enabled or disabled.
Management VLAN ID	The management VLAN ID associated with the management IP address. So user can access the switch via this IP address of this VLAN.

4-10 show serviceport

This command is used to display the service port configuration information.

show serviceport

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following provides an example of the 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
Configured IPv4 Protocol.............DHCP
Configured IPv6 Protocol.............DHCP
IPv6 Autoconfig Mode.................Disabled
Burned In MAC Address................00:10:18:82:06:4D
DHCP Client Identifier...............0D-LINKOS-0010.1882.160C
```

Display Parameters

Interface Status	Indicates the network interface status; it is always considered to be “up”.

IP Address	Indicates the IP address for the given interface. The default IP address is 192.168.0.1/24.
Subnet Mask	Indicates the IP subnet/mask for the given interface.
Default Gateway	Indicates the default gateway for the given IP interface.
IPv6 Administrative Mode	Indicates whether the IPv6 Administrative Mode is enabled or disabled.
Configured IPv4 Protocol	Indicates the IPv4 network protocol being utilized. The options for this parameter are bootp | DHCP | none.
Configured IPv6 Protocol	Indicates The IPv6 network protocol being utilized. The options for this parameter are DHCP | none.
IPv6 Autoconfig Mode	Indicates whether IPv6 Stateless address autoconfiguration is enabled or disabled.
Burned In MAC Address	Indicates the burned in MAC address utilized for in-band connectivity.
DHCP Client Identifier	Only in the event that DHCP is enabled with the **client-id** option on the network port, the client identifier will be displayed in the output of the command. For more information, please see "network protocol dhcp".

IPv6 Management Commands

IPv6 management commands are used to manage a device via an IPv6 address in a switch or via IPv4 routing (i.e., independent from the IPv6 Routing package). For Routing/IPv6 builds of D-LINK OS dual IPv4/IPv6, operation over the service port is enabled. D-LINK OS has the following capabilities:

- The IPv6 addresses and gateways for the service/network ports can be statically assigned.
- An IPv6 link-local address can be pinged over the service/network port.
- Using IPv6 Management commands, SNMP traps and queries can be sent by the user via the service/network port.
- A device can be managed by the user via the network port (as well as via a Routing Interface or the Service port).

4-11 serviceport ipv6 enable

This command is used to enable IPv6 operation on the service port if it has been disabled. However, please note that IPv6 operation is, by default, enabled on the service port.

The **no** command can be used to disable IPv6 operation on the service port.

serviceport ipv6 enable

no serviceport ipv6 enable

Parameters

None

Default

The default is Enabled.

Command Mode

Privileged EXEC

4-12 network ipv6 enable

This command is used to enable IPv6 operation on the network port if it has been disabled. However, please note that IPv6 operation is, by default, enabled on the network port.

The **no** command can be used to disable IPv6 operation on the network port.

network ipv6 enable

no network ipv6 enable

Parameters

None

Default

The default is Enabled.

Command Mode

Privileged EXEC

4-13 serviceport ipv6 address

When working with the service port, the options of this command can be used to configure the IPv6 global address manually, to enable/disable stateless global address autoconfiguration, and to enable/disable DHCPv6 client protocol information on the port.

The **no** command can be used to remove any configured IPv6 prefixes on the service port interface. When used with the address option, the command removes the manually configured IPv6 global address on the network port interface. The command can also be used with the autoconfig option in order to disable the stateless global address autoconfiguration on the service port. Finally, the command can also be used with the DHCP option to in order disable the DHCPv6 client protocol on the service port.

Note: It is possible to configure multiple IPv6 prefixes on the service port.

serviceport ipv6 address { *prefix**/**prefix-length* **[eui64] | autoconfig | dhcp }**

no serviceport ipv6 address { *prefix**/**prefix-length* **[eui64] | autoconfig | dhcp }**

Parameters

prefix/prefix-length	Indicates the IPv6 prefix length value.
autoconfig	Used to configure the stateless global address autoconfiguration capability.
dhcp	Used to configure the DHCPv6 client protocol.

Default

The default is None.

Command Mode

Privileged EXEC

4-14 serviceport ipv6 gateway

This command is used to configure the IPv6 gateway (i.e. default router) information for the service port.

The **no** command is used to remove IPv6 gateways on the service port interface.

Note: For the service port, only a single IPv6 gateway address can be configured. It is possible for there to be a combination of explicitly configured IPv6 prefixes and gateways and IPv6 prefixes and gateways that are set through auto-address configuration via a connected IP router on their service port interface.

serviceport ipv6 gateway *gateway-address*

no serviceport ipv6 gateway

Parameters

gateway-address	Indicates the gateway address in the IPv6 global or link-local address format.

Default

The default is None.

Command Mode

Privileged EXEC

4-15 serviceport ipv6 neighbor

This command is used for the manual addition of IPv6 neighbors to the IPv6 neighbor table for the service port. The entry is automatically converted to a static entry if an IPv6 neighbor already exists in the neighbor table. Also, the neighbor discovery process does not result in static entries being modified. Such entries are, however, treated in the same manner for IPv6 forwarding. Furthermore, when the corresponding interface is operationally active, static IPv6 neighbor entries are applied to both the kernel stack and to the hardware.

The **no** command is used for the removal of IPv6 neighbors from the IPv6 neighbor table for the service port.

serviceport ipv6 neighbor *ipv6-address macaddr*

no serviceport ipv6 neighbor *ipv6-address macaddr*

Parameters

ipv6-address	Indicates the IPv6 address of the neighbor or interface.

Default

The default is None.

Command Mode

Privileged EXEC

4-16 network ipv6 neighbor

This command is used for the manual addition of IPv6 neighbors to the IPv6 neighbor table for this network port. The entry is automatically converted to a static entry if an IPv6 neighbor already exists in the neighbor table. Also, the neighbor discovery process does not result in static entries being modified. Such entries are, however, treated in the same manner for IPv6 forwarding. Furthermore, when the corresponding interface is operationally active, static IPv6 neighbor entries are applied to both the kernel stack and to the hardware.

The **no** command is used for the removal of IPv6 neighbors from the neighbor table.

network ipv6 neighbor *ipv6-address macaddr*

no network ipv6 neighbor *ipv6-address macaddr*

Parameters

ipv6-address	Indicates the IPv6 address of the neighbor or interface.

Default

The default is None.

Command Mode

Privileged EXEC

4-17 network ipv6 address

When working with the network port, the options of this command can be used to configure the IPv6 global address manually, to enable/disable stateless global address autoconfiguration, and to enable/disable DHCPv6 client protocol information on the port. It is possible to configure multiple IPv6 addresses on the network port.

The **no** command can be used to remove any configured IPv6 prefixes. When used with the address option, the command removes the manually configured IPv6 global address on the network port interface The command can also be used with the **autoconfig** option in order to disable the stateless global address autoconfiguration on the network port. Finally, the command can also be used with the **DHCP** option in order to disable the DHCPv6 client protocol on the network port.

network ipv6 address {*prefixs***|***prefix-length* **[eui64] | autoconfig | dhcp}**

no network ipv6 address {*prefix***|***prefix-length* **[eui64] | autoconfig | dhcp}**

Parameters

Prefix/prefix-length	Indicates the IPv6 prefix length value.
autoconfig	Used to configure the stateless global address autoconfiguration capability.
dhcp	Used to configure the DHCPv6 client protocol.

Default

The default is None.

Command Mode

Privileged EXEC

4-18 network ipv6 gateway

This command is used to configure the IPv6 gateway (i.e. default routers) information for the network port.

The **no** command is used to remove IPv6 gateways on the network port interface.

network ipv6 gateway *gateway-address*

no network ipv6 gateway

Parameters

gateway-address	Gateway global or link-local address in IPv6 format.

Default

The default is None.

Command Mode

Privileged EXEC

4-19 show network ipv6 neighbors

This command is used to show information regarding the IPv6 neighbor entries cached on the network port. The information is updated in order to display the type of the entry.

show network ipv6 neighbors

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following provides an example of the command

```
(Routing) #show network ipv6 neighbors

                                                                  Neighbor Age
IPv6 Address              Type      MAC Address         isRtr     State    (Secs)
------------------------  --------- -----               --------- -----    -------
FE80::5E26:AFF:FEBD:852C  Dynamic   5c:26:0a:bd:85:2c   True       Stale   3
```

Display Parameters

IPv6 Address	Indicates the IPv6 address of the neighbor.
Type	Indicates the type of neighbor entry. If the entry is manually configured, the type is Static; if the entry is dynamically resolved, the type is Dynamic.
MAC Address	Indicates MAC Address of the neighbor.
isRtr	Indicates whether or not the neighbor is a router. If TRUE, the neighbor is a router; if FALSE, the neighbor is not a router.
Neighbor State	Indicates the state of the neighbor cache entry. The possible values are as follows: Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Age	Indicates the time (in seconds) that has elapsed since the most recent entry was added to the cache.

4-20 show serviceport ipv6 neighbors

This command is used to show information regarding the IPv6 neighbor entries cached on the service port. The information is updated in order to display the type of the entry.

show serviceport ipv6 neighbors

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following provides an example of the command

```
(Routing) #show serviceport ipv6 neighbors

                                                                  Neighbor Age
IPv6 Address              Type        MAC Address       isRtr    State    (Secs)
------------------------  --------    ----------------- ------    -----   -------
FE80::5E26:AFF:FEBD:852C  Dynamic     00:09:e7:00:00:50 True       Stale   3
```

Display Parameters

IPv6 Address	Indicates the IPv6 address of the neighbor.
Type	Indicates the type of neighbor entry. If the entry is manually configured, the type is Static; if the entry is dynamically resolved, the type is Dynamic.
MAC Address	Indicates the MAC Address of the neighbor.
isRtr	Indicates whether or not the neighbor is a router. If TRUE, the neighbor is a router; if FALSE, the neighbor it is not a router.
Neighbor State	Indicates the state of the neighbor cache entry. The possible values are as follows: Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Age	Indicates the time (in seconds) that has elapsed since the most recent entry was added to the cache.

4-21 show network ipv6 dhcp statistics

This command is used to show the statistics for the DHCPv6 client running on the network management interface.

show network ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following provides an example of the CLI display output for the command

```
(Switching)#show network ipv6 dhcp statistics

DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received..... 0
DHCPv6 Reply Packets Received............. 0
Received DHCPv6 Advertisement Packets Discard.... 0
Received DHCPv6 Reply Packets Discarded..... 0
DHCPv6 Malformed Packets Received......... 0
Total DHCPv6 Packets Received............. 0
DHCPv6 Solicit Packets Transmitted........ 0
DHCPv6 Request Packets Transmitted........ 0
DHCPv6 Renew Packets Transmitted.......... 0
DHCPv6 Rebind Packets Transmitted......... 0
DHCPv6 Release Packets Transmitted........ 0
Total DHCPv6 Packets Transmitted.......... 0
```

Display Parameters

DHCPv6 Advertisement Packets Received	Indicates the number of DHCPv6 Advertisement packets that have been received on the network interface.
DHCPv6 Reply Packets Received	Indicates the number of DHCPv6 Reply packets that have been received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	Indicates the number of DHCPv6 Advertisement packets that have been discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	Indicates the number of DHCPv6 Reply packets that have been discarded on the network interface.
DHCPv6 Malformed Packets Received	Indicates the number of malformed DHCPv6 packets that have been received on the network interface.
Total DHCPv6 Packets Received	Indicates the total number of DHCPv6 packets that have been received on the network interface.
DHCPv6 Solicit Packets Transmitted	Indicates the number of DHCPv6 Solicit packets that have been transmitted on the network interface.

DHCPv6 Request Packets Transmitted	Indicates the number of DHCPv6 Request packets that have been transmitted on the network interface.
DHCPv6 Renew Packets Transmitted	Indicates the number of DHCPv6 Renew packets that have been transmitted on the network interface.
DHCPv6 Rebind Packets Transmitted	Indicates the number of DHCPv6 Rebind packets that have been transmitted on the network interface.
DHCPv6 Release Packets Transmitted	Indicates the number of DHCPv6 Release packets that have been transmitted on the network interface.
Total DHCPv6 Packets Transmitted	Indicates the total number of DHCPv6 packets that have been transmitted on the network interface.

4-22 show serviceport ipv6 dhcp statistics

This command is used to show the statistics for the DHCPv6 client running on the network management interface.

show serviceport ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following provides an example of the CLI display output for the command.

```
(Switching)#show serviceport ipv6 dhcp statistics

DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received..... 0
DHCPv6 Reply Packets Received............. 0
Received DHCPv6 Advertisement Packets Discarded.. 0
Received DHCPv6 Reply Packets Discarded..... 0
DHCPv6 Malformed Packets Received......... 0
Total DHCPv6 Packets Received............. 0
DHCPv6 Solicit Packets Transmitted........ 0
DHCPv6 Request Packets Transmitted........ 0
DHCPv6 Renew Packets Transmitted.......... 0
```

```
DHCPv6 Rebind Packets Transmitted.............. 0
DHCPv6 Release Packets Transmitted.............. 0
Total DHCPv6 Packets Transmitted................ 0
```

Display Parameters

DHCPv6 Advertisement Packets Received	Indicates the number of DHCPv6 Advertisement packets that have been received on the service port interface.
DHCPv6 Reply Packets Received	Indicates the number of DHCPv6 Reply packets that have been received on the service port interface.
Received DHCPv6 Advertisement Packets Discarded	Indicates the number of DHCPv6 Advertisement packets that have been discarded on the service port interface.
Received DHCPv6 Reply Packets Discarded	Indicates the number of DHCPv6 Reply packets that have been discarded on the service port interface.
DHCPv6 Malformed Packets Received	Indicates the number of malformed DHCPv6 packets that have been received on the service port interface.
Total DHCPv6 Packets Received	Indicates the total number of DHCPv6 packets that have been received on the service port interface.
DHCPv6 Solicit Packets Transmitted	Indicates the number of DHCPv6 Solicit packets that have been transmitted on the service port interface.
DHCPv6 Request Packets Transmitted	Indicates the number of DHCPv6 Request packets that have been transmitted on the service port interface.
DHCPv6 Renew Packets Transmitted	Indicates the number of DHCPv6 Renew packets that have been transmitted on the service port interface.
DHCPv6 Rebind Packets Transmitted	Indicates the number of DHCPv6 Rebind packets that have been transmitted on the service port interface.
DHCPv6 Release Packets Transmitted	Indicates the number of DHCPv6 Release packets that have been transmitted on the service port interface.
Total DHCPv6 Packets Transmitted	Indicates the total number of DHCPv6 packets that have been transmitted on the service port interface.

4-23 clear network ipv6 dhcp statistics

This command is used to clear the DHCPv6 statistics on the network management interface.

clear network ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

4-24 clear serviceport ipv6 dhcp statistics

This command is used to clear the DHCPv6 client statistics on the service port interface.

clear serviceport ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

4-25 ping ipv6

This command is used to determine if another computer is present on the network. When initiated from the CLI interface, the ping command provides a synchronous response. In order to use the command, the user must configure the switch for network (in-band) connection. In addition, the source and target devices are required to have the ping utility enabled and running on top of TCP/IP. Then, as long as there is a physical path between the switch and the workstation, the switch can be pinged from any IP workstation to which the switch has been connected through the default VLAN (VLAN 1). The terminal interface transmits a total of three pings to the target station. By using the global IPv6 address of an interface, the *ipv6-address/hostname* parameter can be utilized to ping that interface, while the optional *size* keyword can be used to specify the size of the ping packet. Furthermore, the **outgoing-interface** option can be used to specify the outgoing interface for a multicast IPv4/IPv6 ping.

When using an IPv6 global address *ipv6-global-address/hostname*, the user can utilize the ping or trace route facilities over the service/network ports. The assignment of any IPv6 global addresses or gateways to these interfaces will cause the installation of IPv6 routes within the IP stack, such that the ping or trace route request will then be properly routed out of the service/network port. When referencing an IPv6 link-local address, the user is also required to specify the service or network port interface by utilizing the **serviceport** or **network** parameter.

ping ipv6 {*ipv6-global-address* | *hostname* **| {interface {***slot/port* **| vlan** *vlan-id* **| serviceport | loopback | tunnel | network}** *link-local-address***} [***size datagram-size***] [outgoing-interface {***slot/port* **| vlan 1-4093 | serviceport I network}]}**

Parameters

None

Default

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

Command Mode

- Privileged EXEC
- User EXEC

4-26 ping ipv6 interface

This command is used to determine if another computer is present on the network. In order to use the command, the user must configure switch for network (in-band) connection. In addition, the source and target devices are required to have the ping utility enabled and running on top of TCP/IP. Then, as long as there is a physical path between the switch and the workstation, the switch can be pinged from any IP workstation to which the switch has been connected through the default VLAN (VLAN 1). The terminal interface transmits a total of three pings to the target station. By using the link-local address or global IPv6 address of an interface, the *interface* keyword can be used to ping that interface, while a loopback, network port, serviceport, tunnel, or physical interface can be used as the source. In addition, the optional *size* keyword can be used to specify the size of the ping packet. The *ipv6-address* is used to indicate the link local IPv6 address of the device that the user wants to query, and the **outgoing-interface** option can be used to specify the outgoing interface for a multicast IP/IPv6 ping.

ping ipv6 interface {*slot/port* **| loopback** *loopback-id* **| network | serviceport | tunnel** *tunnel-id***} {vlan 1-4093}**

Parameters

slot/port	Specifies a valid slot or port.
loopback *loopback-id*	Specifies the loopback ID to ping.
network	Specifies the link local address with network port as the next hop interface.
serviceport	Specify a link local address with Service port as the next hop interface.
tunnel *tunnel-id*	Select the tunnel ID interface to designate to initiate the ping function.
vlan	(Optional) Select the VLAN interface (1 – 4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

4-27 traceroute

The **traceroute** command is used to identify the routes that are actually taken by packets as they travel to their destinations through the network on a hop-by-hop basis. When initiated from the CLI interface, the traceroute command continues to provide a synchronous response.

Either the source IP address or the virtual router of the traceroute probes may be specified. It should be noted that the way in which traceroute works is by sending packets that are expected not to reach their final destination but, rather, to trigger ICMP error messages that will be sent back to the source address from each stop along the forward path toward the destination. The user can, by specifying the source address, determine at what point along the forward path a route back to the source address is lacking. It should be noted, however, that this is only useful in the event that the route from the source to the destination and from the destination to the source is symmetric. One common usage, for example, is the sending of a traceroute from an edge router to some target located higher up in the network by use of a source address at a host subnet on the edge router. Doing this allows the user to test whether the location within the network is reachable from the host attached to the edge router. Alternatively, a user could send a traceroute in which an address on a loopback interface serves as the source in order to test reachability from within the network back to the loopback interface address.

In the CLI, the source can be specified as an IPv4 address, a virtual router, or a routing interface. In the event that a routing interface is specified as the source, the traceroute is sent via the primary IPv4 address on the source interface. With SNMP, it is required that the source be specified as an address.

An incoming packet, such as a traceroute response, that arrives on a routing interface will not be accepted by D-LINK OS if the packet's destination address is located on one of the out-of-band management interfaces (that is, the service port or network port). Similarly, a packet that arrives on a management interface will not be accepted by D-LINK OS if that packet's destination is an address located on a routing interface. As such, it would be pointless to send a traceroute on a management interface while utilizing a routing interface address as the source, or to transmit a traceroute on a routing interface while utilizing a management interface as the source. In other words, if a traceroute is being sent on a routing interface, that routing interface or another routing interface must serve as the source. Similarly, if a traceroute is being sent on a management interface, the source must be located on that management interface. Because of this, a management interface or management interface address cannot be specified as the source by a user. Rather, when a traceroute is being sent on a management interface, a source address should not be specified by the user; instead, the system should be allowed to select the source address from the outgoing interface.

traceroute [vrf *vrf-name***] {***ip-address* **| [ipv6] {***ipv6-address* **|** *hostname***}} [initTtl** *initTtl***] [maxTtl** *maxTtl***] [maxFail** *maxFail***] [interval** *interval***] [count** *count***] [port** *port***] [size** *size***] [source {***ip-address* **|** *ipv6-address* **|** *unit/slot/port***}]**

Parameters

By utilizing the options described below, the user can specify the initial and maximum time-to-live (TTL) in probe packets, as well as the size of each probe, the maximum number of failures before termination, and the number of probes sent for each TTL.

vrf *vrf-name*	(Optional) This parameter indicates the name of the VRF instance from which to initiate the traceroute. Tracerouting can only be accomplished for hosts reachable from within the VRF instance. In the event that a source parameter is specified in concert with a vrf parameter, that parameter must be a member of the VRF. Relatedly, it is not possible to use the ipv6 parameter in conjunction with the vrf parameter.
Ip-address	The value for the *ipaddress* should be a valid IP address.
ipv6-address	The value for the *ipv6-address* should be a valid IPv6 address.

hostname	The value for the *hostname* value should be a valid hostname.
ipv6	(Optional) The use of the optional **ipv6** keyword before the *ipv6-address* or *hostname* is possible. If the *ipv6* keyword is used before the *hostname*, the system will try to resolve to an IPv6 address.
initTtl *initTtl*	(Optional) The **initTtl** term is used to specify the initial time-to-live (TTL), which is the maximum number of router hops allowed between the local and remote system. The allowable values range from 0 to 255.
maxTtl *maxTtl*	(Optional) The **maxTtl** term is used to specify the maximum TTL. The allowable values range from 1 to 255.
maxFail *maxFail*	(Optional) The **maxFail** term is used to terminate the traceroute after failing to receive a response for the specified number of consecutive probes. The allowable values range from 0 to 255.
interval *interval*	(Optional) The optional **interval** parameter can be used to specify the time between probes, in seconds. In the event that a response is not received within the interval indicated, then the traceroute will consider that probe a failure (printing *) and send the next probe. If the traceroute does receive a response to a probe within the indicated interval, then it will immediately send the next probe. The allowable values range from 1 to 60 seconds.
count *count*	The optional **count** parameter can be used to specify the number of probes to be sent for each TTL value. The allowable values range from 1 to 10 probes.
port *port*	The optional **port** parameter can be used to specify the destination UDP port of the probe, which should consist of an unused port on the remote destination system. The allowable values range from 1 to 65535.
size *size*	The optional **size** parameter can be used to specify the size, in bytes, for the payload of the Echo Requests sent. The allowable values range from 0 to 39906 bytes.
source {*ip-address* | *ipv6-address* | *unit/slot/port*}	The optional **source** parameter can be used to specify the source IP address or the interface for the traceroute.

Default

- count: 3 probes
- interval: 3 seconds
- size: 0 bytes
- port: 33434
- maxTtl: 30 hops
- maxFail: 5 probes
- initTtl: 1 hop

Command Mode

Privileged EXEC

Example

Some examples of the CLI command are shown below.

traceroute Success:

```
(Routing)# traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3
port 33434 size 43
```

```
Traceroute to 10.240.10.115, 4 hops max 43 byte packets:
1  10.240.4.1       708 msec     41 msec      11 msec
2  10.240.10.115      0 msec      0 msec       0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

traceroute ipv6 Success:

```
(Routing)# traceroute 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port
33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1  2001::2          708 msec     41 msec      11 msec

The above command can also be execute with the optional ipv6 parameter as follows:

(Routing)# traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3
port 33434 size 43
```

traceroute Failure:

```
(Routing)# traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3 port 33434 size
43

Traceroute to 10.40.1.1, 30 hops max 43 byte packets:
1  10.240.4.1        19 msec     18 msec       9 msec
2  10.240.1.252       0 msec      0 msec       1 msec
3  172.31.0.9       277 msec    276 msec     277 msec
4  10.254.1.1       289 msec    327 msec     282 msec
5  10.254.21.2      287 msec    293 msec     296 msec
6  192.168.76.2     290 msec    291 msec     289 msec
7  0.0.0.0          0 msec *

Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

traceroute ipv6 Failure:

```
(Routing)# traceroute 2001::2 initTtl 1 maxFail 0 interval 1 count 3 port 33434 size
43

Traceroute to 2001::2 hops max 43 byte packets:
1  3001::1          708 msec     41 msec      11 msec
2  4001::2          250 msec    200 msec     193 msec
3  5001::3          289 msec    313 msec     278 msec
4  6001::4          651 msec     41 msec     270 msec
5  0                0 msec *

Hop Count = 4 Last TTL = 5 Test attempt = 1 Test Success = 0
```

4-28 traceroute ipv6

This command is used to identify the routes that are actually taken by packets as they travel to their destinations through the network on a hop-by-hop basis. It is required that the *ipv6-address* parameter be a valid IPv6 address. The optional **port** parameter is used to indicate the UDP port that is used as the destination of the packets that are sent as part of the traceroute. This port should consist of an unused port on the destination system. The allowable values for the **port** parameter range from 0 (zero) to 65535. The default value is 33434.

traceroute ipv6 {*ipv6-address* **|** *hostname* **[port]}**

Parameters

ipv6-address	Select the IPv6 address to trace.
hostname	Select the hostname to trace.
port	(Optional) Select the UDP destination port in probe packets.

Default

The default is None.

Command Mode

Privileged EXEC

Console Port Access Commands

In this section, the commands used to configure the console port are described. The user can use a serial cable in order to connect a management host to the console port of the switch directly.

4-29 configure

This command is used to give the user access to the Global Config mode. From the Global Config mode, the user is then able to configure various system settings, including user accounts. From this mode, the user can also enter other command modes, including the Line Config mode.

configure

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

4-30 line

This command is used to give the user access to the Line Console mode, which in turn allows the user to configure the console port and various Telnet settings, as well as the console login/enable authentication.

line {console | telnet | ssh}

Parameters

console	Indicates the console terminal line.
telnet	Indicates the virtual terminal used for remote console access (Telnet).
ssh	Indicates the virtual terminal used for secure remote console access (SSH).

Default

The default is None.

Command Mode

Global Config

Example

The following provides an example of the CLI command.

```
(Routing)(config)#line telnet
(Routing)(config-telnet)#
```

4-31 session timeout

This command is used to specify the maximum connect time (in minutes) allowed without console activity. If a value of 0 is entered, that indicates that a console is allowed to remain connected indefinitely, even without activity. The allowable range of values is 0 to 160.

The **no** command to is used set the maximum connect time (in minutes) allowed without console activity.

session timeout *0-160*

no session timeout

Parameters

None

Default

The default is 5.

Command Mode

Line Config

4-32 show serial

This command is used to call up a display of the serial communication settings for the switch.

show serial

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show serial

Serial Port Login Timeout (minutes)..... 5
Baud Rate (bps)............................. 115200
Character Size (bits)....................... 8
Flow Control................................ Disable
Stop Bits................................... 1
Parity...................................... none
```

Display Parameters

Serial Port Login Timeout (minutes)	Indicates the amount of time (in minutes) for which a serial port connection may remain inactive before the switch will close the connection. Entering a value of 0 caused the timeout to be disabled.
Baud Rate (bps)	Indicates the default baud rate at which a serial port will attempt to make a connection.
Character Size (bits)	Indicates the number of bits in a character, which is always 8.
Flow Control	Indicates whether the Hardware Flow Control is enabled or disabled. (Note that the Hardware Flow Control is always disabled.)
Stop Bits	Indicates the number of Stop bits per character, which is always 1.
Parity	Indicates the parity method used on the Serial Port. (Note that the Parity Method value is always None.)

Telnet Commands

In this section, the commands used to configure and view Telnet settings are described. The user can use Telnet in order to manage the device from a remote management host.

4-33 ip telnet server enable

This command is used to enable Telnet connections to the system and in order to enable the Telnet Server Admin Mode. This command is also used to open the Telnet listening port.

The **no** command is used to disable Telnet access to the system and in order to disable the Telnet Server Admin Mode. This command is also used to close the Telnet listening port and to disconnect all open Telnet sessions.

ip telnet server enable

no ip telnet server enable

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

4-34 ip telnet port

The command is used to change the telnet listening port. The no command is used to change the listening port to default port 23.

ip telnet port <1 - 65535>

Parameters

Listening port <1 - 65535>

Default

The default is 23.

Command Mode

Privileged EXEC

4-35 telnet

This command is used to establish a new outbound Telnet connection to a remote host. It is required that the *host* value be a valid IP address or host name. The allowable values for the *port* parameter are valid decimal integers ranging from 0 to 65535, with the default value being 23. In the event that the **[debug]** command is used, the Telnet options that are currently enabled are displayed. The outbound Telnet operational mode is set by the optional **line** parameter as linemode, where, by default, the operational mode is character mode. The **localecho** option is used to enable local echo.

telnet *ip-address/hostname port* **[debug] [line] [localecho]**

Parameters

ip-address	Select the IPv4/IPv6 address of the remote host.
hostname	Select the hostname of the remote host.
port	Select the port parameter (default: 23).

Default

The default is None.

Command Mode

Privileged EXEC

4-36 telnetcon maxsessions

This command is used to specify the maximum number of simultaneous outbound Telnet sessions. No outbound Telnet session can be established if the value is set to 0.

This command is used to regulate new outbound Telnet connections. In the event that it is enabled, it is possible to establish, new outbound Telnet sessions until the system reaches the maxmum number of allowable simultaneous outbound Telnet sessions. Until an established session is ended or an abnormal network error ends the session, it remains active.

The **no** command is used to set the default value as the maximum number of simultaneous outbound Telnet sessions.

telnetcon maxsessions *<0 - 5>*

no telnetcon maxsessions

Parameters

None

Default

The default is 5.

Command Mode

Privileged EXEC

4-37 telnetcon timeout

This command is used to set the Telnet session timeout value. The unit of time for the timeout value is minutes.

The **no** command is used to set default value as the Telnet session timeout value. The unit of time for the timeout value is minutes.

telnetcon timeout *1-160*

no telnetcon timeout

Parameters

None

Default

The default is 5.

Command Mode

Privileged EXEC

4-38 show telnet

This command is used to display the current outbound Telnet settings. These settings apply, in other words, to Telnet connections that are initiated from the switch to a remote system.

show telnet

Parameters

None

Default

The default is None.

Command Mode

Priviledged EXEC

Display Parameters

Outbound Telnet Login	Indicates the amount of time (in minutes) for which an outbound Telnet

Timeout	session may remain inactive before being logged off.
Maximum Number of Outbound Telnet Sessions	Indicates the allowed number of simultaneous outbound Telnet connections.
Allow New Outbound Telnet Sessions	Indicates whether or not outbound Telnet sessions are allowed.

4-39 show telnetcon

This command is used to display the current inbound Telnet settings. These settings apply, in other words, to Telnet connections initiated from a remote system to the switch.

show telnetcon

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Remote Connection Login Timeout (minutes)	Indicates the amount of time (in minutes) for which a remote connection session may remain inactive before being logged off. The value may be specified as any number from 1 to160. The factory default value is 5.
Maximum Number of Remote Connection Sessions	Indicates the allowed number of simultaneous remote connection sessions allowed. The factory default value is 5.
Allow New Telnet Sessions	When this field is set to no, new Telnet sessions will not be allowed. The factory default value is yes.
Telnet Sessions Currently Active	Lists the currently active Telnet sessions.
Telnet Server Admin Mode	Indicates whether or not the Telnet Admin mode is enabled or disabled.
Telnet Server Port	Indicates the configured TCP port number used by the Telnet server for listening (default: 23).

Secure Shell Commands

The commands the user can use to configure the Secure Shell (SSH) access to the switch are described in this section. The SSH can be used to access the switch from a remote management host.

Note: A maximum of 5 SSH sessions are allowed by the system.

4-40 ip ssh server enable or ip ssh

This command is used to enable SSH access to the system. (The command is the shortened form of the **ip ssh server enable** command.)

ip ssh server enable or ip ssh

no ip ssh server enable

Parameters

None

Default

The default is Enabled.

Command Mode

Privileged EXEC

4-41 ip ssh port

This command is used to configure the TCP port number upon which requests are listened for by the SSH server. Port numbers from 1-65535 are valid.

The **no** command is used to restore the SSH server listen port to its factory default value.

ip ssh port *1-65535*

no ip ssh port

Parameters

None

Default

22

Command Mode

Privileged EXEC

4-42 ip ssh protocol

Use of this command allows the user to set or remove protocol levels (or versions) for the SSH. It is possible to set either SSH1 (1) or SSH2 (2) or both SSH 1 and SSH 2 (1 and 2).

ip ssh protocol [1] [2]

Parameters

None

Default

1 and 2

Command Mode

Privileged EXEC

4-43 ip ssh server enable

This command is used to enable the IP secure shell server. No new SSH connections will be allowed, but the existing SSH connections will continue to work until timed-out or logged-out.

The **no** command is used to disable the IP secure shell server.

ip ssh server enable

no ip ssh server enable

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

4-44 sshcon maxsessions

This command is used to specify the maximum number of SSH connection sessions that are allowed to be established. No ssh connection can be established if the value is set to 0. The range is 0 to 5.

The **no** command is used to set the default value as the maximum number of SSH connection sessions.

sshcon maxsession *0-5*

no sshcon maxsession

Parameters

None

Default

5

Command Mode

Privileged EXEC

4-45 sshcon timeout

This command is used to set the value (in minutes) for the SSH connection session timeout value. If a session has not been idle for the entirety of the value set, it remains active. The time set must consist of a decimal value from 1 to 160.

The **no** command is used to set the default value as the value (in minutes) for the the SSH connection session timeout value.

A change of the timeout value for any active sessions does not go into effect until the session is re-accessed. Also, the new timeout duration will be activated by any keystroke.

sshcon timeout *1-160*

no sshcon timeout

Parameters

None

Default

5

Command Mode

Privileged EXEC

4-46 show ip ssh

This command is used to display the ssh settings.

show ip ssh

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Administrative Mode	Indicates whether the administrative mode of SSH is enabled or disabled.
SSH Port	Indicates the SSH port.
Protocol Level	Indicates the protocol level, which may have the values of version 1, version 2, or both version 1 and version 2.
SSH Sessions Currently Active	Indicates the current number of active SSH sessions.
Max SSH Sessions Allowed	Indicates the maximum number of SSH sessions allowed.
SSH Timeout	Indicates (in minutes) the SSH timeout value.
Keys Present	Indicates the presence or absence of the SSH RSA and DSA key files on the device.
Key Generation in Progress	Indicates whether the generation of RSA or DSA key files is currently in progress.

Management Security Commands

The commands used to generate keys and certificates are described in this section. Such generation can be performed in addition to loading them as before.

4-47 crypto key generate rsa

This command is used to generate an RSA key pair for the SSH. Any existing generated or downloaded RSA key files will be overwritten by the new key files.

The **no** command is used to delete the RSA key files from the device.

crypto key generate rsa

no crypto key generate rsa

Parameters

None

Default

The default is None.

Command Mode

Global Config

4-48 crypto key generate dsa

This command is used to generate a DSA key pair for the SSH. Any existing generated or downloaded DSA key files will be overwritten by the new key files.

The **no** command is used to delete the DSA key files from the device.

crypto key generate dsa

no crypto key generate dsa

Parameters

None

Default

The default is None.

Command Mode

Global Config

Access Commands

The commands in this section are used to close remote connections or in order to view information about connections to the system.

4-49 disconnect

The **disconnect** command is used to close Telnet or SSH sessions. The **all** term is used to close all active sessions, or the *session-id* term is used to specify the session ID to close. Use the **show loginsession** command to view the possible values for *session-id*.

disconnect {*session_id* **| all}**

Parameters

session_id	Select the session ID (0-65535) to close.
all	Select all the remote sessions to close.

Default

The default is None.

Command Mode

Privileged EXEC

4-50 linuxsh

The **linuxsh** command can be used to access the Linux shell. The **exit** command can be used to exit the Linux shell and go back to the D-LINK OS CLI. By default, a given shell session will timeout after five minutes with no activity. This timeout value can be changed, however, by using the command "telnetcon timeout" in the Line Console mode.

linuxsh [*ip-port***]**

Parameters

ip-port	(Optional) Indicates the number of the IP port upon which the telnet daemon listens for connections. This ip-port number must be an integer from 1 to 65535 (default 2324).

Default

2324

Command Mode

Privileged EXEC

4-51 show loginsession

This command is used to display the current Telnet, SSH, and serial port connections to the switch Truncated user names will be displayed as a result of using this command.

show loginsession

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

ID	Indicates the login session ID.
User Name	Indicates the name of the user logged on to the system.
Connection From	Indicates the IP address of the remote client machine or EIA 232 for the serial port connection.
Idle Time	Indicates the amount of time the current session has been idle.c
Session Time	Indicates the total amount of time the current session has been connected.
Session Type	Indicates the type of session, i.e., telnet serial or SSH session.

4-52 show loginsession long

This command is used to display the full user names of those users currently logged in to the switch.

show loginsession long

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following provides an example of the command.

```
(Routing)#show login session long

User Name
-------------
Admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

AAA Commands

In this section, the commands used to add, manage, and delete system users are described. There are two default users set for the D-LINK OS software: admin and guest. System settings can be viewed and configured by the admin user, while they can only be viewed by the guest user.

Note: The admin user cannot be deleted. Only one user with read/write privileges is allowed. However, up to five read-only users can be configured on the system.

4-53 aaa accounting

This command is used in the Global Config mode in order to create an accounting method list for user EXEC sessions, user executed commands, or DOT1X. This list is identified either by **default** or by a user-specified **list_name**. When enabled for a line-mode, accounting records can be sent either at both the beginning and the end (i.e., **start-stop**) or only at the end (i.e., **stop-only**). If the user specifies **none**, then accounting is disabled for the indicated list. If the user specifies **TACACS+** as the accounting method, then accounting records are sent to a TACACS+ server. If the user specifies **radius** as the accounting method, then accounting records are sent to a RADIUS server.

The **no** command is used to delete the accounting method list.

Note: The following stipulations all apply:

- For each exec and commands type, the maximum number of Accounting Method lists that can be created is five.
- For DOT1X, it is only possible to create the default Accounting Method list. No other lists can be created.
- It is possible to use the same list-name for both the exec and commands accounting types.
- The use of AAA Accounting for commands with RADIUS as the accounting method is not possible.
- For DOT1X accounting, the only supported record type is either Start-stop or None, where the use of Start-stop enables accounting and the use of None disables accounting.
- The only accounting method type supported for DOT1X accounting is RADIUS.

aaa accounting {exec | commands | dot1x} {default | list_name} {start-stop | stop-only | none} *method1 [method2…]*

no aaa accounting {exec | commands | dot1x} {default | list_name}

Parameters

exec	Indicates that accounting is provided for user EXEC terminal sessions.
commands	Indicates that accounting is provided for all user executed commands.
dot1x	Indicates that accounting is provided for DOT1X user commands.
default	Indicates that the default list of methods is used for accounting services.
list_name	Indicates the string of characters used to name the list of accounting methods.
start-stop	Indicates that a start accounting notice is sent at the beginning of a process and that a stop accounting notice is sent at the end of the process.
stop-only	Indicates that a stop accounting notice is sent at the end of the requested user process.
none	Indicates that accounting services are disabled on this line.
method	Indicates that either the TACACS+ or the RADIUS server is used for accounting purposes.

Default

The default is None.

Command Mode

Global Config

Example

The following is an example of the command.

```
(Routing)#
(Routing)#configure
(Routing)(config)#aaa accounting commands default stop-only tacacs
(Routing)(config)#aaa accounting exec default start-stop radius
(Routing)(config)#aaa accounting dot1x default start-stop radius
(Routing)(config)#aaa accounting dot1x default none
(Routing)(config)#exit
```

The administrator can change the record type, or the methods list, for the same set of accounting type and list name without being required to first delete the previous configuration.

```
(Routing)#
(Routing)#configure
(Routing)(config)#aaa accounting exec ExecList stop-only tacacs
(Routing)(config)#aaa accounting exec ExecList start-stop tacacs
(Routing)(config)#aaa accounting exec ExecList start-stop tacacs radius
```

In the example above, the first **aaa** command causes method list for exec sessions with the name *ExecList* to be created, with the **record-type** being *stop-only* and the **method** being *TACACS+*. The second command causes the **record type** to be changed to *start-stop* from *stop-only* for the same method list. The third command, used for the same list, causes the **methods** list to be changed to *{tacacs,radius}* from {tacacs}.

The following is another example of the command.

```
(Routing)#
(Routing)#configure
(Routing)(config)#aaa accounting commands userCmdAudit stop-only tacacs radius
(Routing)(config)#no aaa accounting commands userCmdAudit
(Routing)(config)#exit
```

4-54 aaa authentication commands

aaa authentication enable

This command is used to set authentication to allow the accessing of higher privilege levels. The **enableList is the** default enable list. This default list is used by the console and contains the method as “enable” followed by **none**.

For Telnet and SSH users, a different default enable list, **enableNetList**, is used (that is, instead of **enableList)**. This alternative list is applied for Telnet and SSH by default and contains “**enable**” followed by the **deny** methods. In D-LINK OS, the enable password is, by default, not configured. This means that, by default, users of Telnet and SSH will not get access to the Privileged EXEC mode. On the other hand, under the default conditions, a console user will always enter the Privileged EXEC mode without needing to enter the **enable** password.

When using the **enable authentication** command, the default and optional list names created with the **aaa authentication enable** command are used. The user can create a list by entering the **aaa authentication enable list-name method** command, where the *list-name* is any string of characters

used to name the list. The list of methods that the authentication algorithm tries is tried in the sequence in which they are identified in the **method** argument.

If no password is configured, the user manager returns ERROR (not PASS or FAIL) for the enable and line methods, and then moves on to the next configured method in the authentication list. If the method **none** is used, it indicates that no authentication is needed.

A prompt will only appear asking the user for an enable password if one is required. The authentication methods that follow do not require passwords:

1. none
2. deny
3. enable (When no enable password is configured)
4. line (When no line password is configured)

Example

Please consider the examples below.

```
a. aaa authentication enable default enable none
b. aaa authentication enable default line none
c. aaa authentication enable default enable radius none
d. aaa authentication enable default line tacacs none
```

Examples **a** and **b** do not result in a prompt for a password; however, because they contain the RADIUS and TACACS+ methods, respectively, examples **c** and **d** do cause the password prompt to be displayed.

If only enable is included as a login method, and if no enable password is configured, then D-LINK OS does not produce a prompt for a username. In such cases, D-LINK OS only produces a prompt for a password. D-LINK OS supports the configuring of methods after the local method is tried in the authentication and authorization lists. The next configured method is tried only if the user is not present in the local database.

Only if the previous method returns an error are the additional methods of authentication used (that is, they are not used it if simply fails). If the user wishes to ensure that the authentication succeeds even if an error is returned by all the methods, the user should specify **none** as the final method in the command line.

Note: Requests sent to a RADIUS server by the switch include the username **$enabx$**, where **x** indicates the requested privilege level. In order to ensure that enable is authenticated on RADIUS servers, the user should add **$enabx$** users to them. By doing so, the login user ID will now be sent to TACACS+ servers for enable authentication.

The **no** command is used to return to the default configuration.

aaa authentication enable {default | *list-name***}** ***method1 [method2…]***

no aaa authentication enable {default | *list-name***}**

Parameters

default	Indicates that the listed authentication methods that follow this argument are used as the default list of methods when higher privilege levels are used.
list-name	Indicates the string of characters of up to 15 characters in length that is used to name the list of authentication methods that are activated when accessing higher privilege levels.
method1...[method2…]	Indicates that at least one of the following methods will be used:

	• deny: This method is used to deny access. • enable: The enable password is used for authentication. • line: The line password is used for authentication. • none: No authentication is used. • radius: The list of all RADIUS servers is used for authentication. • tacacs: The list of all TACACS+ servers is used for authentication.

Default

This default is default.

Command Mode

Global Config

Example

The following example sets authentication when a user is accessing higher privilege levels.

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

aaa authentication login

This command is used to set authentication at login. The default and optional list names created with the **aaa authentication login** command can be used with the command initially. The user can create a list by entering the **aaa authentication login list-name method** command, where the *list-name* is any string of characters used to name the list. The list of methods that the authentication algorithm tries is tried in the sequence in which they are identified in the *method* argument.

Each successive method of authentication in the list is only used if the previous method returns an error, not in the event that there is an authentication failure. If the user wishes to ensure that the authentication succeeds even if an error is returned by all the methods, the user should specify **none** as the final method in the command line. For example, if **none** is specifically indicated as an authentication method after **radius**, then no authentication is used in the event that the RADIUS server is down.

The **no** command is used to return to the default setting.

aaa authentication login {default | *list-name***}** ***method1 [method2…]***

no aaa authentication login {default | *list-name***}**

Parameters

default	The default Authentication List. For telnet/SSH, the default list is 'networkList'.
list-name	Indicates the string of characters of up to 15 characters in length that is used to name the list of authentication methods that are activated when a user logs in.
method1...[method2…]	Indicates that at least one of the following methods will be used: • enable: The enable password is used for authentication. • line: The line password is used for authentication.

	• local: The local username database is used for authentication. • none: No authentication is used. • radius: The list of all RADIUS servers is used for authentication. • tacacs: The list of all TACACS+ servers is used for authentication.

Default

- *defaultList*: This list only contains the method none and is used by the console.
- *networkList*: This list only contains the method local and is used by telnet and SSH.

Command Mode

Global Config

Example

The following is an example of the command.

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

4-55 authorization commands

This command is used to apply a command authorization method list to an access method (such as console, telnet, or ssh).

The **no** command is used to remove command authorization from a line config mode.

authorization commands {listname | default}

no authorization commands { listname | default }

Parameters

listname	Select authorization for all user executed commands.
default	Select to provide executed authorization.

Default

The default is None.

Command Mode

- Line console
- Line telnet
- Line SSH

Example

The following is an example of the command.

```
(Switching)(config)#line console
(Switching)(config-line)#authorization command list2

(Switching)(config-line)#
```

```
(Switching)(config-line)#exit

(Switching)(config)#
```

4-56 aaa ias-user username

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

The **aaa ias-user username** command is used in the Global Config mode to add the user specified therein to the internal user database. This command also causes the mode to be changed to the AAA User Config mode.

The **no** command is used to remove the user specified therein from the internal database.

aaa ias-user username *user*

no aaa ias-user username *user*

Parameters

user	Select an existing Internal Authentication Server user name.

Default

The default is None.

Command Mode

Global Config

Example

The following is an example of the command.

```
(Routing)#
(Routing)#configure
(Routing)(config)#aaa ias-user username client-1
(Routing)(config-aaa-ias-user)#exit
(Routing)(config)#no aaa ias-user username client-1
(Routing)(config)#
```

4-57 aaa session-id

This command is used in the Global Config mode in order to specify whether or not the same session-id is to be used within a session for Authentication, Authorization, and Accounting service type.

The **no** command is used in the Global Config mode in order to reset the aaa session-id behavior to the default.

aaa session-id [command | unique]

no aaa session-id [command | unique]

Parameters

common	(Optional) Indicates that the same session-id is used for all AAA Service types.
unique	(Optional) Indicates that a unique session-id is used for all AAA Service types.

Default

This default is common.

Command Mode

Global Config

4-58 password (AAA IAS User configuration)

This command is used to specify a password for a given user in the IAS database. The optional parameter **encrypted** is provided in order to indicate that the password assigned to the command is already pre encrypted.

The **no** command is used to clear the password for a given user.

password [encrypted]

no password

Parameters

password	Indicates the password for this level (8-64 characters in length).
encrypted	(Optional) Indicates that the encrypted password is to be entered, with that password being copied from another switch configuration.

Default

The default is None.

Command Mode

AAA IAS User Config

Example

The following is an example of the command.

```
(Routing)#
(Routing)#configure
(Routing)(config)#aaa ias-user username client-1
(Routing)(config-aaa-ias-User)#password c1ient123
(Routing)(config-aaa-ias-User)#no password
```

The following is another example of the command in which a MAC Authentication Bypass (MAB) client is added to the Internal user database.

```
(Routing)#
(Routing)#configure
(Routing)(config)#aaa ias-user username 1f3ccb1157
(Routing)(config-aaa-ias-User)#password 1f3ccb1157
(Routing)(config-aaa-ias-User)#exit
(Routing)(config)#
```

4-59 clear aaa ias-users

This command is used to remove all users from the IAS database.

clear aaa ias-users

Parameters

None

Default

The default is None.

Command Mode

Privileged Config

Example

The following is an example of the command.

```
(Routing)#
(Routing)#clear aaa ias-users
(Routing)#
```

4-60 show aaa ias-users

This command is used to display the configured IAS users and their attributes. The configured passwords are not shown within the show commands output.

show aaa ias-users

Parameters

None

Default

The default is None.

Command Mode

Privileged Config

Example

The following is an example of the command.

```
(Routing)#
(Routing)#show aaa ias-users

UserName
------------
Client-1
Client-2
```

The IAS configuration commands shown in the output of the **show running config** command are shown in the example below. The passwords shown in the output of the command are always encrypted.

```
aaa ias-user username client-1
password a45c74Fdf56a558a2b5cf95573cd633bac2c6c598d54497ad4c46194918F2c encrypted
exit
```

4-61 accounting

This command is used in a Line Configuration mode in order to apply the accounting method list to a line config (console telnet/ssh).

The **no** command is used to remove accounting from a Line Configuration mode.

accounting {exec | commands} {default | *listname***}**

no accounting {exec | commands} {default | *listname***}**

Parameters

exec	Indicates that accounting will be applied for an EXEC session.
commands	Indicates that accounting will be applied for each command execution attempt. In the event that a user is enabling accounting for the exec mode for the current configuration type, then the user will be logged out.
default	Indicates the default Accounting List.
listname	Indicates the string of characters of up to 15 characters in length that is used to name the list.

Default

The default is None.

Command Mode

Line Config

Example

The following is an example of the command.

```
(Routing)#
(Routing)#configure
(Routing)(Config)#line telnet
(Routing)(Config-telnet)#accounting exec default
(Routing)(Config-telnet)#exit
```

4-62 show accounting

This command is used to display the ordered methods for accounting lists.

show accounting

Parameters

None

Default

The default is None.

Command Mode

Privileged Config

Example

The following is an example of a CLI display output for the command.

```
(Routing)#show accounting
Number of Accounting Notifications sent at beginning of an EXEC session:            0
Errors when sending Accounting Notifications beginning of an EXEC session:         0
Number of Accounting Notifications at end of an EXEC session:                      0
Errors when sending Accounting Notifications at end of an EXEC session:            0
Number of Accounting Notifications sent at beginning of a command execution:       0
Errors when sending Accounting Notifications at beginning of a command execution:  0
Number of Accounting Notifications sent at end of a command execution:             0
Errors when sending Accounting Notifications at end of a command execution:        0
```

4-63 show accounting methods

This command is used to display the configured accounting method lists.

show accounting methods

Parameters

None

Default

The default is None.

Command Mode

Privileged Config

Example

The following is an example of a CLI display output for the command.

```
(Routing)#show accounting methods

Acct Type     Method Name          Record Type   Method Type
----------    --------------       -----------   ------------
Exec          dfltExecList         start-stop    TACACS
Commands      dfltCmdsList         stop-only     TACACS
Commands      UserCmdAudit         start-stop    TACACS
DOT1X         dfltDot1xList        start-stop    radius

Line          EXEC Method List     Command Method List
--------      ----------------     ----------------------
Console       dfltExecList         dfltCmdsList
Telnet        dfltExecList         dfltCmdsList
SSH           dfltExecList         UserCmdAudit
```

4-64 show authorization methods

This command is used to display the configured authorization method lists.

show authorization methods

Parameters

None

Default

The default is None.

Command Mode

Privileged Config

Example

The following is an example of a CLI display output for the command.

```
(Routing)#show authorization methods

Command Authorization Method List
-----------------------------------
dfltCmdAuthList     :      none
noCmdAuthList       :      none

Line          Command Method List
--------      ----------------------
Console       dfltCmdAuthList
Telnet        dfltCmdAuthList
SSH           dfltCmdAuthList

Exec Authorization Method List
-----------------------------------
dfltExecAuthList    :      none
noExecAuthList      :      none

Line          Exec Method List
--------      ----------------------
Console       dfltExecAuthList
Telnet        dfltExecAuthList
SSH           dfltExecAuthList
```

4-65 login authentication

This command is used to specify the login authentication method list for a line (that is, console, telnet, or SSH). Use of the default configuration means that the default set with the **aaa authentication login** command is used.

The **no** command is used to return to the default specified by the **authentication login** command.

login authentication {default | *list-name***}**

no login authentication {default | *list-name***}**

Parameters

default	Indicates that the default list created with the **aaa authentication login** command is used.
list-name	Indicates that the indicated list created with the **aaa authentication login** command is used.

Default

The default is None.

Command Mode

Line Config

Example

The following is an example specifying the default authentication method for a console.

```
(Routing)(Config)#line console
(Routing)(Config-line)#login authentication default
```

User Account and Password Commands

4-66 username (Global Config)

The **username** command is used in the Global Config mode in order to add a new user to the local user database. The privilege level, by default, is 1. By using the **encrypted** keyword, an administrator is allowed to transfer local user passwords between devices without being required to know the passwords. When the **password** parameter is used in conjunction with the **encrypted** parameter, the length of the password must be exactly 128 hexadecimal characters. In the event that the password strength feature is enabled, a check for password strength is conducted by the command, after which it returns an appropriate error indicator if the password fails to meet the password strength criteria. Use of the optional parameter **override-complexity-check** causes the password strength validation to be disabled.

The **no** command is used to return to the default specified by **authentication login** command.

username *name* **{password** *password* **[encrypted [override-complexity-check] | level** *level* **[encrypted [override-complexity-check]] | override-complexity-check]} | {level** *level* **[override-complexity-check] password}**

no username *name*

Parameters

name	Indicates the name of the user, which must be 1-64 characters in length.
password *password*	Indicates the authentication password for the user, which typically must be 8-64 characters in length. However, this value can be zero in the event that the **no password min-length** command has been executed. Various special characters may be included in the password, including ! # $ % & ‘ ( ) * + , - / ; < = > @ [\ ] ^ _ ` { | } ~.
level *level*	Indicates the user level, which must be anywhere from 0-15. A level 15 user may assign a level 0 value to another user in order to suspend that user’s access. Otherwise, an access level of 1 can be entered for a non-privileged user (switch > prompt), while an access level of 15 can be entered to provide the highest level of privilege (switch # prompt). If the level is not specified in instances where it is optional, then the privilege level is set at 1.
encrypted	(Optional) Indicates the encrypted password entered, with that password being copied from another switch configuration.
override-complexity-check	(Optional) Indicates that the password strength validation is disabled.

Default

The default is None.

Command Mode

Global Config

Example

In the following example, the user *bob* is configured with the password *xxxyyymmmm* and user level 15.

```
(Routing)(config)#username bob password xxxyyymmmm level 15
```

In the following example, the user *test* is configured with the password *testPassword* and is assigned a user level of *1*. A validation check of the password strength is not conducted.

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

The following is a third example.

```
(Routing)(config)#username test password testtest
```

The following is a fourth example.

```
(Routing)(config)#username test password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdbal
b1b7ab91be842278e5e970dbfc62d16dcd13c0b864 level 1 encrypted override-complexity-check
(Routing)(config)#username test level 15 password


Enter new password: ********


Confirm new password: ********
```

The following is a fifth example.

```
(Routing)(config)#username test level 15 override-complexity-check password

Enter new password: ********

Confirm new password: ********
```

4-67 username name nopassword

This command is used to remove an existing user's password (NULL password).

username *name nopassword* **[level** *level***]**

Parameters

name	Indicates the name of the user, which must be 1-32 characters in length.
password	Indicates the authentication password for the user, which must be 8-64 characters in length.

level *level*	Indicates the user level. A level 15 user may assign a level 0 value to another user in order to suspend that user's access. The range of user levels is 0-15.

Default

The default is None.

Command Mode

Global Config

4-68 username unlock

This command is used to allow the unlocking of a locked user account. Only a Level 15 user can reactivate a locked user account.

username name unlock

Parameters

None

Default

The default is None.

Command Mode

Global Config

4-69 show users

This command is used to display the names and setting of the configured users. Truncated user names will be displayed by the show users command, while the **show users long** command can be used to display the complete user names. Only users with Level 15 privileges can use the **show users** command. Furthermore, the SNMPv3 fields will not be displayed unless SNMP is available on the system.

show users

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

User Name	Indicates the name the given user enters in order to login using either the serial port or Telnet.
User Access Mode	Indicates whether the user is only able to view the parameters on the switch (Level 1) or if the user can also change them (Level 15). By factory default, a “guest” has only Level 1 access while the "admin" user has Level 15 access.

4-70 show users long

This command is used to display the complete list of usernames configured on the switch.

show users long

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

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

4-71 show users accounts

This command is used to display the status of a local user with respect to user account lockout and the age of the user’s password. The command causes truncated user names to be displayed, whereas the **show users long** command can be used to display complete usernames.

show users accounts [detail]

Parameters

detail	(Optional) Display the details of local database users accounts.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the local user database information that is displayed.

```
(Routing)#show users accounts
User Name     Privilege     Password Aging      Password Expiry Date       Lockout
-----------   ----------    ---------------     ---------------------      ---------
Admin         15            ---                 ---                        False
Guest         1             ---                 ---                        False

(Routing)#show users accounts detail
UserName.........................admin
Privilege........................15
Password Aging...................---
Password Expiry Date.............---
Lockout..........................False
Override Complexity Check.........Disable
Password Strength.................---
```

Display Parameters

User Name	Indicates the local user account's user name.
Access Level	Indicates the user's access level, with 1 indicating a non-privileged user (switch> prompt) and 15 indicating the highest level of privilege (switch# prompt).
Password Aging	Indicates the time (in days) until the password configured for the user expires.
Password Expiry Date	Indicates the current password's expiration date in date format.
Lockout	Indicates whether or not the user account is locked out (true or false).

In the event that the "detail" keyword is included, the following additional fields will also be displayed.

Password Override Complexity Check	Indicates the user's password override complexity check status. By default, the check is disabled.
Password Strength	Indicates the strength (strong or weak) of the user password. Only when the Password Strength feature is enabled is this field displayed.

4-72 show users login-history

This command is used to display information regarding the login history of the various users.

show users login-history [name] [long]

Parameters

name	(Optional) Indicates the name of the user, which must be 1-20 characters in length.
long	(Optional)Indicates the full description of the name string.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of user login history outputs.

```
(Routing)#show users login-history
Login Time                Username      Protocol      Location
------------              ----------    ----------    ------------
Jan 19 2005 08:23:48      Bob           Serial
Jan 19 2005 08:42:31      John          SSH           172.16.0.1
Jan 19 2005 08:49:52      Betty         Telnet        172.16.1.7
```

4-73 password (Line Configuration)

The password command is used in the Line Configuration mode to specify a password on a line. By default, no password is specified.
The **no** command is used to remove the password on a line.

password [password]

no password

Parameters

password	(Optional) Indicates the password for the given level, which must be 8-64 characters in length.

Default

The default is None.

Command Mode

Line Config

Example

In the following example, a password mcmxxyyy is specified on a line.

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

The following is a second example of the command.

```
(Routing)(config-line)#password testtest

(Routing)(config-line)#password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1
b1b7ab91be842278e5e970dbfc62d16dcd13c0b864 encrypted

(Routing)(config-line)#password

Enter new password: ********

Confirm new password: ********
```

4-74 password (User EXEC)

This command is used to enable a user to change the password for himself or herself only. The command should be utilized once the existing password has grown too old. After using the command, the user receives a prompt to enter the old password and the new password intended to replace it.

password

Parameters

None

Default

The default is None.

Command Mode

User EXEC

Example

The example that follows shows the prompt sequence provided when executing the password command.

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

4-75 enable password

The **enable password** configuration command is used to set a local password in order to control access to the privileged EXEC mode.

The **no** command is used to remove the password requirement.

enable password

no enable password

Parameters

password	Indicates the password string, which must be 8-64 characters in length.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

```
(Routing)#enable password testtest

(Routing)#enable password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1
b1b7ab91be842278e5e970dbfc62d16dcd13c0b864 encrypted

(Routing)#enable password
Enter old password: ********
Enter new password: ********
Confirm new password: ********
```

4-76 passwords min-length

This command is used to enforce a minimum password length for local users, with the value used also applying to the enable password. The range of valid values is 0-64.

The **no** command is used to reset the minimum password length to the default value.

passwords min-length *0-64*

no passwords min-length

Parameters

None

Default

The default is 8.

Command Mode

Global Config

4-77 passwords history

This command is used to specify the number of previous passwords that are to be stored for each user account. When the password of a local user is changed, the user will be unable to re-use any previously used password stored in the password history. This ensures that passwords are not re-used to frequently by users. The range of valid values is 0-10.

The **no** command is used to reset the password history to the default value.

passwords history *0-10*

no passwords history

Parameters

None

Default

The default is 0.

Command Mode

Global Config

4-78 passwords aging

This command is used to track the aging (in days) of local users' passwords. When the password of user expires, the user will then be given a prompt to change the password before logging in again. The valid range of values is 1-365. The default value is 0, which means that password aging is not tracked.

The **no** command is used to reset the password aging to the default value.

passwords aging *1-365*

no passwords aging

Parameters

None

Default

The default is 0.

Command Mode

Global Config

4-79 passwords lock-out

This command is used to improve the security of the switch by locking user accounts after a certain number of failed logins due to the entry of incorrect passwords. When a given lockout count is configured, a user must enter the correct password within that count in order to log in. Otherwise, further switch access will be denied to the user. A locked user account can only be reactivated by a user with Level 15 access. Password lockouts do not apply to logins attempts made from the serial console. The valid range of values for attempts is 1-5. The default value is 0, which means that no lockout count is enforced.

The **no** command is used to reset the password lockout count to the default value.

passwords lock-out *1-5*

no passwords lock-out

Parameters

None

Default

The default is 0.

Command Mode

Global Config

4-80 passwords strength-check

This command is used to enable the password strength feature, which is used to check the strength of a given password during its configuration.

The **no** command is used set the password strength checking to the default value.

passwords strength-check

no passwords strength-check

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

4-81 passwords strength maximum consecutive-characters

This command is used to specify the maximum number of consecutive characters to be used to ensure password strength. The valid range of values is 0-15,with the default value being 0. Using the minimum value of 0 means that there is no restriction placed on that set of characters.

passwords strength maximum consecutive-characters *0-15*

Parameters

None

Default

The default is 0.

Command Mode

Global Config

4-82 passwords strength maximum repeated-characters

This command is used to specify the maximum number of repeated characters to be used to ensure password strength. The valid range of values is 0-15, with the default value being 0. Using the minimum value of 0 means that there is no restriction placed on that set of characters.

passwords strength maximum repeated -characters *0-15*

Parameters

None

Default

The default is 0.

Command Mode

Global Config

4-83 passwords strength minimum uppercase-letters

This command is used to specify the minimum number of uppercase letters that a password must contain. The valid range of values is 0-16, with the default value being 2. Using the minimum value of 0 designates no restriction placed on that set of characters.

The **no** command is used to reset the minimum number of uppercase letters required in a password to the default value.

passwords strength minimum uppercase-letters *0-16*

no passwords strength minimum uppercase-letters

Parameters

None

Default

The default is 2

Command Mode

Global Config

4-84 passwords strength minimum lowercase-letters

This command is used to specify the minimum number of lowercase letters that a password must contain. The valid range of values is 0-16, with the default value being 2. Using the minimum value of 0 means that there is no restriction placed on that set of characters.

The **no** command is used to reset the minimum number of lowercase letters required in a password to the default value.

passwords strength minimum lowercase-letters *0-16*

no passwords strength minimum lowercase-letters

Parameters

None

Default

The default is 2.

Command Mode

Global Config

4-85 passwords strength minimum numeric-characters

This command is used to specify the minimum number of numeric characters that a password must contain. The valid range of values is 0-16, with the default value being 2. Using the minimum value of 0 means that there is no restriction placed on that set of characters.

The **no** command is used to reset the minimum number of numeric characters required in a password to the default value.

passwords strength minimum numeric-characters *0-16*

no passwords strength minimum numeric-characters

Parameters

None

Default

The default is 2.

Command Mode

Global Config

4-86 passwords strength minimum special-characters

This command is used to specify the minimum number of special characters that a password must contain. The valid range of values is 0-16, with the default value being 2. Using the minimum value of 0 means that there is no restriction placed on that set of characters.

The **no** command is used to reset the minimum number of special characters required in a password to the default value.

passwords strength minimum special-characters *0-16*

no passwords strength minimum special-characters

Parameters

None

Default

The default is 2.

Command Mode

Global Config

4-87 passwords strength minimum character-classes

This command is used to specify the minimum number of characters classes that a password must contain. The classes of characters are uppercase letters, lowercase letters, special characters, and numeric characters. The valid range of value is 0-4, with the default value being 4.

The **no** command is used to reset the minimum number of classes of characters required in a password to the default value.

passwords strength minimum character-classes *0-4*

no passwords strength minimum character-classes

Parameters

None

Default

The default is 4.

Command Mode

Global Config

4-88 passwords strength exclude-keyword

This command is used when configuring the password to exclude the specified keyword. It will ensure that the keyword is not accepted as a substring by the password in any form (for example, in between the string, case in-sensitive, or in reverse). A maximum of up to 3 such keywords can be configured by the user.

The **no** command is used to reset the restriction for the keyword specified or for all the keywords thus configured.

passwords strength exclude-keyword [*keyword***]**

no passwords strength exclude-keyword [*keyword***]**

Parameters

keyword	(Optional)Select the keyword to exclude, range: 2 – 64.

Default

The default is None.

Command Mode

Global Config

4-89 show passwords configuration

This command is used to show the configured password management settings.

show passwords configuration

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

```
(Routing)#show passwords configuration

Passwords Configuration
---------------------------------
Minimum Password Length..................... 1
Password Aging (days)....................... 0
Password History............................ 0
Lockout Attempts............................ 0
Password Strength Check..................... Disable
Minimum Password Uppercase Letters.......... 5
Minimum Password Lowercase Letters.......... 5
Minimum Password Numeric Characters......... 2
Minimum Password Special Characters......... 2
Maximum Password Repeated Characters........ 1
Maximum Password Consecutive Characters..... 0
Minimum Password Character Classes.......... 4
Password Exclude Keywords................... <none>
```

Display Parameters

Minimum Password Length	Indicates the minimum number of characters that are required when changing passwords.
Password Aging	Indicates the period of time (in days) for which a password will be valid.
Password History	Indicates the number of passwords to be stored in order to prevent reuse.
Lockout Attempts	Indicates the number of failed password login attempts allowed before lockout.

Password Strength Check	Indicates whether or not the function to comply with a strong password configuration is enabled or not.
Minimum Password Uppercase Letters	Indicates the minimum number of uppercase characters required when changing passwords.
Minimum Password Lowercase Letters	Indicates the minimum number of lowercase characters required when changing passwords.
Minimum Password Numeric Characters	Indicates the minimum number of numeric characters required when changing passwords.
Minimum Password Special Characters	Indicates the minimum number of special characters required when changing passwords.
Maximum Password Repeated Characters	Indicates the maximum number of repeated characters that a password can contain when configuring passwords.
Maximum Password Consecutive Characters	Indicates the maximum number of allowed consecutive characters when changing passwords.
Minimum Password Character Classes	Indicates the minimum number of character classes (lowercase, uppercase, numeric and special) that are required when configuring passwords.
Password Exclude-Keywords	Indicates the set of keywords that are to be excluded from the configured password in the event that strength checking is enabled.

4-90 show passwords result

This command is used to show information about the last password setting attempt.

show passwords result

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

```
(Routing)# show passwords result
Last User whose password is set .................. guest
Password strength check ......................... Disable
Last Password Set Result:
========================
Password Successfully Configured for User 'guest'.
```

Display Parameters

Last User Whose Password Is Set	Indicates the name of the user whose password was set most recently.
Password Strength Check	Indicates whether or not password strength checking is enabled.
Last Password Set Result	Indicates whether or not the preceding attempt to set a password was successful. In the event that the attempt failed, the reason that it failed is included.

SNMP Commands

In this section, the commands used in order to configure the Simple Network Management Protocol (SNMP) on the switch are described. The user can configure the switch so that it acts as an SNMP agent, which in turn allows it to communicate with SNMP managers on your network.

4-91 snmp-server

This command is used to set the name as well as the physical location of the switch, in addition to the organization responsible for the network. The parameters *name*, *Loc,* and *con* may be a maximum of 255 characters in length.

Note: If you wish to clear the snmp-server, then simply enter an empty string in quotes. For example, entering snmp-server {sysname " "} will clear the system name.

snmp-server {community *community* **| community-group** *community-group* **| contact** *con* | **enable** *traps {bgp|linkmode|multiusers|stpmode|violation}* | **engineID** *{engine-id |default}* | **filter** *filter-name* | **group** *group-name* | **host** *ipaddr ipv6addr hostname* | **location** *Loc* | **sysname** *name* **| user** *user* **| v3-host** *v3-host* **| view** *view***}**

Parameters

community *community*	Select the SNMP community string (1-20 characters).
community-group *community-group*	Select the group name to use when mapping an internal security name for SNMP v1 and SNMP v2.
contact *con*	Select a system contact up to 255 characters in length.
enable *traps*	Select to enable SNMP Traps.
engineID *engine-id*	Select to specify the SNMP engine ID on a local drive.
filter *filter-name*	Select a name to specify a filter entry.
group *group-name*	Select a group name to configure a new SNMP group.
host *ipaddr ipv6addr hostname*	Select a new recipient by entering the IPv4 or IPv6 address/hostname of the SNMP notification host.

location *Loc*	Select a system location up to 255 characters in length.
sysname *sysname*	Select a system name up to 255 characters in length.
user *user*	Select a new SNMP v3 user on the host that can connect to the agent (up to 30 characters).
V3-host *v3-host*	Select a group name (up to 30 characters) to specify the recipient of the SNMP notification.
view-name ***view***	Select a label to display the record, create or update.

Default

The default is None.

Command Mode

Global Config

4-92 snmp-server community

This command is used to add (name) a new SNMP community, and can also be used (optionally) to set the access mode, to set the allowed IP address, and to create a view for the community.

The **no** command is used to remove the community name in question from the table. That is, the name specified indicates the community name that is to be deleted.

Note: The community names listed in the SNMP Community Table must all be unique. As such when multiple entries are made using the same community name, the first of those entries is kept and processed, while all the duplicate entries are ignored.

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

no snmp-server community *community-name*

Parameters

community-name	Indicates a community name associated with the switch, as well as with the set of SNMP managers that manage it at a specified level of privilege. The length of a given *community-name* may be a maximum of 16 case-sensitive characters.
ro | rw | su	(Optional) Indicates the access mode for the SNMP community, which can be public (Read-Only/RO), private (Read-Write/RW), or Super User (SU).
ipaddress *ip-address*	(Optional) Indicates the associated community SNMP packet sending address. It is used in conjunction with the client IP mask value in order to specify the range of IP addresses from which the SNMP clients may utilize that community so as to access the device. Setting a value of 0.0.0.0 will allow access from any IP address. Otherwise, this value is added with the mask in order to specify the range of allowed client IP addresses.
view *view-name*	(Optional) Indicates the name of the view to be created or updated.

Default

The default is as follows:

- public – this community has read-only permissions, a view name of Default, and provides access via all IP addresses
- private – this community has read/write permissions, a view name of Default, and provides access via all IP addresses

Command Mode

Global Config

4-93 snmp-server community-group

This command is used to configure a community access string such that access via the SNMPv1 and SNMPv2c protocols is permitted.

SNMP-server community-group *community-string group-name* **[ipaddress** *ipaddress***]**

Parameters

community-string	Indicates the community that is to be created and then associated with the group. The allowed range of characters is 1 to 20.
group-name	Indicates the name of the group with which the community is associated. The allowed range of characters is 1 to 30 characters.
ipaddress *ipaddress*	(Optional) Indicates the IPv4 address from which the community may be accessed.

Default

The default is None.

Command Mode

Global Config

4-94 snmp-server enable traps violation

This command is interpreted by the Port MAC locking component, which configures a violation action in order to send an SNMP trap with a default trap frequency of 30 seconds. Using the Global command causes the trap violation mode to be configured across all interfaces valid for port-security. There is no global trap mode as such.

The **no** command is used to prevent the sending of any new violation traps.

Note: Please see "IGMP Snooping Configuration Commands" for information regarding other port security commands.

snmp-server enable traps violation

no snmp-server enable traps violation

Parameters

None

Default

The default is Disabled.

Command Mode

- Global Config
- Interface Config

4-95 snmp-server enable traps

This command is used to enable the switch to send out the traps for events.

The **no** command is used to disable the traps.

snmp-server enable traps ?

no snmp-server enable traps

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

Example

The following is an example of the command.

```
(Routing)(Config)#snmp-server enable traps?
<cr>..................Press enter to execute the command.
bgp...................Press enter to execute the command.
linkmode..............Press enter to execute the command.
multiusers............Press enter to execute the command.
stpmod................Press enter to execute the command.
violatio..............Enable/Disable Port Security SNMP violation traps on all
                      interaces.
```

4-96 snmp-server enable traps bgp

When the bgp option is used for the "snmp-server enable traps" command described above, it enables the two traps defined in the standard BGP MIB, RFC 4273. In that case, then in the event that an adjacency reaches the ESTABLISHED state or in the event that a backward adjacency state transition occurs, a trap will be sent.

snmp-server enable traps bgp *state-changes limited*

Parameters

state-changes limited	Indicates that the standard traps defined in RFC 4273 are enabled.

Default

The default is DHCP.

Command Mode

Global Config

4-97 snmp-server enable traps linkmode

This command is used to enable Link Up/Down traps for the entire switch. In the event that they are enabled, link traps are only sent in the event that the Link Trap flag setting for the port is also enabled.

The **no** command is used to disable Link Up/Down traps for the entire switch.

snmp-server enable traps linkmode

no snmp-server enable traps linkmode

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

4-98 snmp-server enable traps multiusers

This command is used to enable Multiple User traps. In the event that the traps are enabled, a Multiple User Trap is sent whenever a user logs in to the terminal interface (EIA 232 or Telnet) and an existing terminal interface session is already ongoing.

The **no** command is used to disable Multiple User traps.

snmp-server enable traps multiusers

no snmp-server enable traps multiusers

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

4-99 snmp-server enable traps stpmode

This command is used to enable the sending of both new root traps and topology change notification traps.

The **no** command is used to disable the sending of both new root traps and topology change notification traps.

snmp-server enable traps stpmode

no snmp-server enable traps stpmode

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

4-100 snmp-server enginelD local

This command is used to configure the SNMP engine ID on a local device.

The **no** command is used to remove the specified engine ID.

CAUTION: If the engine lD is changed, all the SNMP configurations that exist on the box will be invalidated.

snmp-server enginelD local {*engine-id* **| default}**

no snmp-server enginelD local

Parameters

engine-id	A hexadecimal string identifying the engine-id. The allowed range of characters: even hexadecimal numbers from 6 to 32.
Default	This parameter sets the engine-id to the default string, which is based on the device MAC address.

Default

The enginelD is configured by default according to the device MAC address.

Command Mode

Global Config

4-101 snmp-server filter

This command is used to create a filter entry that can then be used to limit which traps will be sent to a host.

The **no** command is used to remove the specified filter.

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

no snmp-server filter

Parameters

filtername	Indicates the label for the filter that is being created. The allowed range of characters is 1 to 30 characters.
oid-tree	Indicates the OID subtree that is to be included or excluded from the filter. Subtrees may be specified numerically (1.3.6.2.4) or via keywords (system), while asterisks can be utilized to specify a subtree in an oid-tree family (1.3.*.4).
included	Indicates that the tree in question is included in the filter.
excluded	Indicates that the tree in question is excluded from the filter.

Default

By defaults, no filters are created.

Command Mode

Global Config

4-102 snmp-server group

This command is used to create an SNMP access group.

The **no** command is used to remove the specified group.

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

no snmp-server group *group-name* **{v1 | v2c | v3 {noauth | auth | priv}} [context** *context-name***]**

Parameters

group-name	Indicates the group name that is used when configuring communities or users. The allowed range of characters is 1 to 30 characters.
v1	Indicates that the group in question can only gain access via SNMPv1.
v2c	Indicates that the group in question can only gain access via SNMPv2c.
v3	Indicates that the group in question can only gain access via SNMPv3.
noauth	Indicates that the group in question can gain access only when not using Authentication or Encryption. This is only applicable if SNMPv3 is selected.
auth	Indicates that the group in question can gain access only when using Authentication (but not Encryption). Applicable only if SNMPv3 is selected.
priv	Indicates that the group in question can gain access only when using both Authentication and Encryption. This is only applicable if SNMPv3 is selected.
context *context-name*	(Optional) Indicates the SNMPv3 context used during access. This is only applicable if SNMPv3 is selected.
read *read-view*	(Optional) Indicates the view that the group in question will use during GET requests. The allowed range of characters is 1 to 30 characters.
write *write-view*	(Optional) Indicates the view that the group in question will use during SET requests. The allowed range of characters is 1 to 30 characters.
notify *notify-view*	(Optional) Indicates the view that the group in question will use when sending out traps. The allowed range of characters is 1 to 30 characters.

Default

Using the default views, generic groups are created for all versions and privileges.

Command Mode

Global Config

4-103 snmp-server host

This command is used to configure the traps to be sent to the specified host.

The **no** command is used to remove the specified host entry.

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

no snmp-server host *host-addr* **{traps | informs} version {1 | 2c}**

Parameters

host-addr	Indicates the IPv4 or IPv6 address of the host to which the trap or inform notification is sent.
community-string	Indicates the community string that is sent as part of the notification. The allowable range of characters is 1 to 20 characters.
version 1	Indicates that SNMPv1 traps will be sent. This option is unavailable in the event that informs is selected.
version 2c	Indicates that SNMPv2c traps will be sent. This option is unavailable in the event that informs is selected. By default, this option is selected.
traps	Indicates that SNMP traps will be sent to the host. By default, this option is selected.
informs	(Optional) Indicates that SNMPv2 inform notifications will be sent to the host.
timeout *seconds*	(Optional) Indicates the number of seconds that the system will wait for an acknowledgment before the inform notification is resent. The default value for this option is 15 seconds. The allowable range of time is 1 to 300 seconds.
retries *retries*	(Optional) Indicates the number of times that an inform notification will be resent. The default value for this option is 3 attempts. The allowed range of retries is 0 to 255 retries.
udp-port *port*	(Optional) Indicates the SNMP trap receiver port. Port 162 is set for this purpose by default.
filter *filter-name*	(Optional) Indicates the filter name that is to be associated with the host in question. Filters can be utilized to specify which traps will be sent to the host. The allowed range of characters is 1 to 30 characters.

Default

The default is as follows: hosts are not configured.

Command Mode

Global Config

4-104 snmp-server port

This command is used to configure the UDP port number upon which requests are listened for by the SNMP server.

The **no** command is used to restore the specified SNMP server listen port to its factory default value.

snmp-server port *1025-65535*

no snmp-server port

Parameters

None

Default

The default is 161.

Command Mode

Privileged EXEC

4-105 snmp-server trapsend

This command is used to set the UDP port that the SNMP server sends traps too.

The **no** command is used to send traps to the default UDP port.

snmp-server trapsend *portid*

no snmp-server trapsend *portid*

Parameters

None

Default

The default is 50505.

Command Mode

Global Config

4-106 snmp-server user

This command is used to create an SNMPv3 user to whom access to the system is granted.

The **no** command is used to remove the specified SNMPv3 user.

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***]**

no snmp-server user *username*

Parameters

username	Indicates the username under which the SNMPv3 user will connect to the switch. The allowed range of characters is 1 to 30 characters.
groupname	Indicates the name of the group to which the user belongs. The allowed range of characters is 1 to 30 characters.
remote *engineid-string*	(Optional) Indicates the engine-id of the remote management station from which the user in question will be connecting. The allowed range of characters is 5 to 32 characters.
auth-md5 *password* **| auth-sha** *password*	(Optional) Indicate the password that the user in question will use for the authentication or encryption mechanism. The allowed range of characters is 1 to 32 characters.
auth-md5-key *md5-key*	(Optional) Indicates a pregenerated MD5 authentication key. The length of this key will be 32 characters.
auth-sha-key *sha-key*	(Optional) Indicates a pregenerated SHA authentication key. The length of this key will be 48 characters
priv-des *password*	(Optional) Indicates the user password for authentication or encryption. The range is 1 to 32 characters.
priv-des-key *des-key*	(Optional) Indicates a pregenerated DES encryption key. The length of this key will be 32 characters if MD5 is selected, whereas it will be 48 characters if SHA is selected.

Default

The default is as follows: No users are created.

Command Mode

Global Config

4-107 snmp-server view

This command is used to create or modify an existing view entry that is being utilized by groups to determine which objects a community or user is granted access to.

The **no** command is used to remove the specified view.

snmp-server view *viewname* **[***oid-tree***] {included | excluded}**

no snmp-server view *viewname* **[***oid-tree***]**

Parameters

viewname	Parameter (range: 1 to 30 characters) label for the view being created.
oid-tree	(Optional) Indicates the OID subtree to be included or excluded from the view, specified numerically (1.3.6.2.4) or via keywords (system).
included	Indicates the included tree.

excluded	Indicates the excluded tree.

Default

The default is as follows: views are created to grant access to the default group.

Command Mode

Global Config

4-108 snmp-server v3-host

This command is used to configure the traps to be sent to the specified host.

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

Parameters

host-addr	Indicates the IPv4 or IPv6 address of the host to which the trap or inform notification is to be sent.
username	Indicates the user (characters: 1 to 30) utilized to send a trap or inform notification. The user in question must be associated with a group that supports the access method and version in question.
traps	Indicates that SNMP traps will be sent to the host. This option constitutes the default option.
informs	Indicates that SNMP inform notifications to be sent to hosts.
timeout *seconds*	Indicates the number of seconds (default: 15 sec., range: 1 to 300 sec.) that the system will wait for an acknowledgment before the inform notification is resent.
retries *retries*	Indicates the number of times (default: 3 attempts, range: 0 to 255) that an inform notification will be resent.
auth	Indicates that authentication is enabled but not encryption.
noauth	Indicates that no authentication or encryption is enabled. This option is the default option.
priv	Indicates that authentication and encryption are enabled.
udpport *port*	Indicates the SNMP Trap receiver port (default: port 162).
filter *filtername*	Indicates the filter name (characters: 1 to 30) that is to be associated with the host in question. Filters can be utilized to specify which traps will be sent to the host.

Default

The default is as follows: views are created to grant access to the default group.

Command Mode

Global Config

4-109 snmptrap source-interface

This command is used in the Global Configuration mode to configure the global source-interface (that is, the source IP address) for all SNMP communication between the server and the SNMP client.

The **no** command is used in the Global Configuration mode to remove the global source-interface (that is, the source IP selection) for all SNMP communication between the server and the SNMP client.

snmptrap source-interface {*slot/port* **| loopback** *loopback-id* **| network | serviceport | tunnel** *tunnel-id* **| vlan** *vlan-id***}**

no snmptrap source-interface

Parameters

slot/port	Indicates the port that will be used as the source interface.
loopback *loopback-id*	Indicates the loopback interface that will be used as the source interface (range: 0 to 7).
tunnel *tunnel-id*	Indicates the tunnel interface that will be used as the source interface (range: 0 to 7).
vlan *vlan-id*	Indicates the VLAN that will be used as the source interface.

Default

The default is None.

Command Mode

Global Config

Example

The following is an example of the CLI display output for the command.

```
(DQS-5000-32Q28-2023)(ConfICig)#snmptrap source-interface ?

<slot/port>.............................Enter an Interface in slot/port format.
loopback................................Configuration of Loopbck Interface.
network.................................Use network source IP address.
serviceport.............................Use serviceport source IP address.
tunnel..................................Configure IPv6 Tunnel.
vlan....................................Configuration of VLAN Interface.
```

4-110 show snmp

This command is used to show the current SNMP configuration.

show snmp

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show snmp

Community-String     Community-Access     View Name       IP Address
------------------   ------------------   ------------    ----------------
D-LINK               Read Only            Default         All

Community-String     Group Name      IP Address
------------------   ------------    ----------------
D-LINK               DefaultRead     All

Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications
Target Address     Type    Community    Version    UDP     Filter     TO      Retries
                                                   Port    name       Sec
----------------   ------- ----------   --------   ------  --------   -----   --------
192.168.1.10       Trap    D-Link                  2                  162

Version 3 notifications
Target Address     Type    Username     Security   UDP     Filter     TO      Retries
                                        Level      Port    name       Sec
----------------   ------- -----------  --------   ------  --------   -----   --------
192.168.1.20       Inform  D-Link       Auth-NoP   162     15         3

System Contact: D-Link_Support
System Location: 2F
```

Display Parameters

Community String	Indicates the community string for the entry that is to be used by the

	SNMPv1 and SNMPv2 protocols to access the switch.
Community Access	Indicates the access type that the community has: • Read on|y • Read write • su
View Name	Indicates the name given to this community.
IP Address	Indicates that access to this community is limited to the given IP address.
Community String	Indicates the community that this mapping configures.
Group Name	Indicates the group that this community is assigned to.
IP Address	Indicates the IP address that this community is limited to.
Target Address	Indicates the address of the host to which traps will be sent.
Type	Indicates the type of message that will be sent, either traps or inform notifications.
Community	Indicates the community to which traps will be sent.
Version	Indicates the version of SNMP that the trap will be sent as.
UDP Port	Indicates the UDP port to which the trap or inform notification will be sent.
Filter name	Indicates the filter by which the traps will be limited for this host.
TO Sec	Indicates the number of seconds before the inform notifications will time out when sent to this host.
Retries	Indicates the number of times that inform notifications will be sent after timing out.
Target Address	Indicates the address of the host to which traps will be sent.
Type	Indicates the type of message that will be sent, either traps or inform notifications.
Username	Indicates the name to which this host has view access.
Security Level	Indicates the security level granted to this host.
UDP Port	Indicates the UDP port to which the trap or inform notification will be sent.
Filter name	Indicates the filter by which the traps will be limited for this host.
TO Sec	Indicates the number of seconds before the inform notifications will time out when sent to this host.
Retries	Indicates the number of times that inform notifications will be sent after timing out.

4-111 show snmp engineID

This command is used to show the currently configured SNMP engineID.

show snmp engineID

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show snmp engineid

Local SNMP engineID: 800000ab0300a0c9000001
```

Display Parameters

Local SNMP EngineID	Indicates the current configuration for the displayed SNMP engineID.

4-112 show snmp filters

This command is used to show the configured filters that are used when sending traps.

show snmp filters [*filtername***]**

Parameters

filtername	(Optional) Select the SNMP filter name to display its configuration.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show snmp filters

Name          OID Tree                Type
----------    --------------------    ----------
```

```
Test          enterprises.937          Included
Test2         enterprises.259          Excluded
```

Display Parameters

Name	Indicates the filter name for the given entry.
OID Tree	Indicates the OID tree that the given entry will include or exclude.
Type	Indicates whether or not the given entry includes or excludes the OID tree.

4-113 show snmp group

This command is used to show the configured groups.

show snmp group [*groupname***]**

Parameters

groupname	(Optional) Select the SNMP group name to display its configuration.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show snmp group

Name           Context   Security  Security        Read          Write         Notify
               Prefix    Model     Level           View          View          View
-----------    -------   --------  --------        --------      --------      --------
D-LINK         ""        V2        NoAuth-NoPriv   Default       ""            ""
DefaultRead    ""        V1        NoAuth-NoPriv   Default       ""            Default
DefaultRead    ""        V2        NoAuth-NoPriv   Default       ""            Default
DefaultRead    ""        V3        NoAuth-NoPriv   Default       ""            Default
DefaultRead    ""        V3        Auth-NoPriv     Default       ""            Default
DefaultRead    ""        V3        Auth-Priv       Default       ""            Default
DefaultSuper   ""        V1        NoAuth-NoPriv   DefaultSuper  DefaultSuper  DefaultSuper
DefaultSuper   ""        V2        NoAuth-NoPriv   DefaultSuper  DefaultSuper  DefaultSuper
DefaultSuper   ""        V3        NoAuth-NoPriv   DefaultSuper  DefaultSuper  DefaultSuper
DefaultWrite   ""        V1        NoAuth-NoPriv   Default       Default       Default
DefaultWrite   ""        V2        NoAuth-NoPriv   Default       Default       Default
```

```
DefaultWrite    ""          V3          NoAuth-NoPriv    Default       Default       Default
DefaultWrite    ""          V3          Auth-NoPriv      Default       Default       Default
DefaultWrite    ""          V3          Auth-Priv        Default       Default       Default
```

Display Parameters

Name	Indicates the name of the group.
Context Prefix	Indicates a defined prefix to apply to the context.
Security Model	Indicates which protocol is allowed to access the system via the given group.
Security Level	Indicates the security level assigned to this group.
Read View	Indicates the view to which this group provides read access.
Write View	Indicates the view to which this group provides write access.
Notify View	Indicates the view to which this group provides trap access.

4-114 show snmp-server

This command is used to show the current SNMP server user configuration.

show snmp-server

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show snmp-server

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

Display Parameters

SNMP Server Port	SNMP server listening port.

SNMP Trap Send Port	SNMP trap listening port.
Net-SNMP Proxy Mode	The SNMP proxy mode.

4-115 show snmp user

This command is used to show the currently configured SNMPv3 users.

show snmp user [*username***]**

Parameters

username	(Optional) Enter the user account of an existing user.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)(Routing)(Config)#show snmp user

Name          Group Name    Auth Meth     Priv Meth     Remote Engine ID
----------    ----------    ----------    ----------    -------------------------
Test          D-Link                                    800000ab0300a0c9000001
Test1         D-Link        SHA           DES           800000ab0300a0c9000001
```

Display Parameters

Name	Indicates the name of the user.
Group Name	Indicates the group that defines the SNMPv3 access parameters.
Auth Method	Indicates the authentication algorithm configured for the given user.
Privilege Method	Indicates the encryption algorithm configured for the given user.
Remote Engine ID	Indicates the engineID for the user that is defined on the client machine.

4-116 show snmp views

This command is used to show the currently configured views.

show snmp views [*viewname***]**

Parameters

viewname	(Optional) Select the SNMP view name to display its configuration.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show snmp views

Name              OID Tree                Type
---------------   --------------------    ----------
Default           iso                     Included
Default           snmpVacmMIB             Excluded
Default           usmUser                 Excluded
Default           snmpCommunityTable      Excluded
DefaultSuper      iso                     Included
```

Display Parameters

Name	Indicates the view name for the given entry.
OID Tree	Indicates the OID tree that the given entry will include or exclude.
Type	Indicates whether or not the given entry includes or excludes the OID tree.

4-117 show trapflags

This command is used to show the trap conditions. The display for the command shows all of the enabled trapflags. By enabling or disabling the trap condition, the user can configure which traps the switch should generate. In the event that a trap condition is enabled and is detected, the trap is sent by the SNMP agent on the switch to all enabled trap receivers. It is not necessary for the user to reset the switch in order to implement any changes. Both cold and warm start traps are continuously generated, and these traps cannot be disabled.

show trapflags

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show trapflags

Authentication Flag.............................. Enable
Link Up/Down Flag................................ Enable
Multiple Users Flag.............................. Enable
Spanning Tree Flag............................... Enable
ACL Traps........................................ Disable
BGP Traps........................................ Disable
DVMRP Traps...................................... Disable
OSPFv2 traps..................................... Disable
PIM Traps........................................ Disable
OSPFv3 Traps..................................... Disable
Power Supply Module state trap................... Enable
Temperature trap................................. Enable
Fan trap......................................... Enable
FIP snooping Traps............................... Enable
```

Display Parameters

Authentication Flag	This parameter indicates whether or not authentication failure traps will be sent. It can be either enabled or disabled (factory default: enabled).
Link Up/Down Flag	This parameter indicates whether or not link status traps will be sent. It can be either enabled or disabled (factory default: enabled).
Multiple Users Flag	This parameter indicates whether or not 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). It can be either enabled or disabled (factory default: enabled).
Spanning Tree Flag	This parameter indicates whether or not spanning tree traps are sent. It can be either enabled or disabled (factory default: enabled).
ACL Traps	This parameter indicates whether or not ACL traps are sent. It can be either enabled or disabled (factory default: disabled).
BGP Traps	This parameter indicates whether or not BGP4 traps are sent. It can be either enabled or disabled (factory default: disabled).. (It should be noted that this field only appears on systems on which the BGPv4 software package is installed.)
DVMRP Traps	This parameter indicates whether or not DVMRP traps are sent. It can

	be either enabled or disabled (factory default: disabled). In the event that any of the trap flags are not enabled, the command display will show *disabled*. Otherwise, the command shows the information for all the enabled traps.
OSPFv2 Traps	This parameter indicates whether or not OSPFv2 traps are sent. It can be either enabled or disabled (factory default: disabled). In the event that any of the OSPF trap flags are not enabled, the command display will show *disabled*. Otherwise, the command shows the information for all the enabled OSPF traps.
PIM Traps	This parameter indicates whether or not PIM traps are sent. It can be either enabled or disabled (factory default: disabled). In the event that any of the trap flags are not enabled, the command display will show *disabled*. Otherwise, the command shows the information for all the enabled traps.
OSPFv3 Traps	This parameter indicates whether or not OSPFv3 traps are sent. It can be either enabled or disabled (factory default: disabled). In the event that any of the trap flags are not enabled, the command display will show *disabled*. Otherwise, the command shows the information for all the enabled traps.
Power Supply Module State trap	This parameter indicates whether or not Power Supply Module State traps are sent. It can be either enabled or disabled (factory default: disabled). In the event that any of the trap flags are not enabled, the command display will show *disabled*. Otherwise, the command shows the information for all the enabled traps.
Temperature trap	This parameter indicates whether or not Temperature traps are sent. It can be either enabled or disabled (factory default: disabled). In the event that any of the trap flags are not enabled, the command display will show *disabled*. Otherwise, the command shows the information for all the enabled traps.
Fan trap	This parameter indicates whether or not Fan traps are sent. It can be either enabled or disabled (factory default: disabled). In the event that any of the trap flags are not enabled, the command display will show *disabled*. Otherwise, the command shows the information for all the enabled traps.
FIP snooping Traps	This parameter indicates whether or not FIP traps are sent. It can be either enabled or disabled (factory default: disabled). In the event that any of the trap flags are not enabled, the command display will show *disabled*. Otherwise, the command shows the information for all the enabled traps.

4-118 show snmp source-interface

The **show snmp source-interface** command is used in the Global Config mode to show the details of the configured global source interface used for an SNMP client. The IP address for the interface that has been selected is used as the source IP address for all communications with the server.

show snmp source-interface

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

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

SNMP trap Client Source Interface.............. serviceport
SNMP trap Client Source IPv4 Address............. 192.168.0.1            [Up]
SNMP trap Client Source IPv6 Address............. fe80::2a0:c9ff:fe00:0   [Up]
```

RADIUS Commands

In this section, the commands used to configure the switch so that it can use a Remote Authentication Dial-In User Service (RADIUS) server on your network for the purposes of authentication and accounting are described.

4-119 aaa server radius dynamic-author

This command is used to enable Change of Authorization (CoA) functionality and in order to enter the dynamic authorization local server configuration mode.

The **no** command is used to disable CoA functionality.

aaa server radius dynamic-author

no aaa server radius dynamic-author

Parameters

None

Default

The default is None.

Command Mode

Global Config

Example

```
(Routing)#configure
(Routing)(Config)#aaa server radius dynamic-author
```

```
(Routing)(Config-radius-da)#
```

```
(Routing)#configure
(Routing)(Config)#no aaa server radius dynamic-author
```

4-120 auth type

This command is used to specify the type of authorization that will be used by the device for RADIUS clients in order to be granted authorization. The given client must match the configured attribute.

The **no** command is used to reset the type of authorization that will be used by the device for RADIUS clients.

auth type {any | all | session-key}

no auth type

Parameters

any	Select any CoA client authentication types. Authentication attributes must match to allow authentication.
all	Select all CoA client authentication types. Authentication attributes must match to allow authentication.
Session-key	Select the session-key to match to authorize authentication.

Default

The default is All.

Command Mode

Dynamic Authorization

Example

```
(Routing)(Config-radius-da)#auth type all
```

```
(Routing)(Config-radius-da)#no auth type
```

4-121 authorization network radius

This command is used to enable the switch to accept VLAN assignments from the RADIUS server.

The **no** command is used to disable the switch's ability to accept VLAN assignments from the RADIUS server.

authorization network radius

no authorization network radius

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

4-122 clear radius dynamic-author statistics

This command is used to clear RADIUS dynamic authorization counters.

clear radius dynamic-author statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following provides an example of the command.

```
(Routing)#clear radius dynamic-author statistics

Are you sure you want to clear statistics? (y/n) y

Statistics cleared.
```

4-123 client

This command is used to specify the IP address or hostname of the AAA server client. To configure the server key at the client level, the optional server key keyword and string argument are used.

The **no** command is used to remove the configured Dynamic Authorization client in the device, as well as the key associated with that client.

client {*ip-address***} [server-key [0 | 7]** *key-string***]**

no client { *ip-address* **|** *hostame* **}**

Parameters

ip-address	Select the IP address of the DAC to configure.
Server-key	(Optional) Select the shared secret string to verify client COA requests for the server.

Default

The default is None.

Command Mode

Dynamic Authorization

Example

```
(Routing)(Config-radius-da)#client 10.0.0.1 server-key 7 device1


(Routing)(Config-radius-da)#no client 10.0.0.1
```

4-124 debug aaa coa

This command is used to show Dynamic Authorization Server processing debug information.

debug aaa coa

Parameters

None

Default

The default is None.

Command Mode

Priviledged EXEC

4-125 debug aaa pod

This command is used to show messages related to packet of disconnect (POD) packets. To disable debugging output, use the no form of this command.

debug aaa pod

no debug aaa pod

Default

The default is Disabled.

Command Mode

Privileged EXEC

4-126 radius server attribute 4

This command is used to specify the RADIUS client that will use the NAS-IP-Address attribute in the event of RADIUS requests. If a given IP address is specified when this attribute is enabled, the RADIUS client will use that IP address when sending the NAS-IP-Address attribute in RADIUS communications. The **no** command is used to disable the NAS-IP-Address attribute global parameter for RADIUS clients. The RADIUS client will not send the NAS-IP-Address attribute along with RADIUS requests when this parameter is disabled.

radius server attribute 4 [*ipaddr***]**

no radius server attribute 4 [*ipaddr***]**

Parameters

4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	(Optional) The IP address of the server.

Default

The default is None.

Command Mode

Global Config

Example

The following provides an example of the command.

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

4-127 radius server host

This command is used to configure the IP address or DNS name that is to be used when communicating with the RADIUS server for the selected server type. When configuring the DNS name or IP address for authenticating or accounting servers, the user can also configure the server name and port number. In the event that the no names are indicating when configuring the authenticating and accounting servers, the command will use DefaulI_RADIUS_Auth_Server and Default_RADlUS_Acct_Server, respectively, as the default names. The same name can be used in configuring more than one authenticating server, whereas the names used for accounting servers should be unique. The configuration of a maximum of 32 authenticating and accounting servers are allowed by the RADIUS client.

If the *auth* parameter is used, the command will configure the IP address or hostname that will be used to connect to a RADIUS authentication server. Up to 3 servers per RADIUS client can be configured. If three servers have already been configured, the command will fail until the user removes one of those servers by utilizing the “no” form of the command. If the optional *port* parameter is used, the command will configure the UDP port number that will be used to connect to the configured RADIUS server (*port* number range: 1 - 65535; default value: 1812).

Note: Set the *port* parameter to 1812 in order to reconfigure a RADIUS authentication server so that the default UDP *port* will be used.

If the *acct* token is used, the command will configure the IP address or hostname that will be used for the RADIUS accounting server. Only one accounting server can be configured, so if one accounting server is already configured, the “no” form of the command must be used to remove that server from the configuration before configuring another one. In doing so, the IP address or hostname that is specified must match that of an accounting server that was previously configured. If the optional *part* parameter is used, the command will configure the UDP port that will be used when connecting to the RADIUS accounting server. In the event that a port is currently configured for the accounting server, the newly specified port will replace the currently configured port (allowed *port* number range: 0 - 65535; default value: 1813).

Note: Set the *port* parameter to 1813 in order to reconfigure a RADIUS accounting server so that the default UDP port will be used.

To delete a configured server entry from the list of configured RADIUS servers, use the **no** version of this command. In the event that the RADIUS authenticating server that is being removed is the active server among those servers that are identified under the same server name, then another server will be selected by the RADIUS client for the purpose of making RADIUS transactions. In the event that the ‘auth' token is used, the RADIUS authentication server that was previously configured will be removed from the configuration. Similarly, in the event that the ‘acct' token is used, the RADIUS accounting server that was previously configured will be removed from the configuration. The *ipaddr*/*dnsname* parameter has to match the DNS name or the IP address of the previously configured RADIUS authentication / accounting server.

radius server host {auth | acct} {*ipaddr* **|** *dnsname***} [name** *servername***] [port** *0-65535***]**

no radius server host {auth | acct} } {*ipaddr* **|** *dnsname***}**

Parameters

acct	Select IP address or hostname of the RADIUS accounting server to configure.
auth	Select IP address or hostname of the RADIUS authentication server to configure.
ipaddr	Indicates the IP address of the server.
dnsname	Indicates the DNS name of the server.
name *servername*	(Optional) Indicates the port number that will be used to connect to the specified RADIUS server.
port *0-65535*	(Optional) Indicates the alias name used to identify the server.

Default

The default is None.

Command Mode

Global Config

Example

The following provides an example of the command.

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

4-128 radius server key

This command is used to configure the key that will be used for RADIUS client communications with the specified server. The shared secret is configured for either the RADIUS authentication or the RADIUS accounting server depending on whether the ‘auth' or 'acct‘ token is used. Either way, the IP address or hostname provided must match that of a previously configured server. Upon this command’s execution, the secret is prompted.

The text-based configuration allows the RADIUS server’s secrets to be supported in both encrypted and non-encrypted formats. When the configuration is saved, these secret keys are stored solely in the encrypted format. If the user wishes to enter the key in the encrypted format, the key must be entered along with the encrypted keyword. Furthermore, these secret keys are displayed in the encrypted format in the show running config command’s display, while these keys cannot be shown in plain text format.

Note: The secret must consist of an alphanumeric value that does not exceed 16 characters.

radius server key {auth | acct} {*ipaddr* **|** *dnsname***} encrypted** *password*

Parameters

acct	Select the valid IP address or hostname of the RADIUS accounting server to configure the shared secret key.
auth	Select the valid IP address or hostname of the RADIUS authorization server to configure the shared secret key.
ipaddr	Indicates the IP address of the server.
dnsmane	Indicates the DNS name of the server.
password	Indicateshe password in the encrypted format.

Default

The default is None.

Command Mode

Global Config

Example

The following provides an example of the CLI command.

```
(Routing)(Config)#radius server key acct 10.240.4.10 encrypted encrypt-string
```

4-129 radius server msgauth

This command is used to enable the use of the message authenticator attribute by the specified RADIUS Authenticating server.

The **no** command is used to disable the use of the message authenticator attribute by the specified RADIUS Authenticating server.

radius server msgauth {*ipaddr* **|** *dnsname***}**

no radius server msgauth {*ipaddr* **|** *dnsname***}**

Parameters

ipaddr	Indicates the IP address of the server.
dnsmane	Indicates the DNS name of the server.

Default

The default is None.

Command Mode

Global Config

4-130 radius server primary

This command is used to specify the configured server that will serve as the primary server among a group of servers that share the same server name. It should be noted, however, that multiple such primary servers can be configured for any group of servers that share the same name. The RADIUS client will, by default, use the primary server that has the specified server name in the event that the client is asked to perform transactions with an authenticating RADIUS server of a specified name. The RADIUS client will only use the backup servers configured with the same server name if it fails to communicate with the primary server for any reason. Such backup servers are identified as secondary servers.

radius server primary {*ipaddr* **|** *dnsname***}**

Parameters

ipaddr	Indicates the IP address of the server.
dnsmane	Indicates the DNS name of the server.

Default

The default is None.

Command Mode

Global Config

4-131 radius server retransmit

This command is used to configure the RADIUS client global parameters specifying the allotted number of times a message is transmitted when an unsuccessful RADIUS authentication event occurs. Once the allotted number is reached and a response is not achieved, the client no longer communicates with other servers.

radius server retransmit *retries*

no radius server retransmit

Parameters

retries	Indicates the maximum number of transmission attempts that will be made (range: 1 - 15).

Default

The default is 4 attempts.

Command Mode

Global Config

4-132 radius source-interface

This command is used to specify the physical or logical interface that will be used as the RADIUS client source interface (i.e., the source IP address). The address configured as the source interface will be used for all RADIUS communications between the RADIUS client and the RADIUS server. More specifically, the source-interface IP address selected will be used to fill the IP header of RADIUS management protocol packets. This in turn allows security devices (such as firewalls) to identify the source packets sent by the specific switch.

If no source-interface is specified, the primary IP address for the outbound (originating) interface will be used as the source address. In the event that the configured interface is down, the RADIUS client will revert back to its default behavior.

The **no** command is used to reset the RADIUS source interface back to the default settings.

radius source-interface {*slotIport* **| loopback** *loopback-id* **| vlan** *vlan- id* | *network* | *serviceport* **}**

no radius source-interface

Parameters

slot/*port*	Indicates the specific port that will be used as the source interface.
loopback *loopback-id*	Indicates the specific loopback interface that will be used as the source interface (range for the loopback ID: 0 to 7).
vlan *vlan-id*	Indicates the specific VLAN that will be used as the source interface.
Network	Indicates the network port as the source interface.
Serviceport	Indicates the serviceport as the source interface.

Default

The default is None.

Command Mode

Global Config

4-133 radius server timeout

This command is used to configure the global parameter for the RADIUS client that defines the timeout value (in seconds) after which retransmission of a request to the RADIUS server must occur if no response has been received. The timeout value must consist of an integer within the range of 1 to 30.

The **no** command is used to reset the timeout global parameter back to the default value.

radius server timeout *seconds*

no radius server timeout

Parameters

seconds	Select the integer (range: 1 – 30) to define the RADIUS server timeout value.

Default

The default is 5.

Command Mode

Global Config

4-134 server-key

This command is used to configure a global shared secret that will then be used for all dynamic authorization clients for which no individual shared secret key is configured.

The **no** command is used to remove the configured secret.

server-key [0 | 7] *key-string*

no server-key

Parameters

0	Indicates that an unencrypted key is to be entered.
7	Indicates that an encrypted key is to be entered.
key-string	Indicates the shared secret string. For an unencrypted key, the maximum length is 128 characters, while for an encrypted key, the maximum length is 256 characters. The secret string will override the global setting for the given client only. The string should be enclosed in quotes in order to use special characters or embedded blanks.

Default

The default is None.

Command Mode

Dynamic Authorization

Example

```
(Routing)(Config-radius-da)#server-key encrypted mydevice

(Routing)(Config-radius-da)#no server-key
```

4-135 show radius servers

This command is used to display the authentication parameters.

show radius servers {*ipaddr* **| name** *hostname***}**

Parameters

ipaddr	Select a valid IP address of the RADIUS server to display its configuration settings.
hostname	Select a valid hostname of the RADIUS server to display its configuration settings.

Default

Not applicable.

Command Mode

User EXEC

Example

```
(Routing)#show radius servers name Default-RADIUS-Server

RADIUS Server Name..................................... CoA-Server-1
Current Server IP Address.............................. 1.1.1.1
Number of Retransmits.................................. 3
Timeout Duration....................................... 15
Deadtime............................................... 0
Port................................................... 3799
Source IP.............................................. 10.27.9.99
RADIUS Accounting Mode................................. Disabled
Secret Configured...................................... Yes
Message Authenticator.................................. Enable
Number of CoA Requests Received........................ 203
Number of CoA ACK Responses Sent....................... 111
Number of CoA NAK Responses Sent....................... 37
Number of Coa Requests Ignored......................... 55
Number of CoA Missing/Unsupported Attribute Requests..... 18
Number of CoA Session Context Not Found Requests....... 5
Number of CoA Invalid Attribute Value Requests......... 11
Number of Administratively Prohibited Requests......... 3
```

4-136 show radius

This command is used to show the values that have been configured for the global parameters of the RADIUS client.

show radius

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing) #show radius

Number of Configured Authentication Servers.....32
Number of Configured Accounting Servers.........32
Number of Named Authentication Server Groups.....15
Number of Named Accounting Server Groups.........3
```

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

4-137 show radius servers

This command is used to show the summary and details for the RADIUS authenticating servers that have been configured for the RADIUS client.

show radius servers [{*ipaddr* **|** *dnsname* **| name [***servername***]}]**

Parameters

ipaddr	(Optional) Indicates the IP address of the authenticating server.
dnsname	(Optional) Indicates the DNS name of the authenticating server.
servername	(Optional) Indicates the alias name used to identify the server.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show radius servers

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

```
(Routing)#show radius servers name

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

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

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

```
(Routing)#show radius servers 192.168.37.58

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

4-138 show radius accounting

This command is used to show a summary of the configured RADIUS accounting servers.

If no parameters are specified, then only the details of the accounting mode and the RADIUS accounting server will be displayed.

show radius accounting name [*servername***]**

Parameters

servername	(Optional) Indicates the alias name used to identify the server.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show radius accounting name

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

(Routing) #show radius accounting name Default_Radius_Server

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

4-139 show radius statistics

This command is used to show the summary statistics for the configured RADIUS Authenticating servers.

show radius statistics {*ipaddr* **|** *dnsname* **| name [***servername***]}**

Parameters

ipaddr	Indicates the IP address of the server.
dnsname	Indicates the DNS name of the server.
servername	(Optional) Indicates the alias name used to identify the server.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show radius accounting statistics 192.168.37.200

RADIUS Accounting Server Name................... Default_RADIUS_Server
Host Address.................................... 192.168.37.200
Round Trip Time................................. 0.00
Requests........................................ 0
Retransmissions................................. 0
Responses....................................... 0
Malformed Responses............................. 0
```

```
Bad Authenticators.............................. 0
Pending Requests................................ 0
Timeouts........................................ 0
Unknown Types................................... 0
Packets Dropped................................. 0
```

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

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

4-140 show radius source-interface

The **show radius source-interface** command is used in the Privileged EXEC mode to show the details of the configured global source interface used for a RADIUS client. The IP address for the interface that has been selected is used as the source IP address for all communications with the server.

show radius source-interface

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

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

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

4-141 show radius statistics

This command is used to show the summary statistics for the configured RADIUS Authenticating servers.

show radius statistics {*ipaddr* **|** *dnsname* **| name [***servername***]}**

Parameters

ipaddr	Indicates the IP address of the server.
dnsname	Indicates the DNS name of the server.
servername	(Optional) Indicates the alias name used to identify the server.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show radius statistics 192.168.37.200

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

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

RADIUS Server Name.............................. Default_RADIUS_Server
Server Host Address............................. 192.168.37.200
Access Requests................................. 0.00
Access Retransmissions.......................... 0
Access Accepts.................................. 0
Access Rejects.................................. 0
Access Challenges............................... 0
```

```
Malformed Access Responses..... 0
Bad Authenticators............. 0
Pending Requests............... 0
Timeouts....................... 0
Unknown Types.................. 0
Packets Dropped................ 0
```

TACACS+ Commands

TACACS+ is used to provide access control, via one or more centralized servers, to networked devices. Much like RADIUS, this protocol allows authentication to be simplified through th use of a single database that can be shared among many clients on a large network. TACACS+ is founded upon the TACACS+ protocol (which is described in RFC1492), but in addition to the basic TACACS+ protocol, it allows for separate authentication, accounting, and authorization services. Also, while the basic TACACS+ protocol is UDP based and utilizes messages that are passed in clear text over the network, the TACACS+ protocol utilizes TCP to ensure reliable delivery, in addition to using a shared key that is configured on both the client and the daemon server to encrypt all messages.

4-142 tacacs-server host

The **tacacs-server host** command is used in the Global Configuration mode to configure a TACACS+ server. This command is used to enter into the TACACS+ configuration mode. The *ip-address*/*hostname* parameter consists of the IP address or the hostname of the TACACS+ server. Multiple **tacacs-server host** commands can be used to specify multiple hosts.

The **no** command is used to delete a specified hostname or IP address. The *ip-address*/*hostname* parameter consists of the IP address of the TACACS+ server.

tacacs-server host [*ip-address* **|** *hostname***]**

no tacacs-server host [*ip-address* **|** *hostname***]**

Parameters

ip-address	(Optional) Select the IP address of the TACACS+ server host to configure.
hostname	(Optional) Select the hostname TACACS+ server host to configure.

Default

The default is None.

Command Mode

Global Config

4-143 key

The key command is used to define the authentication and encryption key strings.

key {*key-string* **|** *encrypted***}**

Parameters

key-string	Indicates a string value, length: 0 – 128 characters.
Encrypted	Indicates a pre-encrypted key.

Default

The default is 0.

Command Mode

TACACS+ Config

4-144 keystring

The keystring command is used to re-confirm the authentication and encryption key function.

key {*key-string* **|** *encrypted***}**

Parameters

key-string	Indicates a string value, length: 0 – 128 characters.
Encrypted	Indicates a pre-encrypted key.

Default

The default is 0.

Command Mode

TACACS+ Config

4-145 port

The port command is used to select the TACACS+ server port number.

port {*port-number***}**

Parameters

port-number	Indicates a port range: 0 – 65535. Default: 49.

Default

The default is 0.

Command Mode

TACACS+ Config

4-146 priority

The priority command is used in the TACACS+ Configuration mode to define the order that servers are used in, where 0 (zero) indicates the highest priority server (range: 0 - 65535).

priority *priority*

Parameters

None

Default

The default is 0.

Command Mode

TACACS+ Config

4-147 timeout

The key command is used to define the timeout value.

timeout {*timeout***}**

Parameters

timeout	Indicates a string value, range: 1 – 30 seconds.

Default

The default is 0.

Command Mode

TACACS+ Config

4-148 tacacs server key

The **tacacs-server** key command is used to set the encryption key and authentication for all TACACS+ communications between the TACACS+ daemon and the switch. The allowed range for the key-string parameter is 0-128 characters, and the parameter is used to specify the encryption key and authentication for all TACACS+ communications between the TACACS+ server and the switch. The key must match that which is used on the TACACS+ daemon.

With text-based configuration, the secrets of the TACACS+ server are supported in both encrypted and non-encrypted formats. When the configuration is saved, these secret keys are stored solely in the encrypted format. If the user wishes to enter the key in the encrypted format, the key must be entered along with the encrypted keyword. Furthermore, these secret keys are displayed in the encrypted format in the show running config command's display, while these keys cannot be shown in plain text format.

The **no** command is used to disable the encryption key and authentication for all TACACS+ communications between the TACACS+ daemon and the switch. The allowed range for the key-string parameter is 0-128 characters. , and the key must match that which is used on the TACACS+ daemon.

tacacs-server key [*key-string* **| encrypted** *key-string***]**

no tacacs-server key *key-string*

Parameters

key-string	(Optional) Select a string length (0 – 128) to define the authentication key, default: none.
encrypted	(Optional) Select a pre-encrypted key to define.

Default

The default is None.

Command Mode

Global Config

4-149 tacacs-server keystring

The **tacacs-server keystring** command is used to specify the global authentication encryption key that is used for all TACACS+ communications between the client and the TACACS+ server.

tacacs-server keystring [key-string | encrypted key-string]

Parameters

None

Default

The default is None.

Command Mode

Global Config

Example

The following provides an example of the CLI command.

```
(Routing)(Config)#tacacs-server keystring

Enter tacacs key: ********
Re-enter tacacs key: ********
```

4-150 tacacs-server source-interface

This command is used in the Global Configuration mode to configure the source interface (that is, the source IP address) for TACACS+ server configuration. The address configured as the source-interface IP address will be used to fill the IP header of management protocol packets. This in turn allows security devices (such as firewalls) to identify the source packets sent by the specific switch.

If no source-interface is specified, the primary IP address for the outbound (originating) interface will be used as the source address.

The **no** command is used to remove the global source interface (that is, the selected source IP) for all TACACS+ communications between the server and the TACACS+ client.

tacacs-server source-interface {*slot/port* **| loopback** *loopback-id* **| vlan** *vlan-id* | *network* | *serviceport* **}**

no tacacs-server source-interface

Parameters

slot/port	Indicates the specific port that will be used as the source interface.
loopback *loopback-id*	Indicates the specific loopback interface that will be used as the source interface (range for loopback ID: 0 to 7).
vlan *vlan-id*	Indicates the specific VLAN that will be used as the source interface.
network	Indicates the network access client.
serviceport	Indicates the serviceport interface ot use as the source interface.

Default

The default is None.

Command Mode

Global Config

Example

The following provides an example of the command.

```
(Config)#tacacs-server source-interface loopback 0
(Config)#tacacs-server source-interface 0/1
(Config)#no tacacs-server source-interface
```

4-151 tacacs-server timeout

The tacacs-server timeout command is used to specify the timeout value for any communications with the TACACS+ servers. The range of the *timeout* parameter is 1-30 seconds. If a timeout value is not specified, then the global timeout will be set to the default value. Those TACACS+ servers not using the global timeout value, however, will retain the timeout values that have been configured for them.

The **no** command is used to reset the timeout value for all TACACS+ servers back to the default value.

tacacs-server timeout *timeout*

no tacacs-server timeout

Parameters

timeout	Select the timeout value (1 – 30 seconds) for the TACACS+ server. Default: 5 seconds.

Default

The default is 5.

Command Mode

Global Config

Configuration Scripting Commands

The use of Configuration Scripting allows the user to generate text-formatted script files that represent a system's current configuration. These configuration script files can be uploaded to a PC or UNIX system and edited, after which the edited files can be downloaded to the system so that the new configuration can be applied. In fact, these configuration scripts can be applied to one or mulitple switches with no modifactions or only minor modifications.

The **show running-config** command (please see "show running-config") can be used to capture a running configuration and transcribe it into a script. The **copy** command (please see "copy") can then be used to transfer the given configuration script to or from the switch.

To view the configuration stored in the startup-config, backup-config, or factory-defaults file, the user can use the **show {***startup-config* **|** *backup-config* **|** *factory-defaults***}** command (please see "show").

In general, scripts should be used on systems with the default configuration; however, it is also possible to apply scripts on systems with configurations other than the default configurations.

Scripts are required to conform to the following rules:

- The file extension for the script must be ".scr".
- The maximum number of scripts allowed on the switch is ten.
- The maximum allowed size for all the script files on the switch combined is 2048 KB.
- The maximum allowed number of command lines for configuration files is 2000.

Single-line annotations for use at the command prompt can be typed in by the user when write testing or configuring scripts in order to improve script readability. The beginning of a comment is flaged by the exclamation point (!) character. More specifically, the comment flag character can be used to begin a word at any point on the command line, with all input following this character being ignored. In other words, any command line beginning with the "!" character is recognized by the parser as a comment line and thus ignored.

The following lines provide an example of a script.

```
! Script file for displaying management access
show telnet !Displays the information about remote connections
! Display information about direct connections
show serial
! End of the script file!
```

Note: In the configuration script, a blank password for a user must be specified as a space within quotes. For example, if the password for user jane is to be changed from a blank password to hello, then the script entry would be as follows:

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

4-152 script apply

This command is used to apply the commands in the script to the switch, where the name of the script to apply is indicated by the *scriptname* parameter.

script apply *scriptname*

Parameters

scriptname	Indicates the file name of the configuration script.

Default

The default is None.

Command Mode

Privileged EXEC

4-153 script delete

This command is used to delete a specified script, with the scriptname parameter indicating the name of the script to be deleted. Alternatively, the **all** option can be used to delete all the scripts currently present on the switch.

script delete {*scriptname* **| all}**

Parameters

scriptname	Indicates the file name of the configuration script.
all	Select to delete all the configuration script files from the switch.

Default

The default is None.

Command Mode

Privileged EXEC

4-154 script list

This command is used to list all of the scripts currently present on the switch. Use of the command will also cause the remaining available places to be shown.

script list

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

4-155 script show

This command is used to show the contents of a script file, with the scriptname parameter indicating the file in question.

script show *scriptname*

Parameters

scriptname	Indicaes the file name of the configuration script.

Default

The default is None.

Command Mode

Privileged EXEC

4-156 script validate

This command is used to validate a script file through parsing of each line in the script file, with the scriptname parameter indicating the name of the script to be validated. The validate option is meant to provide assistance in script development, as the validation is intended to identify any potential problems. That said, it may not be successful in identifying all problems for a given script on every device.

script validate *scriptname*

Parameters

scriptname	Indicates the file name of the configuration script.

Default

The default is None.

Command Mode

Privileged EXEC

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

In this section, the commands used to configure the system prompt and the pre-login banner are described. The pre-login banner consists of the text that is displayed before the user logs in at the User: prompt.

4-157 copy (pre-login banner)

The option to upload or download the CLI Banner to or from the switch is included in the copy command. Local URLs can be specified by using FTP, TFTP, SFTP, SCP, or Xmodem.

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

copy nvram:clibanner <tftp://<ipacldr>/<filepath>/<filename>>

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

4-158 set prompt

This command is used to change the name of the prompt, which may be up to 64 alphanumeric characters long.

set prompt *prompt_string*

Parameters

prompt_string	Indicates the system prompt, up to 64 case sensitive characters.

Default

The default is None.

Command Mode

Privileged EXEC

4-159 set clibanner

This command to is used to configure the pre-login CLI banner prior to displaying the login prompt.

The **no** command is used to remove any configuration of the pre-login CLI banner.

set clibanner *line*

no set clibanner

Parameters

line	This is a parameter consisting of the banner text, where the “” (double quote) symbol is used as a delimiting character. The maximum allowed

length of the banner message is 2000 characters.

Default

The default is None.

Command Mode

Global Config

4-160 show clibanner

This command is used to display the configured pre-login CLI banner, which consists of the text that is displayed before the CLI prompt is displayed.

show clibanner

Parameters

None

Default

No content is displayed before login prompt.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show clibanner

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


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

4-161 hostname

This command is used to set the system hostname. Using it also causes the prompt to be changed. The system hostname may be as many as 64 alphanumeric, case-sensitive characters in length.

hostname *hostname*

Parameters

hostname	Indicates the system prompt, up to 64 case sensitive characters.

Default

The default is None.

Command Mode

Privileged EXEC

Front Panel TAP Interfaces

The commands in this section can be used to enable and monitor the FPTI mode.

4-162 fpti

This command is used to enable the FPTI mode either globally (Global Config mode) or for a specific interface (Interface Config mode).

The **no** command is used to disable the FPTI mode.

fpti

no fpti

Parameters

None

Default

The default is Enabled.

Command Mode

- Global Config
- Interface Config

4-163 show port fpti

This command is used to display the global FPTI mode, as well as the FPTI mode on all the interfaces. If a single interface is specified, then only the FPTI mode for that interface will be displayed.

show port fpti [*slot/port***]**

Parameters

slot/port	(Optional)

Default

The default is None.

Command 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
```

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

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

5. Utility Commands

In this section, the following utility commands available in the D-LINK OS CLI are described:

Note: All of the commands described in this section are included in one of five functional groups:

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

5-1 erase application

This command is used to remove the file specified from the directory of switch file system applications.

erase application

Parameters

None

Default

The default is Disable.

Command Mode

Privileged EXEC

Application Commands

This command is used to make the application began by the designed executable file ready and available to be configured and executed. The way in which the application is run on the switch is determined by the parameters of this command.

An already installed application file name can be used to update the parameters when issuing this command . Doing so will update the configuration for when the application is started the next time.

It should be noted that this command can also be issued for a file that is not currently on the switch. Doing so allows the execution parameters to be preconfigured, with the configuration not taking effect until the executable file is actually included in the switch file system.

The **no** command is used to remove a given configuration of an application for execution on the switch. If the application in question is running when the **no** command is issued, all of the processes associated with the application will be stopped automatically.

5-2 application start

This command is used to initiate the execution of the application specified. Before an application can be started using this command, however, it must be installed.

application start *filename*

Parameters

filename	Indicates the name of application to start.

Default

The default is None.

Command Mode

Privileged EXEC

5-3 application stop

This command is used to stop the execution of the specified application.

application stop *filename*

Parameters

filename	Indicates the name of application to stop.

Default

The default is None.

Command Mode

Privileged EXEC

5-4 show application

This command is used to show the installed applications and their parameters.

show applications

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

filename	Indicates the name of the application.
start-on-boot	Indicates whether or not the application is configured to initiate on boot up. • Yes indicates that the application will initiate on boot up. • No indicates that the application will not initiate on boot up.
auto-restart	Indicates whether or not the application process is configured to restart automatically after it ends. • Yes indicates that the application process will restart after it ends. • No indicates that the application process will not restart automatically after it ends.
Max-CPU-Util	Indicates, as a percentange, the configured application CPU utilization limit. “None” is shown if unlimited.
Max-memory	Indicates, in megabytes, the configured application memory limit. “None” is shown if unlimited.

5-5 show application files

This command is used to show the files in the switch‘s file system application directory.

show application files

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show application files

OpEN application process directory contents:

Total bytes for all files = 5
```

Display Parameters

filename	Indicates the name of the file.
File size	Indicates the number of bytes that the file occupies in the file system.
Directory Size	Indicates the total number of bytes of all the files included in the application directory.

CLI Output Filtering Commands

5-6 show xxx | include “string”

With this filtering command, the command **xxx** is executed, but the output is filtered so that only the lines containing a match for the **“string”** are shown, while all the non-matching lines in the output are not displayed.

Example

The following provides 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
```

5-7 show xxx | include “string” exclude “string2”

With this filtering command, the command **xxx** is executed, but the output is filtered so that only the lines containing a match for the **“string”** match and not containing a match for the **“string2”** are shown, while all the other non-matching lines in the output are also not shown.

Example

The following provides an example of the CLI command.

```
(Routing)#show running-config | include “spanning-tree” exclude “configuration”
spanning-tree bpduguard
spanning-tree bpdufilter default
```

5-8 show xxx | exclude “string”

With this filtering command, the command **xxx** is executed, but the output is filtered so that only those lines not containing a match for the **“string”** are shown.

Example

The following provides 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
```

5-9 show xxx | begin “string”

With this filtering command, the command **xxx** is executed, but the output is filtered so that only those lines beginning with and following the first line containing a match for the **"string"** are shown, while all the preceding lines are not shown.

Example

The following provides 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)#
```

5-10 show xxx | section “string”

With this filtering command, the command **xxx** is executed, but the output is filtered so that only those lines included within the section(s) identified by lines containing a match for the **"string"** and ending with the first line that contains the default end-of-section identifier (i.e. “exit") are shown.

Example

The following provides an example of the CLI command.

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

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

5-11 show xxx | section “string” “string2”

With this filtering command, the command **xxx** is executed, but the output is filtered so that only lines included within the section(s) identified by lines containing a match for the “string” and ending with the first line containing a match for the **“string2”** are shown. If multiple sections that match the specified string criteria are included in the base output, then all such sections are displayed.

5-12 show xxx | section “string” include “string2”

With this filtering command, the command **xxx** is executed, but the output is filtered so that only lines included within the section(s) identified by lines containing a match for the **“string”** and a match for the **“string2”** and ending with the first line containing the default end-of-section identifier (i.e. “exit”) are shown. This filter command can also include “exclude” and user-defined end-of-section identifier parameters.

System Information and Statistics Commands

In this section, the commands used to view information about system components, features, and configurations are described.

5-13 show arp switch

This command is used to show the contents of the Address Resolution Protocol (ARP) table for the IP stack. It should be noted that the IP stack only learns those ARP entries that are associated with the management interfaces – that is, the network or service ports – whereas ARP entries that are associated with routing interfaces are not listed.

show arp switch

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-14 dir

This command is used to list the files included in the directory/mnt/fastpath in flash from the CLI.

dir

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(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_dl.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
```

5-15 show eventlog

This command is used to show the event log. This log contains error messages from the system, and is not cleared upon a system reset.

show eventlog

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show eventlog

                                                                  Time
       File                              Line  TaskID    Code     yyyy/mm/dd hh:mm:ss
EVENT> bootos.c                          192   0E634DDC  AAAAAAAA 2018/04/23 05:34:17
EVENT> bootos.c                          192   0F6A0DDC  AAAAAAAA 2018/04/20 07:23:52
EVENT> bootos.c                          192   0F332DDC  AAAAAAAA 2018/03/24 07:25:27
EVENT> bootos.c                          192   0DEAEDDC  AAAAAAAA 2018/03/19 04:27:02
EVENT> bootos.c                          192   0E068DDC  AAAAAAAA 2018/01/15 00:22:58
EVENT> bootos.c                          192   0DF65DDC  AAAAAAAA 2018/01/11 08:29:45
EVENT> bootos.c                          192   0E7D2DDC  AAAAAAAA 2018/01/10 01:13:58
EVENT> bootos.c                          192   0DD26DDC  AAAAAAAA 2018/01/09 03:48:01
EVENT> bootos.c                          192   0ED02DDC  AAAAAAAA 2018/01/08 00:31:26
EVENT> bootos.c                          192   0DEEBDDC  AAAAAAAA 2018/01/05 00:28:27
EVENT> bootos.c                          192   0DA48DDC  AAAAAAAA 2018/01/04 00:33:50
EVENT> bootos.c                          192   0DF92DDC  AAAAAAAA 2018/01/03 01:08:10
```

```
EVENT> bootos.c                    192   0F61FDDC   AAAAAAAA   2018/01/02 01:05:20
EVENT> bootos.c                    192   0DA00DDC   AAAAAAAA   2017/12/27 10:41:49
EVENT> bootos.c                    192   0DD83DDC   AAAAAAAA   2017/12/27 00:37:50
EVENT> bootos.c                    192   0F46ADDC   AAAAAAAA   2017/10/17 04:12:45
EVENT> bootos.c                    192   0E2E9DDC   AAAAAAAA   2017/10/16 08:23:55
```

5-16 environment temprange

This command is used to specify the temperature range allowed for normal operation.

environment temprange min *-100-100* **max** *-100-100*

Parameters

min *-100-100*	Indicates the minimum temperature allowed for normal operation (range: -100°C to 100°C; default: 0°C).
max *-100-100*	Indicates the maximum temperature allowed for normal operation (range: -100°C to 100°C; default: 0°C).

Default

The default is None.

Command Mode

Global Config

5-17 environment trap

This command is used to configure environment status traps.

environment trap {fan I powersupply | temperature}

Parameters

fan	This parameter is used to enable or disable the sending of traps for fan status events (default: enable).
powersupply	This parameter is used to enable or disable the sending of traps for power supply status events (default: enable).
temperature	This parameter is used to enable or disable the sending of traps for temperature status events (default: enable).

Default

The default is None.

Command Mode

Global Config

5-18 show environment

This command is used to show information regarding system disk space and usage.

show environment

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#show environment

Temp (C)..................................... 53
Fan Speed, RPM............................... 5844
Fan Duty Level............................... 45%
Temperature traps range: 0 to 97 degrees (Celsius)

Temperature Sensors:
Unit    Sensor       Description        Temp (C)   State      Max_Temp (C)
-----   ----------   ---------------    ---------  ---------  ---------------
1       1            Core 0             35         Normal     38
1       2            Core 1             35         Normal     38
1       3            Core 2             35         Normal     39
1       4            Core 3             35         Normal     39
1       5            Switch Temp        53         Normal     54
1       6            Temp_1             38         Normal     39
1       7            Temp_2             40         Normal     41

Fans:
Unit    Fan     Description        Type          Speed   Duty level    State
-----   -----   ---------------    ----------    -----   ----------    ----------
1       1       Fan1_rotor1        Removable     5844    45%           Operational
1       2       Fan1_rotor2        Removable     4804    45%           Operational
1       3       Fan2_rotor1        Removable     5696    45%           Operational
1       4       Fan2_rotor2        Removable     4687    45%           Operational
1       5       Fan3_rotor1        Removable     5648    45%           Operational
1       6       Fan3_rotor2        Removable     4753    45%           Operational
```

```
1       7       Fan4_rotor1       Removable    5696    45%          Operational
1       8       Fan4_rotor2       Removable    4736    45%          Operational

Power Modules:
Unit    Power supply      Description       Type         State
-----   ---------------   ---------------   ----------   ---------------
1       1                 PS-1              Removable    Operational
1       2                 PS-2              Removable    Not powered

Disk usage information:
Unit    Total space (KB)  Free space (KB)   Used space (KB)   Utilization (%)
-----   ---------------   ---------------   ---------------   ---------------
1       999,320           929,064           1,194,772         33
```

Display Parameters

Unit	Indicates the system unit number.
Sensor	Indicates the sensor summary
Description	Indicates the name of the unit.
Temperature	(Optional) Displays information related to the temperature environment.
State	Indicates the condition state of the unit.
Max Temp	(Optional) Displays the maximum posted value for nominal operation.
Fan	(Optional) Displays information relating to the fan environment.
Type	(Optional) Indicates the hardware type.
Speed	(Optional) Indicates the fan speed.
Duty Level	(Optional) Indicates the current operational value of the component.
State	(Optional) Indicates the current state of the component.
Power Supply	(Optional) Displays power supply voltage and current information. If applicable, displays the status of the redundant power supply.
Total Space	Indicates (in KB) the total amount of disk space on the system.
Free Space	Indicates (in KB) the amount of available disk space on the system.
Used Space	Indicates (in KB) the amount of disk space in use on the system.
Utilization	Indicates (as a percentage of total disk space) the amount of disk space in use on the system.

5-19 show version

This command is used to show inventory information for the switch.

Please note that in future releases of the software, the show version command will replace the show hardware command.

show version

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show version

Switch: 1

System Description.............................. DQS-5000-54SQ28 - 48 25GE + 6 100GE,
                                                 2.1.5, Linux 3.16.0-29-generic
Machine Type.................................... DQS-5000-54SQ28 - 48 25GE + 6 100GE
Machine Model................................... DQS-5000-54SQ28
Serial Number................................... SG1F1000068
Part Number..................................... BXS500054SAF.A1
Maintenance Level............................... A1
Manufacturer.................................... D-LINK
Burned In MAC Address........................... 00:05:64:2F:0D:E5
Software Version................................ 1.00.006
Operating System................................ Linux 3.16.0-29-generic
Network Processing Device....................... 6592_B1
Additional Packages............................. BGP-4
................................................. QOS
................................................. Multicast
................................................. IPv6
................................................. Routing
................................................. Data Center
................................................. Open API
................................................. Prototype Open API
```

Display Parameters

System Description	This parameter consists of text that isused to identify the product name of this switch.
Machine Type	Indicates the machine type as defined by the Vital Product Data.
Machine Model	Indicates the machine model as defined by the Vital Product Data.
Serial Number	This parameter consists of the unique box serial number for the switch.

Part Number	This parameter consists of the manufacturing part number.
Maintenance Level	Indicates hardware changes that are of significance to software.
Manufacturer	This parameter consists of a description of the manufacturer.
Burned in MAC Address	Indicates the universally assigned network address.
Software Version	Indicates the release.version.revision number of the code that is currently running on the switch.
Operating System	Indicates the operating system that is currently running on the switch.
Network Processing Device	Indicates the type of the processor microcode being used.
Additional Packages	Indicates the additional packages that have been incorporated into this system.

5-20 show interface

This command is used to display a summary of the statistics for a given specified interface or to display a count of all the CPU traffic based upon the argument.

show interface {*slot/port* **| counters | dampening | debounce | ethernet | lag** *lag-id* **| loopback | priority-flow-control | switchport | tunnel}**

Parameters

slot/port	Select a slot/port interface.
counters	Indicates the summary statistics for all ports on the switch.
dampening	Indicates the interface dampening information.
debounce	Indicates the debounce timer configuration and the current link flap count.
ethernet	Indicates statisctics for a single or all ports.
lag	Indicates the statistics for the LAG interface.
loopback	Indicates the configured Loopback interface information.
priority-flow-control	Indicaes the Priority-Flow-Control information.
switchport	Indicates the statistics for the CPU port on the switch.
tunnel	Indicates the configufed Tunnel interface information.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the show interface output command.

```
(Routing)#show interface switchport

Packets Received Without Error..................... 8229
Broadcast Packets Received......................... 10
Packets Received With Error........................ 0
Packets Transmitted Without Errors................. 8278
Broadcast Packets Transmitted...................... 11
Transmit Packet Errors............................. 0
Address Entries Currently in Use................... 5
VLAN Entries Currently in Use...................... 3
Time Since Counters Last Cleared................... 7 day 18 hr 14 min 46 sec
```

Display Parameters

When the argument is *slot/port*, the display parameters are as follows:

Packets Received Without Error	Indicates the total number of packets received by the processor (including broadcast packets).
Packets Received With Error	Indicates the number of inbound packets which contained errors that prevented them from being delivered to a higher-layer protocol.
Broadcast Packets Received	Indicates the total number of received packets that were directed to the broadcast address.
Receive Packets Discarded	Indicates the number of inbound packets that were selected for discard even though no errors preventing their delivery to a higher-layer protocol had been detected. One potential reason for discarding such packets would be to free up buffer space.
Packets Transmitted Without Error	Indicates the total number of packets transmitted from the interface.
Transmit Packets Discarded	Indicates the number of outbound packets that were selected for discard even though no errors preventing their delivery to a higher-layer protocol had been detected. One potential reason for discarding such packets would be to free up buffer space.
Transmit Packets Errors	Indicates the number of outbound packets that could not be transmitted due to errors.
Collisions Frames	Indicates the best estimate of the overall number of collisions on this Ethernet segment.
Number of link down events	Indicates the counts for the port link down.
Link Flaps	Indicates the port link flaps.
Time Since Counters Last Cleared	Indicates the elapsed time since the statistics for this switch were last cleared in days, hours, minutes, and seconds.

5-21 show interfaces status

This command is used to show information regarding the interface, including its description, speed, port state, and auto-neg capabilities. It is similar to the show port all command, but it also shows additional fields such as the interface description and port-capability.

The interface description itself can be configured through the existing command description <name>, the maximum length of which is 64 characters that are truncated to 28 characters in the output. Using show port description allows the long form of the description to be displayed. The interfaces for which information is displayed by this command include the physical interfaces, LAG interfaces, and VLAN routing interfaces.

show interfaces status [{*slot/port* **| vlan** *id* | *all* | *lag***}]**

Parameters

slot/port	(Optional) Select a slot/port to display its status.
vlan *id*	(Optional) Select a VLAN interface.
all	(Optional) Select to display all interfaces.
lag	(Optional) Select a lag interface.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing #show interfaces status 0/1

Port    Name    Link    Physical    Physical       Media         Flow Control
                State   Mode        Status         Type          Status
-----   -----   -----   -----       ----------     ----------    ----------
0/1             Down    25G Full                   25G-BaseSX    Inactive

Flow Control:Disabled
```

Display Parameters

Port	Indicates the interface that is associated with the rest of the data shown in the row.
Name	Indicates the descriptive user-configured name for the given interface.
Link State	Indicates whether or not the link is up.
Physical Mode	Indicates the duplex and speed settings on the given interface.
Physical Status	Indicates the duplex mode and port speed for physical interfaces, although the physical status of LAGs is not reported. In the event that a port is down, its physical status will be unknown.

Media Type	Indicates the media type of the interface.
Flow Control Status	Indicates the 802.3x flow control status.
Flow Control	Indicates the configured 802.3x flow control mode.

5-22 show interface counters

This command is used to report key summary statistics for all the ports (physical/CPU/port-channel).

show interface counters

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the 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
```

Display Parameters

Port	Indicates the physical port, LAG, or CPU interface that is associated with the rest of the data shown in the row.
InOctets	Indicates the number of inbound octets that have been received by the interface.
InUcastPkts	Indicates the number of inbound unicast packets that have been received by the interface.
InMcastPkts	Indicates the number of inbound multicast packets that have been received by the interface.
InBcastPkts	Indicates the number of inbound broadcast packets that have been received by the interface.
OutOctets	Indicates the number of outbound octets that have been transmitted by the interface.
OutUcastPkts	Indicates the number of outbound unicast packets that have been transmitted by the interface.
OutMcastPkts	Indicates the number of outbound multicast packets that have been transmitted by the interface.
OutBcastPkts	Indicates the number of outbound broadcast packets that have been transmitted by the interface.

5-23 show interface ethernet

This command is used to show detailed statistics for a given specifiied interface or for all the interfaces or for all the CPU traffic based upon the argument.

show interface ethernet {*slot/port* **| all | lag | switchport}**

Parameters

slot/port	Select a slot/port to display its status.
all	Select to display statistics for all ports.
lag	Select a lag interface.
switchport	Select to display statistics for the CPU port on the switch.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command when the **all** keyword is used.

```
(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     8            6            0            0
```

Display Parameters

When a value for *slot/port* is specified, the command causes the following information to be displayed.

Packets Received	• **Total Packets Received (Octets)** – Indicates the total number of octets of data received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets and those in bad packets). This parameter provides a reasonable estimate of Ethernet utilization. If the user requires greater precision, the etherStatsOctets and etherStatsPkts objects should be sampled before and after a common interval. The result for this equation is the value Utilization, which is itself the percent utilization (on a scale of 0 to 100 percent) of the Ethernet segment. • **Packets Received 64 Octets** – Indicates the total number of received packets (including bad packets) that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Received 65-127 Octets** – Indicates the total number of received packets (including bad packets) that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 128-255 Octets** – Indicates the total number of received packets (including bad packets) that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 256-511 Octets** – Indicates the total number of received packets (including bad packets) that were between 256 and 511 octets in length inclusive (excluding framing bits but including octets). • **Packets Received 512-1023 Octets** – Indicates the total number of received packets (including bad packets) that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received1024-1518 Octets** – Indicates the total number of received packets (including bad packets) that were

	between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Rceived > 1518 Octets** – Indicates the total number of received packets that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 64 Octets** – Indicates the total number of received and transmitted packets (including bad packets) that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets RX and TX 65-127 Octets** – Indicates the total number of received and transmitted packets (including bad packets) that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 128-255 Octets** – Indicates the total number of received and transmitted packets (including bad packets) that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 256-511 Octets** – Indicates the total number of received and transmitted packets (including bad packets) that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 512-1023 Octets** – Indicates the total number of received and transmitted packets (including bad packets) that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1024-1518 Octets** – Indicates the total number of received and transmitted packets (including bad packets) that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1519-2047 Octets** – Indicates the total number of received and transmitted packets 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** – Indicates the total number of received and transmitted packets 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** – Indicates the total number of received and transmitted packets 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** – Indicates the total number of received and transmitted packets 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** – Indicates the total number of received packets that were without errors. • **Unicast Packets Received** – Indicates number subnetwork-unicast packets that were delivered to a higher-layer protocol. • **Multicast Packets Received** – Indicates number subnetwork-multicast packets that were delivered to a higher-layer protocol.

	• **Broadcast Packets Received** – Indicates the total number of received good packets that were directed to the broadcast address.
Receive Packets Discarded	Indicates the number of inbound packets that were selected for discard even though no errors preventing their delivery to a higher-layer protocol had been detected. One potential reason for discarding such packets would be to free up buffer space.
Packets Received with MAC Errors	• **Total Packets Received with MAC Errors** – Indicates the total number of inbound packets containing errors that prevented them from being delivered to a higher-layer protocol. • **Jabbers Received** – Indicates the number of received packets that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with a non-integral number of octets (Alignment Error) or a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error). It should be noted that this definition of a jabber is different than that provided in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define a jabber as any packet exceeding 20 ms. The allowed range for detecting a jabber is between 20 ms and 150 ms. • **Fragments/Undersize Received** – Indicates the total number of received packets that were less than 64 octets in length (excluding framing bits but including FCS octets). • **Alignment Errors** – – Indicates the total number of received packets that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets inclusive, but that also had a bad Frame Check Sequence (FCS) with a non-integral number of octets. • **FCS Errors** – – Indicates the total number of received packets that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets inclusive, but that also had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Overruns** – Indicates the total number of frames that were discarded as this port was overloaded with incoming packets, such that it could not keep up with the inflow.
Received Packets Not Forwarded	• **Total Received Packets Not Forwarded** – Indicates the count of valid received frames that were discarded (that is, filtered) by the forwarding process. • **802.3x Pause Frames Received** – Indicates the count of MAC Control frames with an opcode indicating the PAUSE operation that were received on this interface. This count does not change when the interface is operating in half-duplex mode. • **Unacceptable Frame Type** – Indicates the number of frames discarded from this port because they were of an unacceptable frame type.
Packets Transmitted Octets	• **Total Packets Transmitted (Octets)** – Indicates the total number of octets of data received on the network (excluding framing bits but including FCS octets and those in bad packets). This parameter provides a reasonable estimate of Ethernet utilization. If the user requires greater precision, the etherStatsOctets and etherStatsPkts objects should be sampled

	before and after a common interval. • **Packets Transmitted 64 Octets** – Indicates the total number of received packets (including bad packets) that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Transmitted 65-127 Octets** – Indicates the total number of received packets (including bad packets) that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 128-255 Octets** – Indicates the total number of received packets (including bad packets) that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 256-511 Octets** – Indicates the total number of received packets (including bad packets) that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 512-1023 Octets** – Indicates the total number of received packets (including bad packets) that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 1024-1518 Octets** – Indicates the total number of received packets (including bad packets) that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted > 1518 Octets** – Indicates thehe total number of transmitted packets that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Max Frame Size** – Indicates the maximum size of the Info (non-MAC) field that the port in question will receive or transmit. • **Maximum Transmit Unit** – Indicates the maximum Ethernet payload size for the port.
Packets Transmited Successfully	• **Total Packets Transmitted Successfully** – Indicates the number of frames that have successfully been transmitted by the port to its segment. • **Unicast Packets Transmitted** – Indicates the total number of packets, including those that were discarded or not sent, that higher-level protocols asked to be transmitted to a subnetwork-unicast address. • **Broadcast Packets Transmitted** – Indicates the total number of packets, including those that were discarded or not sent, that higher-level protocols asked to be transmitted to the Broadcast address.
Transmit Packets Discarded	Indicates the number of outbound packets that were selected for discard even though no errors preventing their delivery to a higher-layer protocol had been detected. One potential reason for discarding such packets would be to free up buffer space..
Transmit Errors	• **Total Transmit Errors** – Indicates the sum of Single, Multiple, and Excessive Collisions. • **Tx FCS Errors** – Indicates the total number of transmitted packets that had a length (excluding framing bits, but including

	FCS octets) from 64 to 1518 octets inclusive, but that also had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Oversized** – Indicates the total number of frames that exceeded the maximum permitted frame size. This count has a maximum increment rate of 815 counts per sec. at 10 Mb/s. • **Underrun Errors** – Indicates the total number of frames that were discarded due to the transmit FIFO buffer becoming empty during frame transmission.
Transmit Discards	• **Total Transmit Packets Discards** – Indicates the sum total of discarded single collision frames, multiple collision frames, and excesslve frames. • **Single Collision Frames** – Indicates the number of frames successfully transmitted on a particular interface for which transmission was inhibited by exactly one collision. • **Multiple Collision Frames** – Indicates the number of frames successfully transmitted on a particular interface for which transmission was inhibited by multiple collisions. • **Excessive Collisions** – Indicates the number of frames for which transmission failed on a particular interface due to excessive collisions.
Protocol Statistics	**802.3x Pause Frames Transmitted** – Indicates the number of MAC Control frames with an opcode indicating the PAUSE operation transmitted on this interface. This count does not change when the interface is operating in half-duplex mode.
Protocol Statistics	• **STP BPDUs Transmitted** – Indicates the number of Spanning Tree Protocol Bridge Protocol Data Units sent. • **STP BPDUs Received** – Indicates the number of Spanning Tree Protocol Bridge Protocol Data Units received. • **PVST BPDUs Transmitted** – Indicates the number of per VLAN Spanning Tree (PVST) units transmitted. • **PVST BPDUs Received** – Indicates the number of per VLAN Spanning Tree (PVST) units received. • **Rapid-PVST BPDUs Transmitted** – Indicates the number of Rapid per VLAN Spanning Tree (PVST) units transmitted. • **Rapid-PVST BPDUs Received** – Indicates the number of Rapid per VLAN Spanning Tree (PVST) units received. • **RSTP BPDUs Transmitted** – Indicates the number of Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. • **RSTP BPDUs Received** – Indicates the number of Rapid Spanning Tree Protocol Bridge Protocol Data Units received. • **MSTP BPDUs Transmitted** – Indicates the number of Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. • **MSTP BPDUs Received** – Indicates the number of Multiple Spanning Tree Protocol Bridge Protocol Data Units received. • **SSTP BPDUs Transmitted** – Indicates the number of Shared Spanning Tree Protocol Bridge Protocol Data Units sent. • **SSTP BPDUs Received** – Indicates the number of Shared Spanning Tree Protocol Bridge Protocol Data Units received.

Dot1x Statistics	• **EAPOL Frames Transmitted** – Indicates the number of EAPOL frames of any type transmitted by this authenticator. • **EAPOL Start Frames Received** – Indicates the number of valid EAPOL start frames received by this authenticator.
Time Since Counters Last Cleared	Indicates the elapsed time since the statistics for this port were last cleared in days, hours, minutes, and seconds.

If the **all** keyword is used, the following information is displayed.

Total Octets Transmitted	Indicates the total number of octets of data transmitted on the network (excluding framing bits but including FCS octets and those in bad packets). This parameter provides a reasonable estimate of Ethernet utilization. If the user requires greater precision, the etherStatsOctets and etherStatsPkts objects should be sampled before and after a common interval.
Total Octets Received	Indicates the total number of octets of data received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets and those in bad packets). This parameter provides a reasonable estimate of Ethernet utilization. If the user requires greater precision, the etherStatsOctets and etherStatsPkts objects should be sampled before and after a common interval. The result for this equation is the value utilization, which is itself the percent utilization (on a scale of 0 to 100 percent) of the Ethernet segment.
Total Packets Transmitted Successfully	Indicates the number of frames transmitted by this port to its segment.
Total Packets Received Without Error	Indicates the total number of packets that were received without errors.

5-24 show interface ethernet switchport

This command is used to show the information regarding private VLAN mapping for the switch interfaces.

show interface ethernet *interface-id* **switchport**

Parameters

interface-id	Indicates the slot/port for the switch.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

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

Port: 0/1
VLAN Switchport mode:Private Vlan Host
Private VLAN configured Host association:10 20
Private VLAN configured Promiscuous VLANS:
Operational Private VLANS :
```

Display Parameters

Port	The interface ID of the switch.
VLAN switchport mode	Indicates the particular configuration mode.
Private-vlan host-association	Indicates the VLAN association of the private-VLAN host ports.
Private-vlan mapping	Indicates the VLAN mapping of the private-VLAN promiscuous ports.
Operational private VLANS	Indicates the type of association to the interface.

5-25 show mac-addr-table

This command is used to show the forwarding database entries, which are utilized by the transparent bridging function to decide how to forward a received frame.

Enter either the all parameter or the no parameter to show the entire table. To display the table entry for a specific MAC address on the specified VLAN, enter that MAC Address and the VLAN ID. To view summary information about the forwarding database table, enter the count parameter. To view MAC addresses on a specific interface, use the interface {slot/port I lag Lag-id} parameter. To display information about MAC addresses on a specified VLAN, use the vlan vlan_id parameter.

show mac-addr-table [{*macaddr vlan_id* **| all | count | interface {***slot/port* **| lag** *lag-id* **| vlan** *vlan_id***} | vlan** *vlan_id***}]**

Parameters

macaddr	Select a 6 byte MAC address.
vlan_id	Indicates a VLAN ID.
all	Select to indicate all interfaces.
count	Indicates the FDB count.
interface	Indicates the MAC address on the interface.
slot/port	Indicates the slot/port of the interface.
lag *lag-id*	Select to enter interface lag mode.

vlan *vlan_id*	Select to enter VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show mac-addr-table

VLAN ID    MAC Address             Interface    IfIndex      Status
-------    --------------------    ----------   ----------   ----------
1          00:05:64:2F:0D:E5       cpu          235          Management
1          00:05:64:2F:0D:E6       cpu          235          Management
1          00:05:64:2F:0D:E7       cpu          235          Management
```

Display Parameters

The following information is shown if the user does not enter a parameter, the keyword **all**, or the MAC address and VLAN ID.

VLAN ID	Indicates the VLAN in which the MAC address is learned.
MAC Address	Indicates a unicast MAC address that the switch has forwarding and/or filtering information for. The format of the address consists of 6 two-digit hexadecimal numbers separated by colons (for example, **01:23:45:67:89:AB)**.
Interface	Indicates the port through which the address in question was learned.
Interface Index	Indicates the ifIndex of the interface table entry that is associated with the port in quesiton.
Status	Indicates the status of this entry. The meanings for the values are as follows: • **Static** – Indicates that the value of the corresponding instance was added by a user or the system when a static MAC filter was defined. This value cannot be relearned. • **Learned** – Indicates that the value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and that the value is currently in use. • **Management** – Indicates that the value of the corresponding instance (that is, the system MAC address) is also the value of an existing instance of the dot1dStaticAddress. The value is identified with interface 0/1. and is currently used when VLANs are enabled for routing. • **Self** – Indicates that the value of the corresponding instance consists of the address of one of the switch's physical interfaces (that is, the system's own MAC address). • **Other** – Indicates that the value of the corresponding instance

	does not fall under one of the aforementioned categories.

If the **vlan** *vlan_id* is entered, then only the MAC Address, interface, and Status fields will be displayed. If the **interface** *slot/port* parameter is entered, then the VLAN ID will also appear in addition to the MAC Address and Status fields.

The following information is displayed if the **count** parameter is entered:

Dynamic Address count	Indicates the number of MAC addresses in the forwarding database that have been automatically learned.
Static Address (User-defined) count	Indicates the number of MAC addresses in the forwarding database that have been manually entered by a user.
Total MAC Addresses in use	Indicates the number of MAC addresses currently included in the forwarding database.
Total MAC Addresses available	Indicates the number of MAC addresses that the forwarding database can handle.

5-26 process cpu threshold

This command is used to configure the CPU utilization thresholds, with the Rising and Falling thresholds being specified as a percentage of the CPU resources. The utilization monitoring time period must be in multiples of 5 seconds and can be configured to be any value from 5 seconds to 86400 seconds. The configuration of the CPU utilization threshold will be saved across any switch reboot. The configuration of the falling utilization threshold is optional. In the event that the falling CPU utilization parameters are not configured, then the same value used for the rising CPU utilization parameters will be used for the falling parameters.

process cpu threshold type total rising *1-100* **interval <5-86400> {[falling]** *1-100* **interval <5-86400> {[falling]** *1-100* **interval <5-86400>}**

Parameters

None

Default

The default is None.

Command Mode

Global Config

Display Parameters

rising threshold	Indicates the percentage of CPU resources that triggers a notification when exceeded by the configured rising interval (range: 1 to 100; default: 0 (disabled)).

rising interval	Indicates, the duration, in seconds, for the CPU rising threshold violation that must be met to trigger a notification (range: 5 to 86400; default: 0 (disabled)).
falling threshold	Indicates the percentage of CPU resources that triggers a notification when exceeded by the configured falling interval (range: 1 to 100; default: 0 (disabled)).In other words, when the total CPU utilization falls below the specified level for a configured period of time, a notification is triggered. Note that the falling utilization threshold notification is triggered only if a rising threshold notification was previously sent. The falling utilization threshold value must always be set at equal to or less than the rising threshold value.
falling interval	Indicates, the duration, in seconds, for the CPU falling threshold violation that must be met to trigger a notification (range: 5 to 86400; default: 0 (disabled)).

5-27 show process app-list

This command is used to show the user and system applications.

show process app-list

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

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

ID      Name          PID         Admin Status   Auto Restart    Running 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
```

Display Parameters

ID	Indicates the application identifier.
Name	Indicates the name that identifies the process.
PID	Indicates the number that the software uses to identify the process
Admin Status	Indicates the administrative status of the process.
Auto Restart	Indicates whether or not the process will be automatically restarted if it stops.
Running Status	Indicates whether or not the process is currently running.

5-28 show process proc-list

This command is used to show the configured and in-use processes.

show process proc-list

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

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

PID     Process Name    Application ID-Name  Chld  VM Size (KB) VM Peak (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
```

Display Parameters

PID	Indicates the number that the software uses to identify the process.

Process Name	Indicates the name that identifies the process.
Application ID-Name	Indicates the application identifier along with its associated name.
Child	Indicates whether or not the process has spawned a child process.
VM Size	Indicates the virtual memory size.
VM Peak	Indicates the maximum amount of virtual memory that the process has used at any given time.
FD Count	Indicates the file descriptors count for the process.

5-29 show process app-resource-list

This command is used to show the configured and in-use resources of each application.

show process app-resource-list

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

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

ID   Name            PID     Memory Limit    CPU Share   Memory Usage   Max Mem 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
```

Display Parameters

ID	Indicates the application identifier.
Name	Indicates the name that identifies the process.
PID	Indicates the number that the software uses to identify the process.

Memory Limit	Indicates the maximum amount of memory that the process can consume.
CPU Share	Indicates the maximum percentage of CPU utilization that the process can consume.
Memory Usage	Indicates the amount of memory that the process is using currently.
Max Mem Usage	Indicates the maximum amount of memory that the process has used at any time since it was started.

5-30 show process cpu threshold

This command is used to show the percentages of CPU utilization by different tasks.

It should be noted that it is not only the traffic to the CPU that could keep it busy, but the different tasks as well.

show process cpu threshold

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command using Linux.

```
(Switching)#show process cpu

Memory status   Utilization bytes    Report
--------------  -------------------
free            106450944
alloc           423227392

CPU Utilization:

PID     Name                    5 Secs     60 Secs    300 Secs
-------------------------------------------------------------------
765     _interrupt_thread       0.00%      0.01%      0.02%
767     L2X.0                   0.58%      0.35%      0.28%
768     CNTR.0                  0.77%      0.73%      0.72%
773     RX                      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%
```

5-31 show running-config

This command is used to show or record the current settings of different protocol packages supported on the switch. More specifically, it displays or records those commands with settings and configurations that are different from the default values. To display or record those commands with settings and configurations that remain equal to the default value, simply include the **all** option.

It should be noted that the Show running-config command does not show the User Password, even if one different from the default has been set.

The output for the command is displayed in script format, and the output can then be used to configure another switch with the same configuration. The output will be redirected to a script file if the optional *scriptname* is provided with a file name extension of ".scr".

Note: If the **show running-config** command is issued from a serial connection, access to the switch via remote connections (such as Telnet) will be suspended as the output is being generated and shown.

Note: If a text-based configuration file is used, then the **show running-config** command will only show the configured physical interfaces. That is, if any interface contains only the default configuration, then that interface will be skipped when generating the **show running-config** command output. (This is true, in fact, for any configuration mode for which nothing but the default configuration is used.) In other words, the command to enter a particular config mode, as well as its exit command, are both omitted from the generated **show running-config** command output. As a result, they are omitted from the startup-config file when the configuration for the system is saved.

The following keys should be used to navigate the command output.

Key	Action
Enter	Advances one line.
Space Bar	Advances one page.
q	Stops the output and returns to the prompt.

It should be noted that **--More--** or **(q)uit** is shown at the bottom of the output screen until the user reaches the end of the output.

This command is used to display the current settings for the OSPFv2 trapflag status:

- In the event that all the flags are enabled, then **trapflags all** will be displayed by the command.
- In the event that all the flags in a specific group are enabled, then the command will cause the trapflags *group name all* to be displayed.
- If only some but not all of the flags in said group are enabled, the command will cause the **trapflags** *groupname flag-name* to be displayed.

show running-config [all | interface | vpc | *scriptname***]**

Parameters

scriptname	(Optional) Indicates the script file name for writing active configuration.
all	(Optional) Select to display all the running configurations.
interface	Indicates the running configuration for a specified interface.
vpc	Indicates the vpc running configuration.

Default

The default is None.

Command Mode

Privileged EXEC

5-32 show running-config interface

This command is used to show the running configuration for a particular interface, with valid interfaces including physical LAG, tunnel, loopback, and VLAN interfaces.

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

Parameters

interface	Indicates the running configuration for the specified interface.
lag *lag-intf-num*	Indicates the running configuration for the LAG interface.
loopback *loopback-id*	Indicates the running configuration for the loopback interface.
tunnel *tunnel-id*	Indicates the running configuration for the tunnel interface.
vlan *vlan-id*	Indicates the running configuration for the VLAN routing interface.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

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

!Current Configuration:
!
interface 0/1
addport 3/1
```

```
exit
(Routing)#
```

Display Parameters

slot/port	Indicates a given interface in slot/port format.
lag	Indicates the running config for a particular lag interface.
loopback	Indicates the running config for a particular loopback interface.
tunnel	Indicates the running config for a particular tunnel interface.
vlan	Indicates the running config for a particular VLAN routing interface.

5-33 show {startup-config | backup-config | factory-defaults}

This command is used in the CLI to show the content of text-based configuration files (i.e., the startup-config, backup-config, and factory-defaults files) that are saved in a compressed form in flash. When this command is used, the files are decompressed when their content is shown.

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

Parameters

startup-config	Indicates the content of the startup-config file.
backup-config	Indicates the content of the backup-config file.
factory-defaults	Indicates the content of the factory-defaults file.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command when using the **startup-config** parameter.

```
(Routing)#show startup-config


!Current Configuration:
!
!System Description "DQS-5000-54SQ28 - 48 25GE + 6 100GE, 1.00.006, Linux 3.16.0-29-
generic"
!System Software Version   "1.00.006"
!System Up Time            "0 days 0 hrs 0 mins 29 secs"
!Additional Packages       BGP-4,QOS,Multicast,IPv6,Routing,Data Center
```

```
!Current System Time:      Apr 26 13:50:51 2018
!
vlan database
exit
configure
ip routing
vxlan enable
line console
exit
line telnet
exit
line ssh
exit
!
interface loopback 0
ip address 192.168.1.30 255.255.255.255
ip ospf area 1
exit
interface 0/49
speed 40G full-duplex
routing
ip address 2.2.2.2 255.255.255.252
ip ospf area 1
exit
interface 0/50
speed 40G full-duplex
routing
ip address 1.1.1.2 255.255.255.252
ip ospf area 1
exit
router ospf
router-id 192.168.1.30
exit
ipv6 router ospf
exit
exit
```

The following is an example of the CLI display output for the command when using the **backup-config** parameter.

```
(Routing)#show backup-config

!Current Configuration:
!
!System Description "DQS-5000-54SQ28 - 48 25GE + 6 100GE, 1.0.4, Linux 3.16.0-29-
generic"
!System Software Version   "1.00.006"
!System Up Time            "5 days 19 hrs 15 mins 33 secs"
!Additional Packages       BGP-4,QOS,Multicast,IPv6,Routing,Data Center
!Current System Time:      Apr 1 01:55:43 2018
!
```

```
serviceport protocol dhcp
network parms 10.90.90.13 255.255.255.0 0.0.0.0
vlan database
vlan 10,20,30
exit
configure
vxlan enable
line console
exit
line telnet
exit
line ssh
exit
spanning-tree configuration name "DLINK"
spanning-tree configuration revision 1
spanning-tree mst instance 1
spanning-tree mst priority 1 20480
spanning-tree mst vlan 1 10
spanning-tree mst instance 2
spanning-tree mst vlan 2 20
spanning-tree mst instance 3
spanning-tree mst vlan 3 30
interface 0/5
speed 10G full-duplex
addport 3/1
exit
interface 0/6
speed 10G full-duplex
addport 3/1
exit
interface 0/9
speed 10G full-duplex
addport 3/3
exit
interface 0/10
speed 10G full-duplex
addport 3/3
exit
!
snmp-server community "private" rw
interface 0/5
description 'Conn_SW4'
exit
interface 0/6
description 'Conn_SW4'
exit
interface 0/9
description 'Conn_SW2'
exit
interface 0/10
```

```
description 'Conn_SW2'
exit
interface lag 1
switchport mode access
exit
interface lag 3
switchport mode access
exit
router ospf
exit
ipv6 router ospf
router-id 3.3.3.3
exit
exit
```

The following is an example of the CLI display output for the command when using the **factory-defaults** parameter.

```
(Routing)#show factory-config

!Current Configuration:
!
!System Description "DQS-5000-54SQ28 - 48 25GE + 6 100GE, 1.00.006, Linux 3.16.0-29-
generic"
!System Software Version   "1.00.006"
!System Up Time            "0 days 0 hrs 0 mins 29 secs"
!Additional Packages       BGP-4,QOS,Multicast,IPv6,Routing,Data Center
!Current System Time:      Apr 26 13:50:51 2018
!
vlan database
exit
configure
ip routing
vxlan enable
line console
exit
line telnet
exit
line ssh
exit
!
interface 0/49
exit
interface 0/50
exit
router ospf
exit
ipv6 router ospf
exit
exit
```

5-34 show sysinfo

This command is used to show switch information.

show sysinfo

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show sysinfo

System Description.............................. DQS-5000-54SQ28 - 48 25GE + 6 100GE,
                                                 1.00.006, Linux 3.16.0-29-generic
System Name..................................... Switch
System Location.................................
System Contact..................................
System Object ID................................ 1.3.6.1.4.1.171.10.162.3.1
System Up Time.................................. 1 days 20 hrs 3 mins 44 secs Apr 25
01:38:00 2018 UTC

MIBs Supported:

RFC 1907 - SNMPv2-MIB              The MIB module for SNMPv2 entities
HC-RMON-MIB                        The original version of this MIB, published
                                   as RFC3273.
HCNUM-TC                           A MIB module containing textual conventions
                                   for high capacity data types.
SNMP-COMMUNITY-MIB                 This MIB module defines objects to help
                                   support coexistence between SNMPv1, SNMPv2,
                                   and SNMPv3.
SNMP-MPD-MIB                       The MIB for Message Processing and
                                   Dispatching
SNMP-TARGET-MIB                    The Target MIB Module
SNMP-VIEW-BASED-ACM-MIB            The management information definitions for
                                   the View-based Access Control Model for SNMP.
SFLOW-MIB                          sFlow MIB
NAX-ISDP-MIB                       Industry Standard Discovery Protocol MIB
NAX-BOXSERVICES-PRIVATE-MIB        The D-Link Private MIB for NAX Box Services
```

	Feature.
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
NAX-DENIALOFSERVICE-PRIVATE-MIB	The D-Link Private MIB for NAX Denial of Service.
LLDP-MIB	Management Information Base module for LLDP configuration, statistics, local system data and remote systems data components.
LLDP-EXT-MED-MIB	The LLDP Management Information Base extension module for TIA-TR41.4 Media Endpoint Discovery information.
NAX-OPENFLOW-PRIVATE-MIB	The D-Link Private MIB for NAX OpenFlow
SMON-MIB	The MIB module for managing remote monitoring device implementations for Switched Networks
NAX-TIMERANGE-MIB	The D-Link Private MIB for NAX Time Ranges
DISMAN-TRACEROUTE-MIB	The Traceroute MIB (DISMAN-TRACEROUTE-MIB) provides access to the traceroute capability at a remote host.
RFC 1213 - RFC1213-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 2674 - P-BRIDGE-MIB	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.
RFC 2737 - ENTITY-MIB	Entity MIB (Version 2)
RFC 3635 - Etherlike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types
NAX-INVENTORY-MIB	Unit and Slot configuration.
INET-ADDRESS-MIB	This MIB module defines textual conventions for representing Internet addresses.
NAX-LOGGING-MIB	This MIB provides objects to configure and display events logged on this system.
IANA-MAU-MIB	This MIB module defines dot3MauType OBJECT-IDENTITIES and IANAifMauListBits, IANAifMauMediaAvailable, IANAifMauAutoNegCapBits,
NAX-PFC-MIB	The MIB definitions Priority based Flow Control Feature.
NAX-VPC-MIB	The MIB definitions for VPC.
NAX-DOT1X-ADVANCED-FEATURES-MIB	The D-Link Private MIB for NAX Dot1x Advanced Features
NAX-RADIUS-AUTH-CLIENT-MIB	The D-Link Private MIB for NAX Radius Authentication Client.
RADIUS-AUTH-CLIENT-MIB	RADIUS Authentication Client MIB
-MANAGEMENT-ACAL-MIB	The D-Link Private MIB for NAX management acal feature.
RFC 1850 - OSPF-MIB	OSPF Version 2 Management Information Base
RFC 2787 - VRRP-MIB	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
IP-FORWARD-MIB	The MIB module for the management of CIDR

```
                                multipath IP Routes.
NAX-LOOPBACK-MIB                The D-Link Private MIB for NAX Loopback
NAX-BGP-MIB                     The MIB definitions for Border Gateway
                                Protocol Flex package.
NAX-QOS-ACL-MIB                 NAX Flex QOS ACL
NAX-QOS-AUTOVOIP-MIB            NAX Flex QOS VOIP
RFC 2932 - IPMROUTE-MIB         IPv4 Multicast Routing MIB
RFC 5060 - PIM-STD-MIB          Protocol Independent Multicast MIB
DVMRP-STD-MIB                   Distance-Vector Multicast Routing Protocol
                                MIB
NAX-MULTICAST-MIB               The MIB definitions for Multicast Routing
                                Flex package.
MGMD-STD-MIB                    The MIB module for MGMD Management.
RFC 2466 - IPV6-ICMP-MIB        Management Information Base for IP Version
                                6: ICMPv6 Group
NAX-ROUTING6-MIB                The D-Link Private MIB for NAX IPv6 Routing.
NAX-IPV6-LOOPBACK-MIB           The D-Link Private MIB for NAX Loopback IPV6
                                address configuration.
NAX-DCBX-MIB                    The MIB module defines objects to configure
                                DCBX
IEEE8021-CN-MIB                 Congestion notification module for managing
                                IEEE 802.1Qau
LLDP-V2-TC-MIB                  Textual conventions used throughout the IEEE
                                Std 802.1AB version 2 and later MIB modules.
```

Display Parameters

System Description	Indicates text used to identify the switch.
System Name	Indicates the name used to identify the switch. For this parameter, the factory default is blank. For instructions on how to configure the system name, please see “snmp-server”.
System Location	Indicates text used to specify the location of the switch. For this parameter, the factory default is blank. For instructions on how to configure the system location, please see “snmp-server”.
System Contact	Indicates text used to specify a contact person for the switch. For this parameter, the factory default is blank. For instructions on how to configure the system location, please see “snmp-server”.
System ObjectID	Indicates the base object ID for the switch’s enterprise MIB.
System Up Time	Indicates time since the last switch reboot in days, hours and minutes.
MIBs Supported	Indicates the list of MIBs supported by this agent.

5-35 show tech-support

The **show tech-support** command is used to show the system and configuration information for the whole system, or the information for BGP, BGP-IPv6, OSPF, or OSPFv3 when the user contacts technical support. The output for the command includes log history files from previous runs. The output of the command also combines the output for all of the following commands:

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

It should be noted that the log messages are sorted and then shown in reverse chronological order.

show tech-support [{bgp | datacenter | dcvpn | dot1q | dot1s | ipv6 | layer3 | link_dependency | lldp | log | routing | sim | switching | system] [file]} | file]

Parameters

bgp	Indicates bgp related information
datacenter	Indicates datacenter related information.
dcvpn	Indicates dcvpn related information.
dot1q	Indicates dot1q related information.
dot1s	Indicates dot1s related information.
dot3ad	Indicates dot3ad related information.
file	Indicates the file for output dump.
isdp	Indicates isdp related information.
layer3	Indicates layer3 related information.
link_dependency	Indicates link_dependency related information.
lldp	Indicates lldp related information.
log	Indicates log related information.
routing	Indicates routing related information.
sim	Indicates sim related information.
switching	Indicates switching related information.
system	Indicates system related information.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show tech-support

*************** show version ***************


Switch: 1

System Description.............................. DQS-5000-54SQ28 - 48 25GE + 6 100GE,
                                                 2.1.5, Linux 3.16.0-29-generic
Machine Type.................................... DQS-5000-54SQ28 - 48 25GE + 6 100GE
Machine Model................................... DQS-5000-54SQ28
Serial Number................................... 2N38C000068
Part Number..................................... BXS500054SAF.A1
Maintenance Level............................... A
Manufacturer.................................... D-LINK
Burned In MAC Address........................... 00:05:64:2F:0D:E5
Software Version................................ 1.00.006
Operating System................................ Linux 3.16.0-29-generic
Network Processing Device....................... 9324_B1
Additional Packages............................. BGP-4
................................................. QOS
................................................. Multicast
................................................. IPv6
................................................. Routing
................................................. Data Center
................................................. OpEN API
................................................. Prototype Open API

*************** show sysinfo ***************


System Description.............................. DQS-5000-54SQ28 - 48 25GE + 6 100GE,
                                                 2.1.5, Linux 3.16.0-29-generic
System Name.....................................  Switch
System Location.................................
System Contact..................................
System Object ID................................  1.3.6.1.4.1.171.10.162.3.1
System Up Time..................................  1 days 20 hrs 9 mins 18 secs Apr 25
                                                 01:43:34 2018 UTC

MIBs Supported:

RFC 1907 - SNMPv2-MIB........................... The MIB module for SNMPv2 entities
HC-RMON-MIB..................................... The original version of this MIB,
                                                 published as RFC3273.
HCNUM-TC........................................ A MIB module containing textual
                                                 conventions for high capacity data
                                                 types.
```

SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-TARGET-MIB	The Target MIB Module
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
SFLOW-MIB	sFlow MIB
NAX-ISDP-MIB	Industry Standard Discovery Protocol MIB
NAX-BOXSERVICES-PRIVATE-MIB	The Private MIB for NAX Box Services Feature.
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
NAX-KEYING-PRIVATE-MIB	The Private MIB for NAX Keying Utility
LLDP-EXT-DOT3-MIB	The LLDP Management Information Base extension module for IEEE 802.3 organizationally defined discovery information.
NAX-LLPF-PRIVATE-MIB	The Private MIB for NAX Link Local Protocol Filtering.
DISMAN-PING-MIB	The Ping MIB (DISMAN-PING-MIB) provides the capability of controlling the use of the ping function at a remote host.
NAX-OUTBOUNDTELNET-PRIVATE-MIB	The Private MIB for NAX Outbound Telnet
NAX-TIMEZONE-PRIVATE-MIB	The Private MIB for NAX for system time, timezone and summer-time settings
LAG-MIB	The Link Aggregation module for managing IEEE 802.3ad
RFC 1493 - BRIDGE-MIB	Definitions of Managed Objects for Bridges (dot1d)
RFC 2674 - Q-BRIDGE-MIB	The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks
RFC 2863 - IF-MIB	The Interfaces Group MIB using SMIv2
NAX-SWITCHING-MIB	NAX Switching - Layer 2
NAX-PORTSECURITY-PRIVATE-MIB	Port Security MIB.
IANAifType-MIB	This MIB module defines the IANAifType Textual Convention
MAU-MIB	Management information for 802.3 MAUs.
NAX-MVR-PRIVATE-MIB	The Private MIB for MVR Configuration
IEEE8021-PFC-MIB	Priority-based Flow Control module for managing IEEE 802.1Qbb
IEEE8021-PAE-MIB	Port Access Entity module for managing IEEE 802.1X.
NAX-DOT1X-AUTHENTICATION-SERVER-MIB	The Private MIB for NAX Dot1x Authentication Server
RADIUS-ACC-CLIENT-MIB	RADIUS Accounting Client MIB

```
TACACS-CLIENT-MIB.............................. Defines a portion of the SNMP MIB
                                                under the OID pertaining to TACACS+
                                                client configurati
NAX-MGMT-SECURITY-MIB.......................... The Private MIB for NAX Mgmt
                                                Security
RFC 1850 - OSPF-TRAP-MIB....................... The MIB module to describe traps for
                                                the OSPF Version 2 Protocol.
NAX-ROUTING-MIB................................ NAX Routing - Layer 3
IP-MIB......................................... The MIB module for managing IP and
                                                ICMP implementations, but excluding
                                                their management of IP routes.
RFC 1657 - BGP4-MIB............................ Definitions of Managed Objects for
                                                the Fourth Version of the Border
                                                Gateway Protocol (BGP-4) using SMIv2
NAX-QOS-MIB.................................... NAX Flex QOS Support
NAX-QOS-COS-MIB................................ NAX Flex QOS COS
NAX-QOS-DIFFSERV-PRIVATE-MIB................... NAX Flex QOS DiffServ Private MIBs'
                                                definitions draft-ietf-magma-mgmd-
                                                mib-03 MGMD MIB, includes IGMPv3 and
                                                MLDv2.
RFC 5240 - PIM-BSR-MIB......................... Bootstrap Router mechanism for PIM
                                                routers
IANA-RTPROTO-MIB............................... IANA IP Route Protocol and IP MRoute
                                                Protocol Textual Conventions
IPMROUTE-STD-MIB............................... The MIB module for management of IP
                                                Multicast routing, but independent
                                                of the specific multicast routing
                                                protocol in use.
RFC 2465 - IPV6-MIB............................ Management Information Base for IP
                                                Version 6: Textual Conventions and
                                                General Group
RFC 3419 - TRANSPORT-ADDRESS-MIB............... Textual Conventions for Transport
                                                Addresses
NAX-DHCP6SERVER-PRIVATE-MIB.................... The Private MIB for NAX DHCPv6
                                                Server/Relay
NAX-IPV6-TUNNEL-MIB............................ The Private MIB for NAX IPV6 Tunnel.
NAX-FIPSNOOPING-MIB............................ The MIB module defines objects to
                                                configure FIP snooping and monitor
                                                the status of FCoE sessions.
IEEE8021-TC-MIB ............................... Textual conventions used throughout
                                                the various IEEE 802.1 MIB modules.


*************** show hardware ***************



Unrecognized command : show hardware

Error! Command 'show hardware' doesn't exist.
Hence aborting TechSupport execution.

*************** show running-config ***************

!Current Configuration:
!
!System Description "DQS-5000-54SQ28 - 48 25GE + 6 100GE, 1.00.006, Linux 3.16.0-29-
generic"
```

```
!System Software Version "1.00.006"
!System Up Time          "1 days 20 hrs 9 mins 18 secs"
!Additional Packages     BGP-4,QOS,Multicast,IPv6,Routing,Data Center
!Current System Time: Apr 25 01:43:34 2018
!
vlan database
exit
configure
ipv6 pim sparse
ipv6 pim ssm default
vxlan enable
line console
exit
line telnet
exit
line ssh
exit
!
interface 0/1
ip address 10.1.1.2 255.255.0.0
ipv6 pim join-prune-interval 90
ip igmp
ip pim join-prune-interval 90
exit
router ospf
exit
ipv6 router ospf
exit
process cpu threshold type total rising 100 interval 5 falling 100 interval 5
exit

*************** debug crash & kernel logs ***************


*************** Debug crashlog 0 unit 1 ********
Displaying FASTPATH Crash Dump 0
For kernel Crash Dump - osapiDebugCrashDumpDisplay(x,1)
Crash Dump 0 is not found


                                    <Output truncated>
```

5-36 length value

This command is persistent and is used to set the pagination length to a specific number of lines for the sessions specified through configuring on different Line Config modes (telnet/ssh/console).

It should be noted that the **length** command on the Line Console mode applies for Serial Console sessions.

length *value*

no length *value*

Parameters

None

Default

The default is 24.

Command Mode

Line Config

5-37 show terminal length

This command is used to show all the configured terminal length values.

show terminal length

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the 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
```

5-38 memory free low-watermark processor

This command is used to ensure that a notification is sent when the CPU free memory falls below a configured threshold.. Subsequenlty, another notification is produced and sent when the available free memory increases to 10 percent above the specified threshold. However, only one Rising or Falling

memory notification will be generated over any period of 60 seconds in order to prevent the generation of excessive notifications when the free memory fluctuates around the configured threshold, which is specified in kilobytes. A given CPU free memory threshold configuration will be saved across a switch reboot.

memory free low-watermark processor *1-1034956*

Parameters

low-watermark	Indicates the threshold at which a notification message is triggered when the CPU free memory falls below the threshold (range: 1 to the maximum available memory on the switch; default: 0 (disabled)).

Default

The default is None.

Command Mode

Global Config

5-39 clear mac-addr-table

This command is used to dynamically clear any learned entries from the forwarding database. Using the options discussed below, the user can specify the particular set of dynamically-learned forwarding database entries to be cleared.

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

Parameters

all	This parameter causes all the dynamically learned forwarding database entries in the forwarding database table to be cleared.
vlan *vlanId*	This parameter causes all the dynamically learned forwarding database entries for the given vlanId to be cleared.
interface *slot/port*	This parameter causes all the forwarding database entries learned on for the given interface to be cleared.
macAddr [macMask]	This parameter causes all the dynamically learned forwarding database entries that match the range indicated by the MAC address and MAC mask to be cleared. When a MAC mask is not entered, only the specified MAC is cleared from the forwarding database table. MAC address format EEEE.EEEE.EEEE.

Default

The default is None.

Command Mode

Privileged EXEC

Logging Commands

In this section, the commands used to configure the system logging and to view logs and the logging settings are described.

5-40 logging buffered

This command is used to enable logging in to an in-memory log.

The **no** command is used to disable logging in to an in-memory log.

logging buffered

no logging buffered

Parameters

None

Default

The default is Enable.

Command Mode

Global Config

5-41 logging buffered wrap

This command is used to enable the wrapping of in-memory logging when the log file achieves full capacity. Otherwise, the logging will stop when the log file reaches full capacity.

The **no** command is used to disable the wrapping of in-memory logging and configures the logging to be stopped when the log file reaches full capacity.

logging buffered wrap

no logging buffered wrap

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

5-42 logging cli-command

This command is used to enable the CLI command logging feature, which in turn makes the D-LINK OS software capable of logging all the CLI commands issued on the system, with those commands being stored in a persistent log. The **show logging persistent** command is used to show the stored history of CLI commands.

The **no** command is used to disable the CLI command logging feature.

logging cli-command

no logging cli-command

Parameters

None

Default

The default is Disable.

Command Mode

Global Config

5-43 logging console

This command is used to enable logging on to the console. The user can specify the *severitylevel* value as either an integer from 0 to 7 or in a symbolic fashion through the use of one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

The **no** command is used to disable logging on to the console.

logging console [*severitylevel***]**

no logging console

Parameters

severitylevel	(Optional) Select the Logging Severity Level.

Default

The default is Enable.

Command Mode

Global Config

5-44 logging host

This command is used to configure the logging host parameters and allows for the configuration of up to eight hosts.

logging host {*hostaddress* **|** *hostname***}** *addresstype tls* **[anon | x509name]** *certificate-index* **{***port severitylevel***}**

Parameters

hostaddress **|** *hostname*	Indicate the IP address of the logging host.
addresstype	Indicates the type of address being passed (that is, DNS or IPv4).
tls	This parameter is used to enable TLS security for the host.
anon | x509name	(Optional) Indicates the type of authentication mode (that is, anonymous or x509name).
certificate-index	Indicates the certificate number that will be used for authentication (range: 0-8, with index 0 being used for the default file).
port	(Optional) Indicates a port number from 1 to 65535.
severitylevel	(Optional) The value for this parameter can be specified as either an integer from 0 to 7 or in a symbolic fashion through the use of one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default

The default is as follows:

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

Command Mode

Global Config

Example

The following is an example of the CLI display output for 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
```

5-45 logging host reconfigure

This command is used to enable logging host reconfiguration.

logging host reconfigure *hostindex*

Parameters

hostindex	This parameter can be used to enter the Logging Host Index for which to change the IP address.

Default

The default is None.

Command Mode

Global Config

5-46 logging host remove

This command is used to disable logging to host. Please see "show logging hosts" for a list of the host indexes.

logging host remove *hostindex*

Parameters

hostindex	Indicates the Logging Host index to be removed.

Default

The default is None.

Command Mode

Global Config

5-47 logging persistent

This command is used to configure the persistent logging for the switch, with the severity level parameter use to specify the logging messages of different severities. Potential values for the severity level are as follows: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), **debug** (7).

The **no** command is used to disable the persistent logging in the switch.

logging persistent *severity level*

no logging persistent

Parameters

severity level	Indicates the Logging Severity level.

Default

The default is Disabled.

Command Mode

Global Config

5-48 logging protocol

This command is used to configure the logging protocol version number as either 0 or 1. Version 0 is used by RFC 3164 and version 1 is used by RFC 5424.

logging protocol {0 | 1}

Parameters

None

Default

The default is 0 (RFC 3164).

Command Mode

Global Config

5-49 logging syslog

This command is used to enable syslog logging. The optional **facility** parameter can be used to set the default facility used in syslog messages for those components without an internally assigned facility. The *facility* value can consist of one of the following keywords: **kernel**, **user**, **mail**, **system**, **security**, **syslog**, **lpr**, **nntp**, **uucp**, **cron**, **auth**, **ftp**, **ntp**, **audit**, **alert**, **clock**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, **local7**. The default facility is **local7**.

The **no** command is used to disable syslog logging.

logging syslog [facility *facility***]**

no logging syslog [facility *facility***]**

Parameters

facility *facility*	Indicates the Syslog Facility.

Default

The default is Disabled.

Command Mode

Global Config

5-50 logging syslog port

This command is used to enable syslog logging. The value for the *portid* parameter consists of an integer within the range of 1-65535.

The **no** command is used to disable syslog logging.

logging syslog port *1-65535*

no logging syslog port

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-51 logging syslog source-interface

This command is used to specify the logical or physica interface used as the Syslog client source interface. If configured, the source interface address is used for all Syslog communications between the Syslog client and the Syslog server. Otherwise, there will be no change in behavior. Also, the Syslog client will revert to normal behavior if the configured interface is down.

The **no** command is used to remove the configured global source interface (that is, the Source IP selection) for all Syslog communications between the Syslog server and the Syslog client.

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

no logging syslog source-interface

Parameters

slot/port	Indicates the port to be used as the source interface.

loopback *loopback-id*	Indicates the loopback interface to be used as the source interface (range: 0 to 7).
tunnel *tunnel-id*	Indicates the tunnel interface to be used as the source interface (range: 0 to 7).
vlan *vlan-id*	Indicates the VLAN to be used as the source interface.

Default

The default is None.

Command Mode

Global Config

5-52 show logging

This command is used to display the logging configuration information.

show logging

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show logging

Logging Client Local Port               : 514
Logging Client USB File Name            :
Logging Client Source Interface         : (not configured)
CLI Command Logging                     : disabled
Console Logging                         : enabled
Console Logging Severity Filter         : error
Buffered Logging                        : enabled
Buffered Logging Severity Filter        : info
Persistent Logging                      : disabled
Persistent Logging Severity Filter      : alert

Syslog Logging                          : disabled
Syslog Logging Facility                 : local7
```

```
Log Messages Received                    : 229
Log Messages Dropped                     : 0
Log Messages Relayed                     : 0
```

Display Parameters

Logging Client Local Port	Indicates the port on the collector/relay that syslog messages are sent to.
Logging Client Source Interface	Indicates the configured syslog source-interface (source IP address).
CLI Command Logging	Indicates whether CLI Command logging is enabled.
Logging Protocol	Indicates the logging protocol version number. • 0: RFC 3164 • 1: RFC 5424
Console Logging	Indicates whether console logging is enabled.
Console Logging Severity Filter	Indicates the minimum severity for logging to the console log. Specifically, messages with a numerical severity equal to or lower than the minimum severity are logged.
Buffered Logging	Indicates whether buffered logging is enabled.
Persistent Logging	Indicates whether persistent logging is enabled.
Persistent Logging Severity Filter	Indicates minimum severity at which the log entries are retained after a system reboot.
Syslog Logging	Indicates whether syslog logging is enabled.
Syslog Logging Facility	Indicates the value set for the facility in syslog messages.
Log Messages Received	Indicates the number of messages that the log process has received, including messages that were dropped or ignored.
Log Messages Dropped	Indicates the number of messages that could not be processed because of errors or a lack of resources.
Log Messages Relayed	Indicates the number of messages sent to the collector/relay.

5-53 show logging buffered

This command is used to show buffered logging (that is, the system startup and system operation logs).

show logging buffered

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show logging buffered

Buffered (In-Memory) Logging              : enabled
Buffered Logging Wrapping Behavior        : On
Buffered Log Count                        : 210

<190> Apr 27 08:17:16 DQS-5000-54SQ28-2011 PROCMGR[emWeb]: proc_cnfgr.c(714) 1009 %%
No more data in file /tmp/procmgr-app-resource-list.txt
<190> Apr 27 08:16:59 DQS-5000-54SQ28-2011 PROCMGR[emWeb]: proc_cnfgr.c(521) 1008 %%
No more data in file /tmp/procmgr-proc-list.txt
<190> Apr 27 08:16:43 DQS-5000-54SQ28-2011 PROCMGR[emWeb]: proc_cnfgr.c(319) 1007 %%
No more data in file /tmp/procmgr-app-list.txt
```

Display Parameters

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

5-54 show logging hosts

This command is used to show all configured logging hosts.

show logging hosts

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show logging hosts

Index   IP Address/Hostname  Severity   Port    Status  Mode    Auth         Cert#
-----   -------------------  --------   ----    ------  ----    -----------  -----
1       1.1.1.17             critical   514     Active  udp     x509name     6
2       10.130.191.90        debug      10514   Active  tls     x509name     4
3       5.5.5.5              debug      333     Active  tls
```

Display Parameters

Host Index	(This parameter is used for deleting hosts.)
IP Address / Hostname	Indicates the IP address or the hostname of the logging host.
Severity Level	Indicates the minimum severity to log to the given address. The possible values are as follows: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), and debug (7).
Port	Indicates the server port number, which is the port from which syslog messages are sent on the local host.
Status	Indicates the current snmp row status (that is, Active, Not in Service, or Not Ready).
Mode	Indicates the type of security: UDP or TLS.
Auth	Indicates the type of authentication mode: anonymous or x509name.
Cert #	Indicates the certificate number used for authentication (range: 0-8, with Index 0 being used as the default file).

5-55 show logging persistent

The show logging persistent command is used to show persistent log entries. In the event that log-files is specified, then the persistent log files of the system are shown.

show logging persistent [log-files]

Parameters

log-files	(Optional) Indicates the list of persistent log files existing in the system.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the 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
```

Display Parameters

Persistent Logging	Indicates whether persistent logging is enabled or disabled.
Persistent Log Count	Indicates the number of persistent log entries.
Persistent Log Files	Indicates the list of persistent log files in the system. This list will only be displayed if log-files is specified.

5-56 show logging traplogs

This command is used to show SNMP trap events and statistics.

show logging traplogs

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show logging traplogs
```

```
Number of Traps Since Last Reset.................. 84
Trap Log Capacity................................. 256
Number of Traps Since Log Last Viewed............. 84

Log  System Up Time          Trap
---  ----------------------  ------------------------------------------------------
0    Apr 27 08:04:56 2018    Session 0 of type 1 started for user admin connected from
                             EIA-232.
1    Apr 27 08:04:52 2018    Session 0 of type 1 ended for user admin connected from
                             EIA-232.
2    Apr 27 07:55:32 2018    Session 0 of type 1 started for user admin connected from
                             EIA-232.
3    Apr 27 07:55:09 2018    Session 0 of type 1 ended for user admin connected from
                             EIA-232.
---  ----------------------  ------------------------------------------------------
```

Display Parameters

Number of Traps Since Last Reset	Indicates the number of traps since the previous boot.
Trap Log Capacity	Indicates the number of traps that the system can retain.
Number of Traps Since Log Last Viewed	Indicates the number of new traps since the command was last executed.
Log	Indicates the log number.
System Time Up	Indicates the length of time that the system had been running for at the time the trap was sent.
Trap	Indicates the text of the trap message.

5-57 clear logging buffered

This command is used to clear buffered logging (that is, the system startup and system operation logs).

clear logging buffered

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Email Alerting and Mail Server Commands

5-58 logging email

This command is used to enable email alerts and to set the lowest severity level for the emailing of log messages. Specifically, if the user specifies a severity level, then log messages with a severity at or above this level but below the urgent severity level are emailed in a non-urgent manner by being collected together and then emailed when the log time expires. The *severitylevel* value can be specified as either an integer from 0 to 7 or in a symbolic manner with one of the keywords that follows: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), and **debug** (7).

The **no** command is used to disable email alerts.

logging email {*severity* **| from-addr | logtime | message-type | test | urgent}**

no logging email

Parameters

severity	(Optional) Indicates the serverity level of the email alert.
from-addr	Indicates the sender address configuration for the email alert.
logtime	Indicates the log duration configuration in minutes, range: 30 – 1440 minues.
message-type	Indicates the message configuration type: urgent, non-urgent, both.
test	Indicates the test configuration for the email alert configuration.
urgent	Indicates the urgent log message.

Default

The default is Disabled.

Command Mode

Global Config

5-59 logging email urgent

This command is used to set the lowest severity level for which log messages will be e-mailed immediately in a single e-mail message. The *severitylevel* value can be specified as either an integer from 0 to 7 or in a symbolic manner with one of the keywords that follows: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), and **debug** (7). Alternatively, **none** can be specified in order to indicate that log messages are to be collected and sent together in a batch email at a specified interval.

The **no** command is used to reset the urgent severity level back to the default value.

logging email urgent {*severity* **| none}**

no logging email urgent

Parameters

severity	Indicates the severity level of the alert.
none	Indicates that no log messages are emailed as urgent.

Default

The default is as follows: log messages with the Alert (1) and Emergency (0) severity levels are sent immediately.

Command Mode

Global Config

5-60 logging email message-type to-addr

This command is used to configure the email address to which messages are to be sent. The following message types are supported: **urgent**, **non-urgent**, and **both**. Furthermore, multiple email addresses can be configured for each supported severity level. The *to-email-addr* variable will consist of a standard email address, such as, for example, admin@yourcompany.com.

The **no** command is used to remove the configured to-addr field.

logging email message-type {urgent | non-urgent | both} to-addr *to-email-addr*

no logging email message-type {urgent | non-urgent | both} to-addr *to-email-addr*

Parameters

both	Indicates both urgent and non urgent message types.
non-urgent	Indicates non urgent message types.
urgent	Indicates urgent message types.
to-addr *to-email-addr*	Indicates the email address recipient.

Default

The default is None.

Command Mode

Global Config

5-61 logging email from-addr

This command is used to configure the email address of the sender (that is, the switch).

The **no** command is used to remove the configured email source address.

logging email from-addr *from-address*

no logging email from-addr *from-address*

Parameters

from-addr *from-address*	Indicates the sender email address.

Default

The default is service@dlink.com.

Command Mode

Global Config

5-62 logging email message-type subject

This command is used to configure the subject line used for an email of the specified type.

The **no** command is used to remove the configured email subject line for emails of the specified message type and thus restores the subject line to the default email subject.

logging email message-type {urgent | non-urgent | both} subject *subject*

no logging email message-type {urgent | non-urgent | both} subject *subject*

Parameters

both	Indicates both urgent and non urgent message types.
non-urgent	Indicates non urgent message types.
urgent	Indicates urgent message types.
subject *subject*	Indicates the subject line for the email alert.
to-addr *to-address*	Indicates the recipient email address for the alert.

Default

The default is as follows:

- For urgent messages, the subject line, by default, is “Urgent Log Messages”.
- For non-urgent messages, the subject line, by default, is “Non Urgent Log Messages”.

Command Mode

Global Config

5-63 logging email logtime

This command is used to configure the frequency with which non-urgent email messages are sent. That is, non-urgent messages will be collected and sent together in a batch email at the specified interval (valid range: every 30-1440 minutes).

The **no** command is used by default to reset the non-urgent log time back to the default value.

logging email logtime *30-1440*

no logging email logtime

Parameters

None

Default

The default is 30.

Command Mode

Global Config

5-64 logging traps

This command is used to set the severity level at which SNMP traps are to be logged and sent in an email. The *severitylevel* value can be specified as either an integer from 0 to 7 or in a symbolic manner with one of the keywords that follows: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), and **debug** (7).

The **no** command is used to reset the logging severity level for SNMP traps back to the default value.

logging traps *severitylevel*

no logging traps

Parameters

severitylevel	Indicates the alert trap severity level.

Default

The default is as follows: messages with a severity level of 6 or higher are logged.

Command Mode

Global Config

5-65 logging email test message-type

This command is used to send an email to the SMTP server in order to test the email alert function.

logging email test message-type {urgent | non-urgent | both} message-body *msg-body*

Parameters

both	Indicates both urgent and non urgent message types.
non-urgent	Indicates non urgent message types.
urgent	Indicates urgent message types.
message-body *msg-body*	Indicates the message string for the email body of the alert message.

None

Default

The default is No default value.

Command Mode

Global Config

5-66 show logging email config

This command is used to show information about the configuration.

show logging email config

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show logging email config

Email Alert Logging.............................. disabled
```

```
Email Alert From Address..................... service@dlink.com
Email Alert Urgent Severity Level............ alert
Email Alert Non Urgent Severity Level........ warning
Email Alert Trap Severity Level.............. info
Email Alert Notification Period.............. 30 min

Email Alert To Address Table:

Email Alert Subject Table:
For Msg Type urgent, subject is.............. Urgent Log Messages
For Msg Type non-urgent, subject is.......... Non Urgent Log Messages
```

Display Parameters

Email Alert Logging	Indicates whether the feature is enabled or disabled.
Email Alert From Address	Indicates the email address of the sender (that is, the switch).
Email Alert Urgent Severity Level	Indicates the lowest severity level that is considered to be urgent. Messages with this level of severity or above are sent immediately.
Email Alert Non Urgent Severity Level	Indicates the lowest severity level that is considered to be non-urgent. Messages with this level of severity and above, up to the designated urgent level, are collected and sent together in a batch email. Any log messages with a lower level of severity are not sent via email message at all.
Email Alert Trap Severity Level	Indicates the lowest severity level at which traps are logged.
Email Alert Notification Period	Indicates the amount of time to wait between the sending of non-urgent messages.
Email Alert to Address Table	Indicates the configured email recipients.
Email Alert Subject Table	Indicates the subject lines to be included with emails of urgent (Type 1) and non-urgent (Type 2) messages.
For Msg Type urgent, subject is	Indicates the configured email subject for the sending of urgent messages.
For Msg Type non-urgent, subject is	Indicates the configured email subject for the sending of non-urgent messages.

5-67 show logging email statistics

This command is used to show email alerting statistics.

show logging email statistics

Parameters

None

Default

The default is No default value.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show logging email statistics

Email Alert operation status..................... disabled

Email Alert Statistics:
No of email Failures so far...................... 0
No of email sent so far.......................... 0
Time since last email Sent....................... 00 days 00 hours 00 mins 00  secs
```

Display Parameters

Email Alert Operation Status	Indicates the operational status of the email alert feature.
No of Email Failures	Indicates the number of email messages for which unsuccessful send attempts have been made.
No of Email Sent	Indicates the number of email messages that have been sent from the switch since the counter was last cleared.
Time Since Last Email Sent	Indicates the amount of time since the most recent email was sent from the switch.

5-68 clear logging email statistics

This command is used to reset the email alerting statistics.

clear logging email statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-69 mail-server

This command is used to configure the SMTP server to which email alert messages are sent by the switch and also to change the mode to the Mail Server Configuration mode. The address of the server can be in either the IPv4 or DNS name format.

The **no** command is used to remove the previously specified SMTP server from the configuration.

mail-server {*ip-address* **| ipv6address |** *hostname***}**

no mail-server {*ip-address* **| ipv6address |** *hostname***}**

Parameters

ipaddress	Indicates the IP address of the mail server.
Ipv6address	Indicates the IPv6 address of the mail server.
Host-name	Indicates the hostname of the mail server.

Default

The default is None.

Command Mode

Global Config

5-70 security

This command is used to set the email alerting security protocol by enabling the use of TLS authentication by the switch with the SMTP Server. However, no email will be sent to the SMTP server if the TLS mode is enabled on the switch but is not supported by the SMTP server itself.

security {tlsv1 | none}

Parameters

none	Indicates normal socket communication.
tlsv1	Indicates TLSv1 socket communication.

Default

The default is None.

Command Mode

Mail Server Config

5-71 port (Mail Server Config Mode)

This command is used to configure the TCP port that is to be used for communication with the SMTP server. For TLSv1, the recommended port is 465, whereas for no security (i.e., none), it is 25. However, the allowed range of ports is any nonstandard port in the range from 1 to 65535.

port {465 | 25 | *1-65535***}**

Parameters

None

Default

The default is 25.

Command Mode

Mail Server Config

5-72 username (Mail Server Config)

This command is used to configure the login ID used by the switch to perform authentication with the SMTP server.

username *name*

Parameters

username	Indicates the mail server username configuration. Username length: 1 to 49 characters.

Default

The default is admin.

Command Mode

Mail Server Config

5-73 password (Mail Server Config Mode)

This command is used to configure the password used by the switch to perform authentication with the SMTP server.

password *password*

Parameters

password	Indicates the password string for the mail server configuration.

Default

The default is admin.

Command Mode

Mail Server Config

5-74 show mail-server config

This command is used to show information regarding the email alert configuration.

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

Parameters

ip-address	Indicates the IP address for the mail server configuration.
hostname	Indicates the hostname for the mail server configuration.
all	Indicates all the configuration settings for the mail server.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show mail-server all config

Mail Servers Configuration:
No of mail servers configured..................... 1
Email Alert Mail Server Address.................. 192.168.1.1
Email Alert Mail Server Port..................... 25
Email Alert SecurityProtocol..................... none
Email Alert Username............................. Tester
```

```
Email Alert Password.............................. 123456789
```

Display Parameters

No of mail servers configured	Indicates the number of SMTP servers that are configured on the switch.
Email Alert Mail Server Address	Indicates the IPv4 address or DNS hostname for the configured SMTP server.
Email Alert Mail Server Port	Indicates the TCP port used by the switch to send email to the SMTP server.
Email Alert Security Protocol	Indicates the security protocol (TLS or none) used by the switch to perform authentication with the SMTP server.
Email Alert Username	Indicates the username used by the switch to perform authentication with the SMTP server.
Email Alert Password	Indicates the password used by the switch to perform authentication with the SMTP server.

System Utility and Clear Commands

In this section, the commands used to help troubleshoot issues with connectivity and to restore the factory defaults of various configurations are described.

5-75 clear config

This command is used to reset the configuration of the switch back to that included in the factory-defaults configuration file, if that file is present, without the switch being powered off. In the event that the factory-defaults configuration file is not present, then the application of D-LINK OS compile time defaults to the switch occurs instead. When this command is issued, a prompt appears asking for confirmation that the reset should proceed. If the user enters y at the prompt, then the current configuration of the switch will automatically be reset to the default values. Entering y does not, however, reset the switch itself.

clear config

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-76 clear counters

This command is used to clear the statistics for all the ports, for a specified slot/port, or for an interface on a VLAN based on the argument. In the event that a virtual router is specified, then the statistics for the ports included on the virtual router will be cleared. In contrast, if no router is specified, then the information for the default router is then displayed.

clear counters {*slot/port* **| all [vrf** *vrf-name***] | lag [***lag-intf-num***] | nvgre | vlan** *id* | **vxlan}**

Parameters

slot/port	Indicates a slot/port interface.
all	Select to clear all L1/L2 counters on all interfaces including IP counters.
lag	Select to clear LAG interface statistics.
nvgre	Select to clear the NVGRE tunnel counters.
vlan *id*	Indicates a VLAN interface.
vxlan	Select to clear all VXLAN tunnel counters.

Default

The default is None.

Command Mode

Privileged EXEC

5-77 clear ip access-list counters

This command is used to clear the counters of the specified IP ACL and the IP ACL rule.

clear ip access-list counters {*acl-ID* **|** *acl-name* **}**

Parameters

acl-ID 1-199	Indicates the ACL ID to clear counters, range: 1 – 199.
acl-name	Indicates the ACL name to clear counters, up to 31 characters in length.

Default

The default is None.

Command Mode

Global Config

5-78 clear ipv6 access-list counters

This command is used to clear the counters of the specified IP ACL and the IP ACL rule.

clear ipv6 access-list counters *acl-name*

Parameters

acl-name	Indicates the ACL name to clear counters, up to 31 characters.

Default

The default is None.

Command Mode

Privileged EXEC

5-79 clear mac access-list counters

This command is used to clear the counters of the specified MAC ACL and MAC ACL rule.

clear mac access-list counters *acl-name*

Parameters

acl-name	Indicates the ACL name to clear counters, up to 31 characters.

Default

The default is None.

Command Mode

Privileged EXEC

5-80 clear pass

This command is used to reset all the user passwords back to the factory defaults without having to power off the switch. When this command is issued, the user will be prompted to confirm that the password reset should proceed.

clear pass

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-81 clear traplog

This command is used to clear the trap log.

clear traplog

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-82 clear vlan

This command is used to reset the VLAN configuration parameters back to the factory defaults.

clear vlan

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-83 logout

This command is used to close the current telnet connection or to reset the current serial connection.

Note: Please be sure to save any configuration changes before logging out.

logout

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

5-84 ping

This command is used to ascertain whether or not another computer is on the network. The ping yields a synchronous response when it is initiated from the CLI interface.

Note: For related information regarding the ping command for IPv6 hosts, please see “ping ipv6”.

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

Parameters

Through use of the options described below, the user can specify both the number and size of Echo Requests, as well as the interval to wait between Echo Requests.

vrf *vrf-name*	(Optional) Indicates the name of the virtual router within which to initiate the ping. In the event that no virtual router is specified, then the ping will be initiated in the default router instance.
address	Indicates the IPv4 or IPv6 addresses to ping.
count *count*	(Optional) The **count** parameter can be used to specify the number of ping packets (that is, ICMP Echo requests) to send to the destination address that is specified in the ip-address field (range: 1 to 15 requests).
interval	(Optional) The **interval** parameter can be used to specify the time, in seconds, between Echo Requests (range: 1 to 60 seconds).
size *size*	(Optional) The **size** parameter can be used to specify the size, in bytes,

	for the payload of the transmitted Echo Requests (range: 0 to 65507 bytes).
source	The **source** parameter can be used to specify the source IP/IPv6 address or interface to be used when the Echo request packets are sent.
hostname	The *hostname* parameter can be used to resolve the hostname to an IPv4 or IPv6 address. To resolve the hostname to an IPv6 address, the Ipv6 keyword is specified. If no keyword is specified, then the hostname is resolved to an IPv4 address.
ipv6	Using the **ipv6** optional keyword, which can be used before either the *ipv6-address* or *hostname* argument, before the hostname will attempt to resolve the hostname directly to the IPv6 address. The keyword cab also be used to ping a link-local IPv6 address.
interface	The interface keyword can be used to ping a link-local IPv6 address over an interface.
link-local-address	Indicates the link-local IPv6 address that is to be pinged over an interface.
outgoing-interface	(Optional) The outgoing-interface parameter can be used to specify the outgoing interface for a multicast IP/IPv6 ping.

Defaulta

The default is as follows:

- Count: 1
- Interval: 3 seconds
- Size: 0 bytes

Command Mode

- Privileged EXEC
- User EXEC

Example

The following provide examples of the CLI command.

The following are examples of 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
```

The following are examples of 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
```

5-85 quit

This command is used to close the current telnet connection or to reset the current serial connection. The system will ask the user whether or not to save any configuration changes before quitting.

quit

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

5-86 reload

This command is used to reset the switch without having to power it off, where ”reset” means that all the network connections will be terminated and the boot code will be executed. In order to initialize itself, the switch then uses the stored configuration. The user will be prompted to confirm that the requested reset should proceed, and the LEDs on the switch indicate whether or not a reset has been successful.

In the event that ONIE is installed, the os parameter will be added to the reload command. The use of this parameter will enable the user to boot back into ONIE.

reload [configuration [*scriptname***]| os]**

Parameters

configuration	This parameter causes the configuration to be gracefully reloaded. In the event that no configuration file is specified, then the startup-config file will be loaded.
scriptname	Indicates the configuration file to load. The extension must be included in the scriptname.
os	The os reload feature is used to remove the OS and reinstall the new NOS.

Default

The default is None

Command Mode

Privileged EXEC

5-87 copy

The **copy** command is used to upload and download files to and from the switch. Files can be uploaded and downloaded from a server using FTP, TFTP, Xmodem, Ymodem, or Zmodem. Also, it should be noted that a password is required if FTP is used.

copy *source destination*

Replace the *destination* and *source* parameters with the options indicated in “Copy Parameters”. Meanwhile, use one of the following values for the *url* source or destination:

(xmodem | tftp://*ipaddr***|hostname |** *ip6address* **|** *hostname/filepath/filename* **[noval] | sftp | scp://** *username@ipaddr* **|** *ipv6address/filepath/filename* **| ftp://***user@ipaddress* **|** *hostname/filepath/filename***}**

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

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

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

For FTP, TFTP, SFTP and SCP, the *ipaddr/hostname* parameter consists of the host name of the server or the IP address, filepath indicates the path to the file, and *filename* consists of the name of the file that the user wants to upload or download. For SFTP and SCP, the *username* parameter consists of the username used for logging into the remote server via SSH.

Note: *ip6address* also constitutes a valid parameter for the routing of packages that support IPv6.

If the user wishes to copy OpenFlow SSL certificates to the switch using TFTP or XMODEM, then only the following options relevant to the OpenFlow SSL certificates should be used:

copy [<mode/file>] nvram:{openflow-ss1-ca-cert | openflow-ssl-cert | openflow-ssl-priv-key}

Parameters

source	Indicates the originating location of the source.
destination	Indicates the intended location to store

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following provides an example of the downloading and applying of the 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.
```

Copy Parameters

Source	Destination	Description
`nvram:application: sourcefilename`	*url*	Indicates the filename of the 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.
`nvram: core-dump`	tftp://<ipaddress | hostname>/ <filepath>/<filename> | frtp://<user>@<ipaddr | hostname>/<path>/<filename> | scp://<user>@<ipaddr | hostname>/<path>/<filename> | sftp://<user>@<ipaddr | hostname>/<path>/<filename>	Uploads the core dump file included 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 the 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 the 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 for NVRAM to the factory-defaults file.
`url`	nvram:application *destfilename*	Indicates the destination file name for the application file.
`url`	nvram:application *destfilename*	Downloads an application to the system.

Source	Destination	Description
url	nvram:backup-config	Downloads the configuration to the startup configuration.
url	nvram:ca-root *index*	Downloads the CA certificate file to the /mnt/fastpath directory and sends the index number name for 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 sends the index number name for the downloaded file to CA*index*.key.
url	nvram:client-ssl-cent *1-8*	Downloads the client certificate to the /mnt/fastpath directory and sends the index number to name the downloaded file to CA*index*.pem.
url	nvram:fastpath.ctg	Downloads the binary config file to the system.
url	nvram:script *destfflename*	Downloads a configuration script file to the system. During the downloading of the configuration script, the copy command validates the script. In the event of an error, the command lists all the lines at the end of the validation process and prompts the user to confirm before copying the script file.
url	nvram:script *destfflename* noval	When this option is used, the copy command will not validate the downloaded script file. The followins is an example of the CLI command: `(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 of relevance, please see “Secure Shell Commands”.
url	nvram:sshkey-rsa1	Downloads an SSH key file.
url	nvram:sshkey-rsa2	Downloads an SSH key file.
url	nvram:openflow-ss1-ca-cert	Downloads an Openflow CA Certificate.
url	nvram:openflow-ss1-cert	Downloads an Openflow Switch Certificate.
url	nvram:openflow-ss1-priv-key	Downloads an Openflow Private Key.
url	nvram:startup-config	Downloads the startup configuration file to the system.

Source	Destination	Description
url	ias-users	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the IAS user database of the switch is replaced with the users and their attributes included in the downloaded file.
url	nvram:tech-support-cmds	Downloads the file containing the list of commands to be displayed when using the show tech-support command.
url	{active | backup}	Downloads an image from the remote server to either image.

5-88 write memory

This command is used to save any running configuration changes to NVRAM to ensure that the changes will persist across a reboot. The command is effectively the same as the **copy system:running-config nvram:startup-conflg** command. The **confirm** keyword can be used to directly save the configuration to NVRAM without a prompt for a confirmation being presented.

write memory [confirm]

Parameters

confirm	(Optional) Select to directly save the configuration to NVRAM without user prompt confirmation.

Default

The default is None.

Command Mode

Privileged EXEC

IP Address Conflict Commands

These commands are used to troubleshoot IP address conflicts.

5-89 ip address-conflict-detect run

Use this command to run active address conflict detection. Gratuitous ARP packets for IPv4 addresses are sent on the switch.

ip address-conflict-detect run

Parameters

None

Default

The default is None.

Command Mode

- Global Config
- Virtual Router Config

5-90 show ip address-conflict

The command shows the status information for the last detected address conflict.

show ip address-conflict [vrf *vrf-name*]

Parameters

vrf	Display IP address conflict information for a Virtual Router instance.
vrf-name	Displays the VPN routing/forwarding instance name.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show ip address-conflict

Address Conflict Detection Status..... Conflict Detected
Last Conflicting IP Address..... 192.168.0.1
Last Conflicting MAC Address..... 6C:EC:5A:07:E1:06
Time Since Conflict Detected..... 4 days 4 hrs 22 mins 36 secs
```

Display Parameters

Address Conflict Detection Status	Reports any detected address conflict on any IP address.

Last Conflicting IP Address	Display last detected IP Address conflict on any interface.
Last Conflicting MAC Address	Display last detected MAC Address conflict on any interface.
Time Since Conflict Detected	Displays days, hours, minutes and seconds since last detected conflict.

5-91 clear ip address-conflic-detect

Clears detected address conflict status information for a specified virtual router. The command executes on default router if no specified router is given.

clear ip address-conflict-detect [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Enter to clear the detected conflict event for the specified virtual router instance.

Default

The default is None.

Command Mode

Privileged EXEC

Serviceability Packet Tracing Commands

These commands allow network engineers to diagnose D-LINK OS products.

CAUTION: Debug output can be long and may adversely affect system performance.

5-92 capture start

Start allows for manual capturing of 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.

capture start [{all | receive | transmit}]

Parameters

all	Capture all traffic.
receive	Capture only received traffic.
transmit	Capture only transmitted traffic.

Default

The default is None.

Command Mode

Privileged EXEC

5-93 capture stop

Stop allows for manual ending of CPU packet capturing for packet trace.

capture stop

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-94 capture

This command allows for configuration of file capture options (persistent across a reboot cycle.

capture {file | remote | line | USB}

Parameters

file	In capture file mode, packets are saved to a file on NVRAM (maximum file size default: 524288 bytes). File can be transferred to TFTP server via TFTP, SFTP, SCP via CLI, and SNMP. File format: pcap Naming: cpuPktCapture.pcap Use network analyzer tools such as Wireshark® or Ethereal® to review

	file. The file capturing function terminates any remote capture sessions and line capturing. Once activated, file capturing does not stop until the process reaches maximum file size or until function is manually stopped using the command capture stop.
remote	In remote capture mode, captured packets are diverted in real time to an external PC running Wireshark tool (Microsoft® Windows®). Captured packets are sent to the Wireshark tool via a TCP connection. Remote capture is enabled or disabled using the CLI. Configure the IP port number (default: 2002) to connect to the Wireshark switch. Configure the firewall if installed to allow for traffic between the Wireshark PC and the switch. The firewall must be configured to allow the Wireshark PC to initiate TCP connections to the switch. A successful client connection to the switch allows CPU packets to be sent to the client PC, Wireshark then receives the packets and displays them. The session continues until terminated by either end. Starting a remote capture session automatically terminates the file capture and line capturing.
line	In capture line mode, captured packets are saved in RAM and can be displayed on the CLI. Starting a line capture automatically terminates the following: remote capture session and capturing into a file. The maximum allowed packets for capturing: 128 packets, maximum 128 bytes each.
USB	ln capture file mode, packets are saved to a USB destination. The valid name length is 1 to 64 characters. The file extension is added automatically.

Default

The default is None.

Command Mode

Global Config

5-95 capture remote port

Remote Port configures file capture options. The command is persistent across a reboot cycle. The parameter is a TCP port number: 1024-49151.

capture remote port *1024-49151*

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-96 capture file size

File size is used to configure file capture options. The command is persistent across a reboot cycle. The *max-file-size* parameter: maximum pcap file size range is 2 to 512 kB.

capture file size *max-file-size*

Parameters

max-file-size	Indicates the file size in KB, range: 2 – 512 kilobytes.

Default

The default is None.

Command Mode

Global Config

5-97 capture line wrap

Line wrap enables wrapping of captured packets in line mode when packet size reaches full capacity.

No command disables wrapping of captured packets stops function when the captured packet capacity is full.

capture line wrap

no capture line wrap

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-98 show capture packets

Capture packets displays packets captured and saved to RAM. Captured packets received or transmitted through the CPU are saved to RAM. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. Only the first 128 bytes are saved; data exceeding 128 bytes is not in the CLI.

The capture function stops automatically when the 128 bytes limit is reached. Captured packets are not retained after a reload cycle.

show capture packets

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-99 cpu-traffic direction

CPU-traffic direction interface associates CPU filters to an interface or list of interfaces (physical or logical LAG). The statistics counters are updated only for the configured interfaces. Traces are available for the configured interfaces.

Note: VLAN tag headers as the packet to the CPU should be considered as a tagged packet.

No command removes all interfaces from the CPU filters.

cpu-traffic direction {tx | rx | both} interface *interface-range*

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

Parameters

both	Select to match ingress and egress packets.
rx	Select to match egress packets.
tx	Select to match ingress packets.

Default

The default is None.

Command Mode

Global Config

5-100 cpu-traffic direction match cust-filter

CPU-traffic direction match allows custom filter configuration. The statistics and/or traces for the configured filters are obtainable at the specific offset for the packet matching configured data. The default mask is 0xFF. Three different offsets can be specified as the match conditions. The latest custom filter overrides the previous configuration.

Note: VLAN tag headers as the packet to the CPU should be considered as a tagged packet.

No command removes the configured custom filter.

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

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

Parameters

both	Select to match both ingress and egress packets.
rx	Indicates the egress packet.
tx	Indicates the ingress packet.
offset1	Select to configure the offset for custom filter. A hex value strings is required.
data1	Select to configure the matching custom filter. A hex value strings is required.
mask# *mask#*	(Optional) Select to configure the matching conditions.

Default

The default is None.

Command Mode

Global Config

5-101 cpu-traffic direction match srcip

CPU-traffic direction match configures the source IP address-specific filter. Use the command to obtain the statistics and/or the traces for configured filters matching configured source IP/Mask.

No command disables the configured source IP address filter.

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

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

Parameters

both	Select to match both ingress and egress packets.
rx	Indicates the egress packet.
tx	Indicates the ingress packet.
ipaddress	Indicates the IP address for the srcip filter.
mask *mask*	(Optional) Select the IP address for the subnet mask. Default: 255.255.255.255.

Default

The default is None.

Command Mode

Global Config

5-102 cpu-traffic direction match dstip

Configure the destination IP address-specific filter. The statistics and/or the traces of the configured filters are used for the matching IP/Mask packet.

No command disables the configured destination IP address filter.

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

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

Parameters

both	Select to match both ingress and egress packets.
rx	Indicates the egress packet.
tx	Indicates the ingress packet.
ipaddress	Indicates the IP address for the dstip filter.
mask *mask*	(Optional) Select the IP address for the subnet mask. Default: 255.255.255.255.

Default

The default is None.

Command Mode

Global Config

5-103 cpu-traffic direction match dstmac

Configure the destination IP address-specific filter. The statistics and/or the traces of the configured filters are used for the matching IP/Mask packet.

No command disables the configured destination IP address filter.

cpu-traffic direction {tx | rx | both} match dstmac *macaddress* **[mask** *mask***]**

no cpu-traffic direction {tx | rx | both} match dstmac *macddress* **[mask** *mask***]**

Parameters

both	Select to match both ingress and egress packets.
rx	Indicates the egress packet.
tx	Indicates the ingress packet.
macaddress	Indicates the MAC address for the dstmac filter.
mask *mask*	(Optional) Select the IP address for the subnet mask. Default: 255.255.255.255.

Default

The default is None.

Command Mode

Global Config

5-104 cpu-traffic direction match dsttcp

Cnfigure the source or destination TCP port-specific filter. The statistics and/or the traces of the configured filters are used for the matching TCP port packet.

No command removes the configured source/destination TCP port filter.

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

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

Parameters

both	Select to match both ingress and egress packets.
rx	Indicates the egress packet.
tx	Indicates the ingress packet.
srctcp	Select to configure SRCTCP filter options.
dsttcp	Select to configure DSTTCP filter options.
port	Indicates the port value (0 – 65535).
mask *mask*	(Optional) Select the IP address for the subnet mask.

	Default: 255.255.255.255.

Default

The default is None.

Command Mode

Global Config

5-105 cpu-traffic direction match dstudp

Configure the destination IP address-specific filter. The statistics and/or the traces of the configured filters are used for the matching IP/Mask packet.

No command disables the configured destination IP address filter.

cpu-traffic direction {tx | rx | both} match dstudp *ipaddress* **[mask** *mask***]**

no cpu-traffic direction {tx | rx | both} match dstudp *ipaddress* **[mask** *mask***]**

Parameters

both	Select to match both ingress and egress packets.
rx	Indicates the egress packet.
tx	Indicates the ingress packet.
port	Indicates the port value value (0 – 65535).
mask *mask*	(Optional) Indicates the IP address for the subnet mask. Default: 255.255.255.255.

Default

The default is None.

Command Mode

Global Config

5-106 cpu-traffic direction match filter

The command is used to configure the filter type.

No command disables the configured filter.

cpu-traffic direction match {tx | rx | both} match dstudp filter

Parameters

both	Select to match both ingress and egress packets.

rx	Indicates the egress packet.
tx	Indicates the ingresspacket.
port	Indicates the port value value (0 – 65535).
mask *mask*	(Optional) Indicates the designated subnet mask address. Default: 255.255.255.255.

Default

The default is None.

Command Mode

Global Config

Example

The following shows an example of the command.

```
(Routing)(Config)#cpu-traffic direction both match filter ?

all    Configure all filters as matching condition.
arp    Select ARP protocol as matching condition.
bcast  Select BCAST option to match broadcast packets.
bgp    Select BGP protocol as matching condition.
custom Select custom option to match all packets that match custom values.
dhcp   Select DHCP protocol as matching condition.
dstip  Select DSTIP option to match all packets with specified destination IP.
dstmac Select DSTMAC option to match all packets with specified destination MAC.
dsttcp Select DSTTCP option to match all packets with specified TCP destination port.
dstudp Select DSTUDP option to match all packets with specified UDP destination port.
ip     Select IP protocol as matching condition.
lacpdu Select LACP protocol as matching condition.
lldp   Select LLDP protocol as matching condition.
mcast  Select MCAST option to match multicast packets.
ospf   Select OSPF protocol as matching condition.
srcip  Select SRCIP option to match all packets with specified source IP.
srcmac Select SRCMAC option to match all packets with specified source MAC.
srctcp Select SRCTCP option to match all packets with specified TCP source port.
srcudp Select SRCUDP option to match all packets with specified UDP source port.
stp    Select STP protocol as matching condition.
ucast  Select UCAST option to match unicast packets.
udld   Select UDLD protocol as matching condition.
```

5-107 cpu-traffic direction match srcudp

Configure the source or destination UDP port-specific filter. The statistics and/or the traces of the configured filters are used for the matching source/destination UDP port.

No command removes the configured source/destination UDP port filter.

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

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

Parameters

both	Select to match both ingress and egress packets.
rx	Indicates the egress packet.
tx	Indicates the ingress packet.
srctcp	Select to configure SRCTCP filter options.
dsttcp	Select to configure DSTTCP filter options.
port	Indicates the port value (0 – 65535).
mask *mask*	(Optional) Indicates the designated subnet mask address. Default: 255.255.255.255.

Default

The default is None.

Command Mode

Global Config

5-108 cpu-traffic mode

Configure CPU-traffic mode. RX/TX direction packets are matched when the mode is enabled.

No command disables CPU-traffic mode.

cpu-traffic mode

no cpu-traffic mode

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-109 cpu-traffic trace

Configure CPU packet tracing. Packet is received through multiple components. When enabled and tracing is configured, the packets are traced as defined by filter. Enable dump-pkt to display the first 64 bytes of the packet and trace statistics.

No command disables CPU packet tracing and dump-pkt (if configured).

cpu-traffic trace {dump-pkt}

no cpu-traffic trace {dump-pkt}

Parameters

dump-pkt	Select to enable packet dump option.

Default

The default is Disabled.

Command Mode

Global Config

5-110 show cpu-traffic

Use this command to display the current configuration parameters.

show cpu-traffic

Parameters

None

Default

The default is None.

Command 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
```

5-111 show cpu-traffic interface

Displays interface statistics for configured filters. Filter specific statistics (e.g., stp, udld, arp etc) can be displayed. Do not specify a filter to display all configured filters. Additionally, the source/destination (IP, TCP, UDP or MAC) with filters can be used as command option to obtain statistics.

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

Parameters

Intf-range *slot/port*	Indicates the slot/port interface.
all	Select to display the statistics for all interfaces.
cpu	Indicates the CPU port packets.

Default

The default is None.

Command Mode

Privileged EXEC

5-112 show cpu-traffic summary

Display summary statistics for configured filters on all interfaces.

show cpu-traffic summary

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

```
(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
```

5-113 show cpu-traffic trace

Displays traced information (all available packets or specific filter [e.g., stp, udld, arp etc]). Additionally, the source/destination (IP, TCP, UDP or MAC) with filters can be used as command option to obtain statisticsfrom history. Enable to display packet dump (buffer size: first 64 bytes) information and packet trace statistics.

show cpu-traffic trace *filter*

Parameters

filter	Indicates the following filters: STP, LACPDU, ARP, UDLD, LLDP, IP, OSPF, BGP, DHCP, BCAST, MCAST, UCAST, SRCIP, DSTIP, SRCMAC, DSTMAC, CUSTOM, SRCTCP, DSTTCP, SRCUDP, DSTUDP.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

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

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()
<00:06:10> Freed
0000 00 10 18 82 18 b3 00 10 10 10 10 10 81 00 00 01        ................
0010 00 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...........
```

5-114 clear cpu-traffic

Clears cpu-traffic statistics or trace information on all interfaces.

clear cpu-traffic {counters | traces}

Parameters

counters	Select to clear CPU traffic counters on all interfaces.
traces	Select to clear CPU traffic tracess on all interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

5-115 debug aaa accounting

In User Manager, debug accounting configuration and functionality.

No command turns off debugging of User Manager accounting functionality.

debug aaa accounting

no debug aaa accounting

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-116 debug aaa authorization commands

In User Manager, enable tracing for AAA. The command is used to debug authorization configuration and functionality.

No command turns off debugging of User Manager authorization.

debug aaa authorization commands

no debug aaa authorization commands

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

```
(Routing)#debug aaa authorization commands

User Mgr authorization debug is enabled.

(Routing)#no debug aaa authorization commands

User Mgr authorization debug is Disabled.
```

5-117 debug arp

Enables ARP debug protocol messaging. Optionally, command execution can be performed through a specified virtual router.

No command disables ARP debug protocol messaging.

debug arp [vrf *vrf-name***]**

no debug arp

Parameters

vrf *vrf-name*	(Optional) Select to configure ARP Debug flag of a virtual router.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-118 debug auto-voip

Enables Auto VOIP debug messaging. Optional parameters trace H323, SCCP, or SIP packets.

No command disables Auto VOIP debug messaging.

debug auto-voip [H323 | SCCP | SIP]

no debug auto-voip

Parameters

H323	Select to trace H323 packets.

SCCP	Select to trace SCCP packets.
SIP	Select to trace SIP packets.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-119 debug clear

Disable all previously enabled debug traces.

debug clear

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-120 debug console

Enable the display of debug trace output on the respective login session. To view trace output, the debug console display must be enabled. Once enabled, the debug trace output is available for display on the respective debug console; the function remains in effect for the life of the login session. This command is not persistent across resets.

Note: The debug console command directs debug data to a login session. The filter, specified by the console logging command, determines message severity level.

No command disables the debug trace output display on the respective login session.

debug console

no debug console

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-121 debug crashlog

View information contained in the crash log file. The crash log file includes the following:

- 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)

debug crashlog {[kernel] *crashlog-number* **[upload** *url***] | proc | verbose | deleteall | data** ***crashdump-number*****}**

Parameters

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.
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	Indicates the ID of the component listed as crash fault.
item-number	Indicates the item number.
additional-parameter	Additional parameters to include.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-122 debug crashlog kernel

Display the dmesg log from the specified kdump slot.

debug crashlog kernel *crashlog-number*

Parameters

crashlog-number	Indicates the crashlog number.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-123 debug crashlog kernel upload

Upload the specified kernel dump to a designated TFTP server.

debug crashlog kernel *crashlog-number* **upload** *tftpaddress*

Parameters

crashlog-number	Indicates the crashlog number.
tftpaddress	Indicates the TFTP URL to upload the crashlog in the following format: tftp://<ipaddress>/<filepath>/<filename>.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-124 debug dcbx packet

Enable debug tracing for Tx/Rx DCBX packets.

debug dcbx packet: {receive | transmit}

Parameters

receive	Select to turn on DCBX receive packet debug trace.
transmit	Select to turn on DCBX transmit packet debug trace.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-125 debug debug-config

Download or upload the debug-config.ini file. The file executes CLI commands (including devshell and drivshell commands) for specific predefined events.

Manually create a debug config file to download to the switch.

debug debug-config {download <*url*> | upload <*url*>}

Parameters

download <*url*>	Select to enter the URL to download the debug-config file. Format: tftp://<ipaddress>/<filepath>/<filename>.
upload <*url*>	Select to enter the URL to upload the debug-config file. Format: tftp://<ipaddress>/<filepath>/<filename>.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-126 debug dhcp packet

Displays debug information related to DHCPv4 client activities and traced DHCPV4 packets to and from the local DHCPv4 client.

No command disables debug trace output display for DHCPV4 client activity.

debug dhcp packet [transmit | receive]

no debug dhcp packet [transmit | receive]

Parameters

transmit	(Optional) Select to turn on DHCPv4 client transmit packet debug trace.
receive	(Optional) Select to turn on DHCPv4 client receive packet debug trace.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-127 debug dot1x packet

Enable dot1x packet debug tracing.

No command disables dot1x packet debug tracing.

debug dot1x packet [transmit | receive]

no debug dot1x packet [transmit | receive]

Parameters

transmit	(Optional) Select to turn on dot1x client transmit packet debug trace.
receive	(Optional) Select to turn on dot1x client receive packet debug trace.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-128 debug dynamic port

The command enables dynamic port debugging.

No command disables the debugging function.

debug dynamic ports

no debug dynamic ports

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-129 debug exception

Display core dump features support.

No command disables the debug exception.

debug exception

no debug exception

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-130 debug fip-snooping

Use the command to debug the Fibre Channel over Ethernet Initialization Protocol (FIP) snooping on the device.

No command disables the fip-snooping.

debug fip-snooping packet {filter [dst-mac | fip-proto-code | src-intf | src-mac | vlan] | receive | transmit}

no debug fip-snooping packet {filter [dst-mac | fip-proto-code | src-intf | src-mac | vlan] | receive | transmit}

Parameters

packet	Turns on the fip-snooping packet debug trace.
dst-mac	Filter trace output on match condition based on a Destination MAC Address.
fip-proto-code	Filter based on FIP protocol codes. Use bitmap of supported types to match on multiple types.
src-intf	Filter trace output on match condition based source interface.
src-mac	Filter trace output on match condition based on a Source MAC Address.
vlan	Filter trace output on match condition based VLAN.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-131 debug igmpsnooping packet

Enable tracing of switch Tx/Rx IGMP Snooping packets .

No command disables tracing of IGMP Snooping packets.

debug igmpsnooping packet [transmit | receive]

no debug igmpsnooping packet [transmit | receive]

Parameters

transmit	(Optional) Select to turn on IGMP snooping transmit packet debug trace.
receive	(Optional) Select to turn on IGMP snooping receive packet debug trace.

Default

The default is Dissabled.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

```
(Routing)#debug igmpsnooping packet transmit


<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185420002]: igmp_snooping_debug.c(116)
908 % Pkt TX - Intf: 0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac:
```

```
01:00:5e:00:00:01 Src_IP:9.1.1.1 Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group:
225.0.0.1
```

Display Parameters

TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is slot/port (internal interface number). Unit is always shown as 1 for interface on a non-stacking device.
Src_Mac	Source MAC address of the packet
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.
Dest_IP	The destination multicast IP address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • Membership Query – IGMP Membership Query • V1_Membership_Report – IGMP Version 1 Membership Report • V2_Membership_Report – IGMP Version 2 Membership Report • V3_Membership_Report – IGMP Version 3 Membership Report • V2_Leave_Group – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

Example

The following is an example of the command.

```
(Routing)#debug igmpsnooping packet receive


<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116)
908 % Pkt RX - Intf: 0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac:
01:00:5e:00:00:05 Src_IP: 11.1.1.1 Dest_IP: 225.0.0.5 Type: Membership_Query Group:
225.0.0.5
```

Display Parameters

RX	A packet received by the device.
Intf	The interface that the packet 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_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the ip header in the packet.
Dest_IP	The destination multicast ip address in the packet.

Type	The type of IGMP packet. Type can be one of the following: • Membership_Query – IGMP Membership Query • V1_Membership_Report – IGMP Version 1 Membership Report • V2_Membership_Report – IGMP Version 2 Membership Report • V3_Membership_Report – IGMP Version 3 Membership Report • V2_Leave_Group – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

5-132 debug ip acl

Enable debug of IP Protocol packets based on corresponding ACL criteria.

No command disables IP Protocol packets debug.

debug ip acl acl *Number*

no debug ip acl acl *Number*

Parameters

acl *Number*	Indicates a valid ACL Number.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-133 debug ip bgp

The debug ip bgp command (privileged EXEC mode) enables BGP event debug tracing. The system logs Debug messages according to severity level. To print logs on the console, enable console logging at the DEBUG level (logging console debug command). See “logging console”.

Debug options for a specific peer are defined by combining peer specific and global options.

Enabling one packet type option enables packet tracing in both the inbound and outbound.

No command disables debug tracing of BGP events.

debug ip bgp [vrf *vrf-name***] {***ipv4-address* **|** *ipv6-address***} [events | in | keepalives | notification | open | out | refresh | updates]**

no depub ip bgp [events | keepalives | notification | open | refresh | updates]

Parameters

vrf *vrf-name*	Indicates the BGP information of a virtual router.
ipv4-address	Indicates the IPv4 address of the peer.
ipv6-address	Indicates the IPv6 address of the peer.
events	(Optional) Trace adjacency state events.
in	Indicates the Debug BGP received packets.
keepalives	(Optional) Trace transmit and receive of KEEPALIVE packets.
notification	(Optional) Trace transmit and receive of NOTIFICATION packets.
open	(Optional) Trace transmit and receive of OPEN packets.
out	Indicates the Debug BGP sent packets.
refresh	(Optional) Traces transmit and receive of ROUTE REFRESH packets.
updates	(Optional) Traces transmit and receive of UPDATE packets.

Default

The default is Default.

Command Mode

Privileged EXEC

5-134 debug ip vrrp

Enable VRRP debug protocol messaging.

No command disables VRRP debug protocol messaging.

debug ip vrrp

no debug ip vrrp

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-135 debug ipv6 dhcp

Displays debug information about DHCPv6 client activities, additionally the command traces DHCPv6 packets to and from the local DHCPv6 client.

No command disables the display for the debug trace output (DHCPv6 client activity) function.

debug ipv6 dhcp

no debug ipv6 dhcp

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-136 debug ipv6 ospfv3 packet

Enable IPv6 OSPFv3 packet debug tracing.

No command disables IPv6 OSPFv3 packet tracing.

debug ipv6 ospfv3 packet

no debug ipv6 ospfv3 packet

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-137 debug isdp packet

Enable tracing of transmitted and received ISDP packets from the switch.

No command disables tracing of received/transmitted ISDP packets.

debug isdp packet [receive | transmit]

no debug isdp packet [receive | transmit]

Parameters

transmit	(Optional) Select to turn on ISDP transmit packet debug trace.
receive	(Optional) Select to turn on ISDP receive packet debug trace.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-138 debug lacp packet

Enable tracing of received and transmitted LACP packets from the switch.

No command disables received/transmitted LACP packet tracing.

debug lacp packet

no debug lacp packet

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

Example

A sample output of the trace message is shown below.

```
(Routing)#debug lacp packet


<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
```

5-139 debug mldsnooping packet

Trace received and transmitted MLD snooping packets. The following information: source address, destination address, control packet type, packet length, and the specific type of interface (received or transmitted) in which it was received.

No command disables received/transmitted MLD snooping packet debug tracing.

debug mldsnooping packet [receive | transmit]

no debug mldsnooping packet [receive | transmit]

Parameters

transmit	(Optional) Select to turn on MLD snooping transmit packet debug trace.
receive	(Optional) Select to turn on MLD snooping receive packet debug trace.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-140 debug ospf packet

Enable tracing of received and transmitted OSPF packets from the switch or a specified virtual router.

No command disables OSPF packet tracing.

debug ospf packet [vrf *vrf-name***]**

no debug ospf packet

Parameters

vrf *vrf-name*	(Optional) Select to configure OSPF packet Debug flags of a virtual router.

Default

The default is Disabled.

Command Mode

Privileged EXEC

Example

Sample outputs of the trace messages are shown below.

```
(Routing)#debug ospf packet
```

```
<15> JAN 02 11:03:31 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25430 % Pkt RX -
Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:224.0.0.5 AreaId:0.0.0.0 Type:HELLO NetMask:255.255.255.0 D
esigRouter:0.0.0.0 Backup:0.0.0.0

<15> JAN 02 11:03:35 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25431 % Pkt TX -
Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:DB_DSCR Mtu:1500 Options:E
Flags: I/M/MS Seq:126166

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25434 % Pkt RX -
Intf:2/0/48 Src
IP:192.168.50.2 DestIp:192.168.50.1 AreaId:0.0.0.0 Type:LS_REQ Length: 1500

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25435 % Pkt TX -
Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:LS_UPD Length: 1500

<15> JAN 02 11:03:37 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25441 % Pkt TX -
Intf:2/0/48 Src
Ip:10.50.50.1 DetIp:224.0.0.6 AreaId:0.0.0.0 Type:LS_ACK Length: 1500
```

Display Parameters

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).
SrcIp	The source IP address in the IP header of the packet.
DestIp	The destination IP address in the IP header of the packet.
AreaId	The area ID in the OSPF header of the packet.
Type	Could be one of the following: • HELLO – Hello packet • DB_DSCR – Database descriptor • LS_REQ – LS Request • LS_UPD – LS Update • LS_ACK – LS Acknowledge

The following are OSPF packet fields resulting from a trace.

HELLO packet field definitions:

Netmask	The netmask in the hello packet.
DesignRouter	Designated Router IP address.
Backup	Backup router IP address.

DB_DSCR packet field definitions:

MTU	MTU.
Options	Options in the OSPF packet.
Flags	Could be one or more of the following: • I – Init • M – More • MS – Master/Slave
Seq	Sequence Number of the DD packet.

LS_REQ packet field definitions:

Length	Length of packet.

LS_UPD packet field definitions:

Length	Length of packet.

LS_ACK packet field definitions:

Length	Length of packet.

5-141 debug ping packet

Enable ICMP echo request and response tracing. Ping tracing of network/service port for switching packages can be traced with this command. Pings can also be traced on specified virtual router.

No command disables ICMP echo request and response tracing.

debug ping packet [vrf *vrf-name***]**

no debug ping packet

Parameters

vrf *vrf-name*	(Optional) Configure Ping Packet Debug flags of a virtual router.

Default

The default is Disabled.

Command Mode

Privileged EXEC

Example

A sample output of the trace message is shown below.

```
(Routing)# debug ping packet

<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), SRC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

Display Parameters

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.
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.

5-142 debug sflow packet

Enable sFlow debug packet tracing.

No command disables sFlow debug packet tracing.

debug sflow packet

no debug sflow packet

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-143 debug spanning-tree bpdu

Enable spanning tree received and transmitted BPDU tracing.

No command disables spanning tree BPDU tracing.

debug spanning-tree bpdu

no debug spanning-tree bpdu

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-144 debug spanning-tree bpdu receive

Enable received spanning tree BPDU tracing. Enable spanning tree on the device and interface to allow for monitoring of packets for a specified interface.

No command disables tracing of received spanning tree BPDUs.

debug spanning-tree bpdu receive

no debug spanning-tree bpdu receive

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

Example

A sample output of the trace message is shown below.

```
(Routing)#debug spanning-tree bpdu receive


<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
```

Display Parameters

RX	A packet received by the device.
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 from 0 to 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

5-145 debug spanning-tree bpdu transmit

Enable transmitted spanning tree BPDU tracing. Enable spanning tree on the device and interface to allow for monitoring of packets for a specified interface.

No command disables tracing of transmitted spanning tree BPDUs.

debug spanning-tree bpdu transmit

no debug spanning-tree bpdu transmit

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Routing)#debug spanning-tree bpdu transmit


<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
```

Display Parameters

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 aslways 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 from 0 to 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

5-146 debug tacacs

Enable TACACS+ debugging.

debug tacacs {packet | accounting | authentication | authoriation}

Parameters

accounting	Displays information about accountable events as they occur.
authentication	Displays information about AAA/TACACS+ authentication.
authorization	Displays information about AAA/TACACS+ authorization.
packet	Displays information about TACACS+ packets.

Default

The default is None.

Command Mode

Global Config

5-147 debug transfer

Enable file transfers debugging.

No command disables file transfer debugging.

debug transfer

no debug transfer

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-148 debug udld events

Enable UDLD event debugging.

No command disables the debugging of UDLD process events or packet events.

debug udld events

no debug udld {events | packets}

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-149 debug udld packet receive

Enable received UDLD packet debugging.

No command disables the debugging of UDLD packet receipts.

debug udld packet receive

no debug udld packet receive

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-150 debug udld packet transmit

Enable transmitted UDLD PDU debugging. Use the no form of this command to disable UDLD debugging.

debug udld packet transmit

No debug udld packet

Parameters

events	Turn on UDLD events debug trace.
packet	Turn on UDLD packet debug trace.

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-151 show debugging

Display the packet tracing configuration.

show debugging

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show debugging

Console display of debug output is enabled.
```

5-152 exception core-file

Configure a prefix for a core-file name. The following are examples of a generated core file name with the prefix:

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 a **hostname** is configured, the core file name takes on the defined hostname. Otherwise the MAC address is used as the core name (prefix length: 15 characters) when generating a core dump file.

No command resets to factory default the exception core file prefix configuration. The hostname and time-stamp are disabled.

exception core-file {*file-name-prefix* **| [hostname] | [time-stamp]}**

no exception core-file

Parameters

file-name-prefix	Enter the coredump file name up to 15 characters. File name can consist of -, _, alphanumerics.
hostname	(Optional) Select to append hostname to coredump file name.
time-stamp	(Optional) Select to append time-stamp to coredump file name.

Default

The default is Core.

Command Mode

Global Config

5-153 exception dump filepath

Configure a TFTP/FTP server file-path (NFS mounted or USB device subdirectory) for dumping core files.

No command resets to factory default the exception dump filepath configuration.

exception dump filepath *dir*

no exception dump filepath

Parameters

dir	Enter the path to store the coredump.

Default

The default is None.

Command Mode

Global Config

5-154 exception dump ftp-server

Configure remote FTP server (address) for core file dumping. Anonymous FTP is the default for the username and password; anonymous FTP must first be enabled on the FTP server.

No command resets the exception dump remote FTP server configuration to the factory default, includes FTP username and password.

exception dump ftp-server *ip-address* **[{username** *user-name* **password** *password***}]**

no exception dump ftp-server

Parameters

ip-address	Enter the IP address of the FTP server.
username *user-name*	(Optional) Enter FTP user name.
password *password*	(Optional) Enter FTP password associated with the listed user name.

Default

The default is None.

Command Mode

Global Config

5-155 exception dump nfs

Configure NFS mount point to NFS file system for core file dumping.

No command resets to factory defaults the exception dump NFS mount point configuration.

exception dump nfs *ip-address/dir*

no exception dump nfs

Parameters

ip-address/dir	Enter the IP address and path to the NFS mount point.

Default

The default is None.

Command Mode

Global Config

5-156 exception dump stack-ip-address

Configure a remote server for the purpose of dumping the core file in the event of a device crash.

No command resets to factory defaults the exception dump remote server configuration.

exception dump stack-ip-address {[add] [remove} *ip-address***} {[protocol]** *dhcp/ static***}**

no enable exception dump stack-ip-address

Parameters

ip-address	Enter the IP address of the server.
add	Enter the IP address for the alternative IP pool to be assigned to the device's service port in the stack.
protocol	Enter the type of protocol definition for the service port for a crash event.
remove	Enter the IP address to remove from the alternative IP pool.

Default

The default is None.

Command Mode

Global Config

5-157 exception dump tftp-server

Configure a remote TFTP server for core file dumping.

No command resets to factory defaults the exception dump remote server configuration.

Note: Available only on selected Linux-based platforms.

exception dump tftp-server {*ip-address***}**

no enable exception dump tftp-server

Parameters

ip-address	Enter the IP address of the TFTP server.

Default

The default is None.

Command Mode

Global Config

5-158 exception kernel-dump

Enable kernel crash core dumping (kdump). The system requires a reboot if the function is enabled.

No command disables kernel crash core dumping (kdump). The specified crash log number is deleted.

exception kernel-dump

no exception kernel-dump *crashlog-number*

Parameters

crashlog-number	Indicates the number identifying the crashlog.

Default

The default is None.

Command Mode

Global Config

5-159 exception kernel-dump path

Set the kernel crash core dump (kdump) entry path.

No command sets to default the kernel crash core dump (kdump) entry path.

exception kernel-dump path *path*

no exception kernel-dump path

Parameters

path	Set path to save kernel dump log files to.

Default

The default is None.

Command Mode

Global Config

5-160 exception protocol

Specify the protocol to store the core dump file.

No command resets the exception protocol configuration to factory default.

exception protocol {nfs | tftp | ftp | local | none}

no exception protocol

Parameters

nfs	Configure protocol to upload coredump to the NFS share.
tftp	Configure protocol to upload coredump to the TFTP server.
ftp	Configure protocol to upload coredump to the FTP server.
local	Configure protocol to generate coredump on Switch local file system.
none	Disable coredump.

Default

The default is None.

Command Mode

Global Config

5-161 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.

exception switch-chip-register {enable | disable}

Parameters

enable	Enable switch-chip-register dump in case of an exception.
disable	Disable switch-chip-register dump in case of an exception.

Default

The default is Disabled.

Command Mode

5-162 Global Configshow exception kernel-dump

Display the viewable kernel dump and available slot settings.

show exception kernel-dump

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show exception kernel-dump

Admin Mode..................................... False
Maximum Records................................ 3
Available Records.............................. 0
Kernel Dump Storage Path....................... /mnt/fastpath/crashlogs/kdump
```

5-163 show exception kernel-dump list

Display captured dumps.

show exception kernel-dump list

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-164 show exception kernel-dump log

Display specified kdump slot dmesg log.

show exception kernel-dump log *crashlog-number*

Parameters

crashlog-number	Select the record number to view.

Default

The default is None.

Command Mode

Privileged EXEC

5-165 mbuf

Configure memory buffer (MBUF) threshold limits and generate MBUF limit alerts.

mbuf {falling-threshold | rising threshold | severity}

Parameters

falling-threshold	Set memory buffer minimum (%), usage below minimum triggers an alert; range: 1 to 100 (default: 0, disabled).
rising threshold	Set memory buffer maximum (5), exceeding usage triggers an alert; range: 1 to 100 (default: 0, disabled).
severity	Defines severity level of Mbuf logs; range: 1 to 7 (default: 5).

Default

The default is None.

Command Mode

Global Config

5-166 write core

Generate an on-demand core dump file; suggested method to test core dump setup.

Example:

For a configured TFTP protocol, the **write core test** command is used to test connectivity with a TFTP server.

Similarly, by configuring the protocol to **nfs**, it can be used to mount and unmount the file system, providing a status result.

Note: write core reloads the non-malfunctioning switch if it hasn't crashed.

For **write core** test commands, the destination file name is used for the TFTP test. Specifying the destination file name can be set when the protocol is configured as TFTP.

write core [test [dest_file_name]]

Parameters

test	(Optional) Select to tests the core dump setup.
dest_file_name	(Optional) Indicates the test file name to be uploaded.

Default

The default is None.

Command Mode

Privileged EXEC

5-167 show exception

Display the configuration parameters to generate a core dump file.

show exception

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

```
(Routing)#show exception

Coredump file name                      core
Coredump filename uses hostname         False
Coredump filename uses time-stamp       TRUE
NFS Mount point                         NFS mount point configuration
TFTP Server Address                     TFTP server configuration
```

```
FTP Server IP                          FTP server configuration
FTP user name                          FTP user name
FTP password                           FTP password
File path                              Remote file path
Protocol                               none
Switch Chip Register Dump              Switch chip register dump configuration
Stack IP Address Protocol              dhcp
Stack IP Address
```

5-168 show exception core-dump-file

Display current local file system, core dump files.

show exception core-dump-file

Parameters

None

Default

The default is None.

Command Mode

- Config Mode
- Privileged EXEC

5-169 show exception log

Display current local file system, core dump traces.

show exception log [previous]

Parameters

previous	(Optional) Display coredump log file from the previous coredump run.

Default

The default is None.

Command Mode

- Config Mode
- Privileged EXEC

5-170 show mbuf total

Display the memory buffer (MBUF) Utilization Monitoring parameters.

show mbuf total

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show mbuf total

Mbufs Total..................................... 246
Mbufs Free...................................... 246
Mbufs Rx Used................................... 0
Mbufs Rx Norm Used.............................. 0
Mbufs Rx Mid2 Used.............................. 0
Mbufs Rx Mid1 Used.............................. 0
Mbufs Rx Mid0 Used.............................. 0
Mbufs Rx High Used.............................. 0
Mbufs Tx Used................................... 0
Total Rx Norm Alloc Attempts.................... 0
Total Rx Mid2 Alloc Attempts.................... 37989
Total Rx Mid1 Alloc Attempts.................... 13044
Total Rx Mid0 Alloc Attempts.................... 0
Total Rx High Alloc Attempts.................... 0
Total Tx Alloc Attempts......................... 16480
Total Rx Norm Alloc Failures.................... 0
Total Rx Mid2 Alloc Failures.................... 0
Total Rx Mid1 Alloc Failures.................... 0
Total Rx Mid0 Alloc Failures.................... 0
Total Rx High Alloc Failures.................... 0
Total Tx Alloc Failures......................... 0
```

5-171 show msg-queue

Display message queues.

show msg-queue

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show msg-queue

Queue     Queue    Messages        Threads waiting   Messages       Send    Recv
ID        Name     in Queue        to Send           Receive High   Wait    Wait
--------  -------  --------------- ---------------   ------------   ------ -----
e6fc063c  BGP      Receive_q0      0                 0              0       0       $00000000$
          ?????    $08f0259a$ DebugQueues + 0x3ba
0ee64274 NIM EVENT RESPO       0          0          0        1     $00000000$ ????? $082a245d$
nimDoNotify + 0x41d
0ee370ec nimRifHpcMsgRsp       0          0          0        0     $00000000$ ?????
$00000000$ ?????
e6fa0e8c errDisableQueue       0          0          1        1     $00000000$ ?????
$00000000$ ?????
e6f9e804 das_Mgmt_Queue        0          0          0        1     $00000000$ ?????
$00000000$ ?????
e6f9e174 bfdEventMsgQ          0          0          1        0     $00000000$ ?????
$00000000$ ?????
f3457f14 mlag_bulk_ctrl_       0          0          1        1     $00000000$ ?????
$00000000$ ?????
f533cd64 mlag_ckpt_queue       0          0          1        0     $00000000$ ?????
$00000000$ ?????
dbd63634 mlag_ctrl_msg_q       0          0          1        1     $00000000$ ?????
$00000000$ ?????
dc9f6fc4 dcpdp_queue           0          0          1        0     $00000000$ ?????
$00000000$ ?????
0ee2defc mlag_queue            0          0          1        1     $00000000$ ?????
$00000000$ ?????
e6f9a3f4 VPC Consistency       0          0          1        0     $00000000$ ?????
$00000000$ ?????
e6f97944 stats_app_queue       0          0          1        1     $00000000$ ?????
$00000000$ ?????
e6f97464 rpcap_Usb_Captu       0          0          1        0     $00000000$ ?????
$00000000$ ?????
e6f96d34 rpcap_CPU_Pkt_Q       0          0          0        0     $00000000$ ?????
$00000000$ ?????
e6f96ad4 rpcap_Mgmt_Queu       0          0          0        1     $00000000$ ?????
$00000000$ ?????
e6f965c4 fip keepalive q       0          0          1        0     $00000000$ ?????
$00000000$ ?????
e6f96384 fip timer q           0          0          0        1     $00000000$ ????? $089640085$
fipSnoopTask + 0x115
e6f960ac fip event q           0          0          0        1     $00000000$ ????? $089640044$
fipSnoopTask + 0xd4
e6f95eac fip session q         0          0          0        0     $00000000$ ????? $089640007$
fipSnoopTask + 0x97
```

```
e6f94874 mvr_PDU_Queue          0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f94674 mvr_Mgmt_Queue         0          0          0          1     $00000000$ ?????
$00000000$ ?????
e6f93e74 openflowDatapat        0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f93cc4 OFPROTO_FP_RCV_        0          0          0          0     $00000000$ ????? $08d0df95$
run + 0x85
e6f93514 openflowProtoQu        0          0          0          0     $00000000$ ????? $08d00e01$
openflowProtoTask + 0x2e1
e6f93314 openflowQueue          0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f8f13c boxsReqQ               0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f8ef44 boxsRespQ              0          0          0          0     $00000000$ ????? $083dc0b5$
boxsReqTask + 0x2e5
e6f8c5ac udldPduQueue           0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f8c3ac udldProcessQueu        0          0          0          1     $00000000$ ?????
$00000000$ ?????
e6f8b724 isdpPduQueue           0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f8b524 isdpProcessQueu        0          0          0          1     $00000000$ ?????
$00000000$ ?????
e6f8acec dhcpClientQueue        0          0          0          1     $00000000$ ????? $082eeeaf$
dhcpClientTask + 0xef
e6f89d84 lldp_Queue             0          0          1          2     $00000000$ ?????
$00000000$ ?????
e6f89814 dcvpnRIOTMlagQu        0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f87b04 dcVpnRIOTSockMs        0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f86dfc dcVpnRIOTCnfgrQ        0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f86444 dcvpn_mlag_queu        0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f84f6c dcVpnAgeEventQu        0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f82f84 OSPFv3 Proto_q3        0          0          0          0     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f82d84 dcVpnL2addrQueu        0          0          1          0     $00000000$ ?????
$00000000$ ?????
c2ffdda4 dcVpnCnfgrQueue        0          0          1          3     $00000000$ ?????
$00000000$ ?????
e6f82aac OSPFv3 Proto_q2        0          0          0          0     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f828ac OSPFv3 Proto_q1        0          0          0          0     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f82544 OSPFv3 Proto_q0        0          0          0          3     $00000000$ ?????
$00000000$ ?????
e6f81a24 DHCPv6 Server P        0          0          1          2     $00000000$ ?????
$00000000$ ?????
e6f81274 OSPFV3 redist q        0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f81074 OSPFV3 task que        0          0          0          4     $00000000$ ?????
$00000000$ ?????
e6f7f364 ip6Map_Process_        0          0          1         42     $00000000$ ?????
$00000000$ ?????
e6f7f094 ip6Map_Exceptio        0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f7ee8c ip6Map_LocalDat        0          0          1          3     $00000000$ ?????
$00000000$ ?????
```

```
e6f7d37c voip_Queue              0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f7d17c aclEventQueue           0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f77c54 pimsmMapDataPkt         0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f77a4c pimsmMapCtrlPkt         0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f777e4 pimsmMapEventsQ         0          0          0         37     $00000000$ ?????
$00000000$ ?????
e6f77574 pimsmMapAppTmrQ         0          0          0          2     $00000000$ ????? $08a852ea$
pimsmMapTask + 0x1bb
e6f76414 pimdmMapCtrlPkt         0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f76214 pimdmMapEventsQ         0          0          0          4     $00000000$ ?????
$00000000$ ?????
e6f75eb4 pimdmMapAppTmrQ         0          0          0          0     $00000000$ ????? $08a4f671$
pimdmMapTask + 0x13d
e6f7512c dvmrpMapPktQueu         0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f74f2c dvmrpMapMsgQueu         0          0          0          2     $00000000$ ?????
$00000000$ ?????
e6f74bec dvmrpMapAppTime         0          0          0          0     $00000000$ ????? $089fdf74$
dvmrpMapTask + 0x100
e6f74704 mgmdMapPktQueue         0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f74504 mgmdMapMsgQueue         0          0          0         10     $00000000$ ?????
$00000000$ ?????
e6f741a4 mgmdMapAppTimer         0          0          0          1     $00000000$ ????? $08a395c8$
mgmdMapTask + 0x184
e6f727f4 bgpMapNbrAutode         0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f7251c BGP Protocol_q5         0          0          0          0     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f7231c BGP Protocol_q4         0          0          0          1     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f72044 BGP Protocol_q3         0          0          0          1     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f71e44 BGP Protocol_q2         0          0          0          1     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f71b6c BGP Protocol_q1         0          0          0          0     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f7196c BGP Protocol_q0         0          0          0          4     $00000000$ ????? $08f02283$
DebugQueues + 0xa3
e6f7077c mcastMapPktMsgQ         0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f7039c mcastMapMsgQueu         0          0          0          6     $00000000$ ?????
$00000000$ ?????
e6f70134 mcastMapAppTmrM         0          0          0          2     $00000000$ ????? $08a1b29d$
mcastMapTask + 0x1b1
e6f6fe54 Bgp Redist Q            0          0          0          2     $00000000$ ?????
$00000000$ ?????
e6f6fc5c Bgp-Proc-Q              0          0          0          3     $00000000$ ????? $08471f78$
bgpProcTask + 0x68
e6f6edd4 RLIM cnfgr queu         0          0          1          1     $00000000$ ?????
$00000000$ ?????
d9bd0dec RLIM-t task que         0          0          1          0     $00000000$ ?????
$00000000$ ?????
d99d0dec RLIM task queue         0          0          1          3     $00000000$ ?????
$00000000$ ?????
d98d0dec rtrDiscProcessQ         0          0          1          4     $00000000$ ?????
$00000000$ ?????
```

```
d9fd0dec IP_Helper_Fwd_Q       0          0          1         1     $00000000$ ?????
$00000000$ ?????
e6f6eb44 vrrp_Queue            0          0          1         3     $00000000$ ?????
$00000000$ ?????
f31f233c openrMsgQueue         0          0          1         3     $00000000$ ?????
$00000000$ ?????
f31e170c ipMapArpMlagQue       0          0          1         1     $00000000$ ?????
$00000000$ ?????
f31b8ae4 ARP Timer_q0          0          0          0         1     $00000000$ ?????
$00000000$ ?????
df4f8a84 arpUnkL2Queue         0          0          0         1     $00000000$ ?????
$00000000$ ?????
df4f888c arpCbQueue            0          0          0         3     $00000000$ ????? $08e4f851$
ipMapArpCallbackTask + 0xf1
f344d43c arpReissueQueue       0          0          0         0     $00000000$ ?????
$00000000$ ?????
e6f40064 pbr_Queue             0          0          1         1     $00000000$ ?????
$00000000$ ?????
e6f3e6d4 ipMap_Process_Q       0          0          1        70     $00000000$ ?????
$00000000$ ?????
e6f3e3ac ipMap_ARP_Queue       0          0          0         0     $00000000$ ????? $08e687df$
ipMapForwardingTask + 0x9f
e6f3e1fc ipMap_Fwd_HighP       0          0          0         0     $00000000$ ????? $08e687df$
ipMapForwardingTask + 0x9f
e6f3df24 ipMap_Fwd_Prior       0          0          0         2     $00000000$ ?????
$00000000$ ?????
e6f3dd24 ipMap_Fwd_Queue       0          0          0         0     $00000000$ ????? $08e687df$
ipMapForwardingTask + 0x9f
e6f3ce9c sshdQueue             0          0          1         1     $00000000$ ?????
$00000000$ ?????
e6f3c1e4 ssltQueue             0          0          1         1     $00000000$ ?????
$00000000$ ?????
e6f3bcb4 RAGUARD Evnt Q        0          0          0         1     $00000000$ ?????
$00000000$ ?????
f7193874 sflowPacketQueu       0          0          0         0     $00000000$ ?????
$00000000$ ?????
e6f37e44 sflowPacketQueu       0          0          0         0     $00000000$ ?????
$00000000$ ?????
e6f37c44 sflowEventQueue       0          0          0         1     $00000000$ ?????
$00000000$ ?????
e6f368e4 dos_Queue             0          0          1         1     $00000000$ ?????
$00000000$ ?????
df1f87dc dhcpsMap_Fwd_Qu       0          0          1         0     $00000000$ ?????
$00000000$ ?????
e6f357ec LogCfgQ               0          0          1         1     $00000000$ ?????
$00000000$ ?????
e6f350ac DHCP Server Pro       0          0          1         1     $00000000$ ?????
$00000000$ ?????
e6f34bd4 trapQueue             0          0          1         2     $00000000$ ?????
$00000000$ ?????
f3429134 dot3ad_mlag_pdu       0          0          1         0     $00000000$ ?????
$00000000$ ?????
f5300c34 dot3ad_queue          0          0          1         6     $00000000$ ?????
$00000000$ ?????
f311021c dot3ad_timer_qu       0          0          1         6     $00000000$ ?????
$00000000$ ?????
e6f30ee4 snoop_MLD_PDU_Q       0          0          0         0     $00000000$ ?????
$00000000$ ?????
e6f30cdc snoop_IGMP_PDU_       0          0          0         0     $00000000$ ?????
$00000000$ ?????
e6f30a0c snoop_Timer_Que       0          0          0        67     $00000000$ ?????
$00000000$ ?????
```

```
e6f30804 snoop_MFDB_Noti       0          0          0          0     $00000000$ ????? $092fd6e5$
snoopTask + 0x3b5
e6f3058c snoop_Queue           0          0          0          4     $00000000$ ????? $092fd3e9$
snoopTask + 0xb9
e6f2f064 tacacs_queue          0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f2e87c macal_Queue           0          0          1          1     $00000000$ ?????
$00000000$ ?????
df3f8b34 dot1s_mlag_help       0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f2d994 radiusClusterin       0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f2d794 radius_queue          0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f2c434 dot1xQueue            0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f2b7ac dot1s_signal_qu       0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f2b5ac dot1s_stateCB_q       0          0          0         64     $00000000$ ?????
$00000000$ ?????
e6f2b24c dot1s_queue           0          0          0         67     $00000000$ ?????
$00000000$ ?????
e6f2a724 dot1qMsgQueue         0          0          1          2     $00000000$ ?????
$00000000$ ?????
e6f29ee4 edb queue             0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f2874c snmp trap queue       0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f2825c DAI Pkt Q             0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f28064 DAI Evnt Q            0          0          0          1     $00000000$ ?????
$00000000$ ?????
e6f276b4 DHCPV6 snp pkt        0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f2734c DHCPV6 snp evnt       0          0          0          1     $00000000$ ?????
$00000000$ ?????
e6f26a2c DHCP snp pkt q        0          0          0          0     $00000000$ ?????
$00000000$ ?????
e6f2682c DHCP snp evnt q       0          0          0          1     $00000000$ ?????
$00000000$ ?????
e6f25f14 pml_Queue             0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f256cc fdb_mlag_age_qu       0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f254cc fdb_mlag_queue        0          0          1          0     $00000000$ ?????
$00000000$ ?????
e6f248a4 FDQ-Q                 0          0          1          3     $00000000$ ?????
$00000000$ ?????
e6f2416c ErspanCnfgrQueu       0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f22e0c TimeRange Proce       0          0          1          2     $00000000$ ?????
$00000000$ ?????
e6f217cc cmgrInsertQueue       0          0          1         15     $00000000$ ?????
$00000000$ ?????
e6f215d4 cmgrQueue             0          0          1          7     $00000000$ ?????
$00000000$ ?????
e6f1fac4 bfd_pdu_queue         0          0          0          0     $00000000$ ????? $081cd258$
hapiBroadBfdCtrlTask + 0x98
e6f1e08c hapiMcAsyncQ          0          0          1          1     $00000000$ ?????
$00000000$ ?????
e6f1ddb4 hapiMcastRpfAsy       0          0          0          0     $00000000$ ????? $08120ee1$
hapiBroadL3McastAsyncRpfHandle + 0x51
```

```
e6f1dbb4 hapiMcastAsyncC       0          0          0        1     $00000000$ ????? $0812146b$
hapiBroadL3McastAsyncRouteAddDeleteHandle + 0x8b
e6f1d40c hapiL3WaitQ           0          0          0        1     $00000000$ ?????
$00000000$ ?????
e6f1d204 hapiBroadL3Link       0          0          0        1     $00000000$ ????? $081c1d36$
hapiBroadL3AsyncTask + 0x106
e6f1cd2c hapiL3WakeQ           0          0          1        1     $00000000$ ?????
$00000000$ ?????
e6f1b66c hapiL2AsyncCmdQ       0          0          1        1     $00000000$ ?????
$00000000$ ?????
e6f1b194 hapiLagAsyncCmd       0          0          0        1     $00000000$ ????? $08103d4e$
hapiBroadLagAsyncProcessMessages + 0x7e
e6f1ad1c hapiDot1sAsyncC       0          0          0       19     $00000000$ ????? $0810a445$
hapiBroadDot1sStateAsyncSet + 0x675
f10e8964 hapiL2AsyncCmdQ       0          0          1        0     $00000000$ ?????
$00000000$ ?????
f10e8714 hapiL2McastAsyn       0          0          0        0     $00000000$ ?????
$00000000$ ?????
f10e823c hapiL2McastAsyn       0          0          0        0     $00000000$ ?????
$00000000$ ?????
f10c051c hapiL2AddrFlush       0          0          1        1     $00000000$ ?????
$00000000$ ?????
f53008c4 dtlAddrQueue          0          0          1        1     $00000000$ ?????
$00000000$ ?????
f10bdc1c hapiLinkStatusQ       0          0          1        1     $00000000$ ?????
$00000000$ ?????
f10bd8bc hapiDebounceTim       0          0          1        0     $00000000$ ?????
$00000000$ ?????
f10bd26c hapiRxTxCapture       0          0          1        0     $00000000$ ?????
$00000000$ ?????
f10bcd94 hapiRxQueue           0          0          1        3     $00000000$ ?????
$00000000$ ?????
f10bc8bc hapiTxBpduQ           0          0          1        0     $00000000$ ?????
$00000000$ ?????
f3105ccc dtlqueue              0          0          1        3     $00000000$ ?????
$00000000$ ?????
f10b8b3c dapiDebugQueue        0          0          1        0     $00000000$ ?????
$00000000$ ?????
0edb611c cli_web_mgr_que       0          0          1        0     $00000000$ ?????
$00000000$ ?????
f1085bac userMgrQueue          0          0          0        0     $00000000$ ?????
$00000000$ ?????
f105d3a4 NIM-Q                 0          0          1       54     $00000000$ ?????
$00000000$ ?????
f10218d4 Cnfgr_Msg_Q2          0          0          0       95     $00000000$ ????? $08284615$
cnfgrApiInit + 0x1a5
f1020694 Cnfgr_Msg_Q1          0          0          1        1     $00000000$ ?????
$00000000$ ?????
f22f8b7c Routing Timer_q       0          0          0        0     $00000000$ ?????
$00000000$ ?????
f22def44 debug_cfg_queue       0          0          1        0     $00000000$ ?????
$00000000$ ?????
f730f394 LogUsbQueue           0          0          1        0     $00000000$ ?????
$00000000$ ?????
f7308efc LoqEmailAlert         0          0          1        0     $00000000$ ?????
$00000000$ ?????
f730725c LogQ                  0          0          1        1     $00000000$ ?????
$00000000$ ?????
```

5-172 debug packet-trace

Enable trace function for the packet trace feature.

debug packet-trace

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

sFlow Commands

sFlow monitors high-speed switch and routed networks to give complete visibility into network activity, enabling effective management and control of network resources.

5-173 sflow receiver

Configure the following sFlow: owner string, receiver timeout, max datagram size, IP address, and port.

No command sets the sFlow collector parameters to defaults.

Note: This command configures a receiver as a nontimeout entry. Unlike entries configured with a specific timeout value, this command is persistent and available in show running-config. As a nontimeout entry, the related sampler and pollers information is persistent and available in the running-config.

sflow receiver *rcvr_idx* **{owner** *owner-string* **{timeout** *rcvr_timeout* **| notimeout} | max-datagram** *size* **| ip** *ip* **| port** *port***}**

no sflow receiver *indx* **{ip** *ip-address* **| maxdatagram** *size* **| owner** *string* **timeout** *interval* **| port** *14-port***}**

Parameters

rcvr_idx	
owner *owner-string*	The identity string (sFlowRcvrTable) for the receiver, range: 127 characters (default: null string). An empty string indicates an unclaimed entry and the configuration is set to default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. Before assigning a receiver to a sampler/poller, the entry must be first claimed, set owner string to non-null value.

timeout *rcvr_timeout*	Time string, in seconds (range: 0-2147483647, default: 0), states the remaining value before sampler/poller is released, no further samples are transmitted to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the expiration.
notimeout	Entries with notimeout entry are assigned config until the assigned otherwise.
max-datagram *size*	The defined maximum number of data bytes for a single sample datagram (range: 200 to 9116, default: 1400). Set management entity to avoid fragmentation of the sFlow datagrams.
ip *ip*	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams are sent.
port *port*	The destination Layer4 UDP port for sFlow datagrams, range is 1-65535. The default is 6343.

Default

The default is None.

Command Mode

Global Config

5-174 sflow receiver owner timeout

Configure receiver as a timeout entry. Indicated information related to sampler and pollers are also displayed in the running-config (persistent).

Receiver configures set to a specific value are not displayed in running-config. Sampler and poller information related to this receiver is also not displayed in running-config.

sflow receiver *index* **owner** *owner-string* **timeout**

Parameters

index	Receiver index identifier, range: 1 to 8.
owner *owner-string*	Corresponding owner name of receiver, entity in use for sFlowRcvrTable. The range is 127 characters, default is a null string. An empty string indicates an unclaimed entity and receiver configuration is set to the default. Before an entity can claimed--to assign a receiver to a sampler or poller--an sFlowRcvrTable entry, it must first be unclaimed, owner string to be set to a non-null value.

Default

The default is None.

Command Mode

Global Config

5-175 sflow receiver owner notimeout

Configure a receiver as a non-timeout entry. The command does not have a timeout value making it persistent, it displays in running-config. As a non-timeout entry, the related sampler / poller information is displayed in the running-config.

When configured with a specific value, the receiver configuration is not shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

sflow receiver *rcvr_idx* **owner** *owner-string* **notimeout**

Parameters

rcvr_idx	Receiver index identifier.
owner *owner-string*	Owner string corresponds to the receiver name. The identity string (range: 127 characters, default: null string). The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. Before an entity can claimed--to assign a receiver to a sampler or poller--an sFlowRcvrTable entry, it must first be unclaimed, owner string to be set to a non-null value.

Default

The default is None.

Command Mode

Global Config

5-176 sflow sampler

Configure new sFlow sampler instance on an interface or range of interfaces for data source, rcvr_idx must be valid.

No command resets sFlow sampler instance to default settings.

Note: Poller is defined as a data source configured to collect flow samples.

sflow sampler {*rcvr-indx* **| rate** *sampling-rate* **| maxheadersize** *size***}**

no sflow sampler {*rcvr-indx* **| rate** *sampling-rate* **| maxheadersize** *size***}**

Parameters

rcvr-indx	sFlow Receiver for reception of flow samples. A value of zero (0) defines that receiver is not configured, packets will not be sampled. Only active receivers can be set. Expiration on a receiver also expires all associated samplers. Possible values are 1-8. The default is 0.
rate *sampling-rate*	The statistical sampling rate for defined packet sampling. A value of 1

	counts all packets, while a value of 0 disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. Range: 1024 – 65536, 0. The default is 0.
maxheadersize *size*	Maximum number of bytes to be copied from the sampler packet. The range is 20-256, default is 128. Set to zero (0) to set parameters to their corresponding default value.

Default

The default is None.

Command Mode

interface Config

5-177 sflow poller

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance on an interface or range of interfaces for this data source if rcvr_idx is valid.

Use the **no** command to reset the sFlow poller instance to the default settings.

Note: The sFlow task is heavily loaded when the sFlow polling interval is configured at the minimum value (i.e., one second for all the sFlow supported interfaces). In this case, the sFlow task is always busy collecting the counters on all the configured interfaces. This can cause the device to hang for some time when the user tries to configure or issue show sFlow commands. To overcome this situation, sFlow polling interval configuration on an interface or range of interfaces is controlled as mentioned below:

1. The maximum number of allowed interfaces for the polling intervals max (1, (interval - 10)) to min ((interval + 10), 86400) is:
   interval * 5
2. For every one second increment in the polling interval that is configured, the number of allowed interfaces that can be configured increases by 5.

sflow poller {*rcvr-indx* **| interval** *poll-interval***}**

no sflow poller {*rcvr-indx* **| interval** *poll-interval***}**

Parameters

rcvr-indx	Enter the sFlow Receiver associated with the sampler/poller. A value of zero (0) means that no receiver is configured. The range is 1-8. The default is 0.
interval *poll-interval*	Enter the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. When set to zero (0), all the poller parameters are set to their corresponding default value. The range is 0-86400. The default is 0. A value of N means once in N seconds a counter sample is generated.

Default

The default is None.

Command Mode

Interface Config

5-178 sflow sampler rate

Use this command to set the sampling rate for ingress/egress/flow-based sampling on this interface.

Use the **no** command to remove the sampling rate for ingress/egress/flow-based sampling on this interface.

sflow sampler rate *value*

no sflow sampler rate value

Parameters

value

Default

The default is 0 (sampling rate).

Command Mode

Interface Config

5-179 sflow source-interface

Specify the physical or logical interface for use with the sFIow client source interface. Once configured, source Interface address is used for all sFlow communications between the sFlow receiver and the sFlow client. When configured interface is down, sFlow client returns to normal operation.

No command resets the sFlow source interface to default.

sflow source-interface {*slot/port* **| loopback** *loopback-id* **| network | serviceport | tunnel** *tunnel-id* **| vlan** *vlan-id***}**

no sflow source-interface

Parameters

slot/port	Specifies the port to use as the source interface.
loopback *loopback-id*	Specifies the loopback interface to use as the source interface. The range of the loopback lD is 0 to 7.
network	Specifies the network source IP address
serviceport	Specifies the serviceport source IP address

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

Default

The default is None.

Command Mode

Global Config

5-180 show sflow agent

The sFlow agent is used to collect time-based sampling of network interface statistics and flow-based information. The sampling is sent to the configured sFlow receivers. The command displays sFlow agent information.

show sflow agent

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI output example.

```
(Routing)#show sflow agent

sFlow Version..................................... 1.3;
IP Address........................................ 10.131.12.66
```

Display Parameters

sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string has the following structure: MIB Version, Organization, Software Revision. • MIB Version: 1.3, the version of this MIB. • Organization: Company • Revision: 1.0.
IP Address	The IP address associated with the agent sampling.

5-181 show sflow pollers

Display the sFlow polling instances available on the switch. Use “-” for range.

show sflow pollers

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch) #show sflow pollers

Poller Data Source   Receiver Index  Poller Interval
------------------   --------------  ---------------
0/1                  1               10
```

Display Parameters

Poller Data Source	sFlowDataSource (slot/port) for this sFlow sampler. The agent only supports Physical ports.
Receiver Index	sFlowReceiver associated with the identified sFlow counter poller.
Poller Interval	Interval period between called counter samplings associated with the data source.

5-182 show sflow receivers

Display configuration information related to the sFlow receivers.

show sflow receivers [index]

Parameters

index	(Optional) Enter Receiver Index <1-8>.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of a CLI display output (sflow receivers).

```
(Routing)#show sflow receivers 1

Receiver Index..................................... 1
Owner String....................................... minorblues
Time out........................................... 0
IP Address:........................................ 0.0.0.0
Address Type....................................... 1
Port............................................... 6343
Datagram Version................................... 5
Maximum Datagram Size.............................. 1400
```

The following is an example of a show CLI display output (receiver configured as a non-timeout entry).

```
(Routing)#show sflow receivers

Rcvr Index   Owner String    Timeout      Max Dgram Size     Port    IP Address
-----------  --------------  -----------  --------------     -----   -----------
1            minorblues      No Timeout   1400               6343    0.0.0.0
2                            0            1400               6343    0.0.0.0
3                            0            1400               6343    0.0.0.0
4                            0            1400               6343    0.0.0.0
5                            0            1400               6343    0.0.0.0
6                            0            1400               6343    0.0.0.0
7                            0            1400               6343    0.0.0.0
8                            0            1400               6343    0.0.0.0

(Routing)#show sflow receivers 1

Receiver Index..................................... 1
Owner String....................................... minorblues
Time out........................................... 0
IP Address:........................................ 0.0.0.0
Address Type....................................... 1
Port............................................... 6343
Datagram Version................................... 5
Maximum Datagram Size.............................. 1400
```

Display Parameters

Receiver Index	sFlow Receiver associated with the sampler/poller.
Owner String	Identity string for receiver, used by FlowRcvrTable entry.
Time Out	The period of time (seconds) before receiver is released and transmission samples to sFlow receiver is halted. A no timeout value defines sFlow receiver as a non-timeout entry.
Max Datagram Size	Maximum number of bytes allowed in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.
IP Address	The sFlow receiver IP address.
Address Type	The sFlow receiver IP address type. IPv4 address value is 1.
Datagram Version	sFlow protocol version to be used when sending samples to sFlow receiver.

5-183 show sflow samplers

Display the sFlow sampling instances available on the switch.

show sflow samplers

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an output example.

```
(Routing)#show sflow samplers

Sampler Data Source     Receiver Index  Remote Agent    Ingress Sampling Rate
--------------------    --------------  ------------    ---------------------
0/1                     1               2               1024

Flow Sampling Rate   Egress Sampling Rate    Max Header Size    IP ACL     MAC ACL
------------------   --------------------    ---------------    ------     --------
2048                 4096                    128                1001
```

Display Parameters

Sampler Data Source	sFlowDataSource (slot/port) for this sFlow sampler. This agent only supports Physical ports.
Receiver Index	sFlowReceiver configured for this sampler.
Remote Agent	Remote agent instance index number.
Ingress Sampling Rate	Sampling rate for the ingress.
Flow Sampling Rate	Statistical sampling rate for packet sampling from this source.
Egress Sampling Rate	Sampling rate for the egress.
Max Header Size	Maximum number of bytes from a packet required to form a flow sample.
IP ACL	Associated IP ACL.
MAC ACL	Associated MAC ACL.

5-184 show sflow source-interface

Display the sFlow source interface available on the switch.

show sflow source-interface

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)#show sflow source-interface

sFlow Client Source Interface.................... serviceport
sFlow Client Source IPv4 Address................. 192.168.0.1               [Up]
sFlow Client Source IPv6 Address................. fe80::205:64ff:fe2f:f80   [Up]
```

Display Parameters

sFlow Client Source Interface	Physical or logical interface ID configured as the sFlow client source interface.

sFlow Client Source IPv4 Address	IP address of interface configured for the sFlow client source interface.

Switch Database Management Template Commands

Switch Database Management (SDM) templates allow for combinations of scaling factors in order to allocate resources. In addition, SDM templates enable the reallocation of system resources to support a different mix of features based on network requirements.

5-185 sdm prefer

Sets the template to active after the next reboot. The keywords are as follows:

- **dual-ipv4-and-ipv6** – Filters subsequent template choices supporting both IPv4 and lPv6, and maximizes the number of IPv4 and IPv6 unicast routes while limiting the number of ECMP next hops in each route to 4. The **data-center** template supports more ECMP next hops entries than dcvpn-data-center:

```
dual-ipv4-and-ipv6 alpm:

ARP Entries..................................... 2560
IPv4 Unicast Routes............................. 32768
IPv6 NDP Entries................................ 2560
IPv6 Unicast Routes............................. 24576
ECMP Next Hops.................................. 48
IPv4 Multicast Routes........................... 0
IPv6 Multicast Routes........................... 0

dual-ipv4-and-ipv6 alpm:

ARP Entries..................................... 2560
IPv4 Unicast Routes............................. 32768
IPv6 NDP Entries................................ 2560
IPv6 Unicast Routes............................. 24576
ECMP Next Hops.................................. 16
IPv4 Multicast Routes........................... 0
IPv6 Multicast Routes........................... 0
```

- **ipv4-routing** – Filters subsequent template choices to those that support IPv4, and not IPv6. The IPv4-routing default template maximizes the number of IPv4 unicast routes, while limiting the number of ECMP next hops in each route to 4. The **data-center default** template supports increases the number of ECMP next hops to 32 and reduces the number of routes. The **data-center plus** template increases the number of ECMP next hops to 32 while keeping the maximum IPv4 routes.

Note: A reboot is required after setting the template.

No command reverts to the default template. A reboot is required.

sdm prefer {dual-ipv4-and-ipv6 { alpm | data-center | dcvpn-data-center | default} | ipv4-routing {alpm | {data-center {default | plus} dcvpn-data-center | default}}

no sdm prefer

Parameters

dual-ipv4-and-ipv6 alpm	Lists the scaling parameters for the the Dual IPv4 and IPv6 alpm template supporting more IPv4 unicast routes.
dual-ipv4-and-ipv6 data-center	List the scaling parameters for the Dual IPv4 and IPv6 template supporting more ECMP next hops entries than dcvpn-data-center.
dual-ipv4-and-ipv6 dcvpn-data-center	List the scaling parameters for the Dual IPv4 and IPv6 template supporting less ECMP next hops entries than data-center.
dual-ipv4-and-ipv6 default	List the scaling parameters for the the Dual IPv4 and IPv6 default template supporting balance IPv4 and IPv6 entries.
ipv4-routing alpm	List the scaling parameters for the IPv4-only template supporting more IPv4 routes.
ipv4-routing data-center default	List the scaling parameters for the IPv4-only template maximizing the number of unicast routes and also supporting more ARP entries in IPv4 routes.
ipv4-routing data-center plus	List the scaling parameters for the IPv4-only template maximizing the number of ARP entries and IPv4 routes.
ipv4-routing dcvpn-data-center	List the scaling parameters for the IPv4-only template maximizing the number of MAC address entries.
ipv4-routing default	List the scaling parameters for the IPv4-only template supporting the default setting.

Default

The default is ipv4-routing data-center plus.

Command Mode

Global Config

5-186 show sdm prefer

Use this command to view the currently active SDM template and its scaling parameters, or to view the scaling parameters for an inactive template. When invoked with no optional keywords, this command lists the currently active template and the template that will become active on the next reboot, if it is different from the currently active template. If the system boots with a non-default template, and you clear the template configuration, either using no sdm prefer or by deleting the startup configuration, show sdm prefer lists the default template as the next active template. To list the scaling parameters of a specific template, use that template's keyword as an argument to the command.

Use the optional keywords to list the scaling parameters of a specific template.

show sdm prefer [dual-ipv4-and-ipv6 {default | data-center | alpm | data-center | dcvpn-data-center| default} | ipv4-routing {default | data-center {default | plus}}]

Parameters

dual-ipv4-and-ipv6 default	(Optional) List the scaling parameters for the template supporting IPv4 and IPv6.
ipv4-routing	List template parameters for IPv4-only template.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an output sample of a SDM template. The next active SDM template has not been changed.

```
(Router)#show sdm prefer

The current template is the Dual IPv4 and IPv6 template.

ARP Entries..................................... 2560
IPv4 Unicast Routes............................. 8160
IPv6 NDP Entries................................ 2560
IPv6 Unicast Routes............................. 2048
ECMP Next Hops.................................. 48
IPv4 Multicast Routes........................... 1536
IPv6 Multicast Routes........................... 512
```

Display Parameters

ARP Entries	The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.
IPv4 Unicast Routes	The maximum number of IPv4 unicast forwarding table entries.
IPv6 NDP Entries	The maximum number of IPv6 Neighbor Discovery Protocol (NDP) cache entries.
IPv6 Unicast Routes	The maximum number of IPv6 unicast forwarding table entries.
ECMP Next Hops	The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.

SFP Transceiver Commands

Display SFP transceiver information. Transceivers that are compliant with the SFF-8472 (SFP+, SFP28) and SFF-8436(QSFP+, QSFP28) standards are supported.

5-187 show fiber-ports optical-transceiver

Display the diagnostic information of the SFP. The values are derived from the SFP's A2 (Diagnostics) table using the I²C interface.

show fiber-ports optical-transceiver {all | *slot/port*}

Parameters

all	Enter all for all interfaces.
slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show fiber-ports optical-transceiver all


                    Link   Link                        Nominal
                    Length Length                      Bit
                   50um   62.5um                      Rate
Port  Vendor Name   [m]    [m]    Serial Number   Part Number [Mbps] Rev   Compliance
----- --------      -----  ------ ------------    ----------  ----------   ----------
0/1   D-LINK        8      3      SA011G4000005   DEM-431XT    10300        10GBase-SR
0/2   D-LINK        8      3      SA011G4000005   DEM-431XT    10300  A     10GBase-SR
0/3   D-LINK        8      3      SA011G4000005   DEM-431XT    10300  C1    10GBase-SR
0/49  Volex Inc.    0      0      26201134400002  VAHS-26-0256 10300  x1    40GBase-CR4

(Routing)#show fiber-ports optical-transceiver 0/49

                    Link   Link                        Nominal
                    Length Length                      Bit
                   50um   62.5um                      Rate
Port  Vendor Name   [m]    [m]    Serial Number   Part Number [Mbps] Rev   Compliance
----- --------      -----  ------ ------------    ----------  ----------   ----------
0/49  Volex Inc.    0      0      26201134400002  VAHS-26-0256  10300   x1    40GBase-CR4
```

Display Parameters

Port	Indicates the port interface.
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.

5-188 show fiber-ports optical-transceiver-info

Display SFP vendor-related information. The values are derived from the SFP's A0 table using the I²C interface.

show fiber-ports optical-transceiver-info {all | *slot/port***}**

Parameters

All	Enter all for all interfaces.
slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Switching)#show fiber-ports optical-transceiver-info all

Port    Vendor Name       Link Length 50um [m]  Link Length 62.5 um [m]
-----   ----------------  --------------------  -----------------------
0/49    DQS-5000-54SQ28                      8                         3
0/51    DQS-5000-54SQ28                      8                         3
0/52    DQS-5000-54SQ28                      8                         3

Serial Number   Part Number  Nominal Bit Rate [Mbps]    Rev
-------------   -----------  -----------------------    -----
A7N2018414      AXM761       10300                      10
A7N2018472      AXM761       10300                      10
A7N2018501      AXM761       10300                      10

(Switching)#show fiber-ports optical-transceiver-info 0/49

Port    Vendor Name       Link Length 50um [m]  Link Length 62.5 um [m]
```

```
-----   ----------------  --------------------  ------------------------
0/49    DQS-5000-54SQ28                      8                         3

Serial Number   Part Number  Nominal Bit Rate [Mbps]    Rev
-------------   -----------  ----------------------    -----
A7N2018414      AXM761       10300                     10
```

Display Parameters

Port	Indicates the interface port.
Vendor Name	The full name of listed corporation, suggested: abbreviation of corporation name, SCSI company code, or the stock exchange symbol. The name is 1 to 16 ASCII characters in length.
Link Length 50um	The supported link length while operating in compliance with applicable standards using 50 micron multimode OM2 [500 MHz * km at 850nm] fiber. A value of zero designates no support for 50 micron multimode fiber or that the length information must be determined from the transceiver technology.
Link Length 62.5um	The link length as 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 designates no support for 62.5 micron multimode fiber or that the length information must be determined from the transceiver technology.
Serial Number	The serial number for the transceiver. The serial number is 1 to 16 ASCII characters in length. A zero value in the field indicates an unspecified vendor serial number.
Part Number	The vendor part number or product name. A zero value in the field indicates an unspecified vendor serial number
Nominal Bit Rate	The nominal bit (signaling) rate in 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 zero value indicates an unspecified bit rate to be determined from the transceiver technology. The actual information transfer rate is dependent on the encoding of the data, as defined by the encoding value.
Rev	Vendor product revision number. An empty field indicates that the vendor revision is unspecified.

Remote Monitoring Commands

Remote Monitoring (RMON) allows for the collection of network traffic data. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).

Note: No configuration commands are available for ether stats and high capacity ether stats. The data source for ether stats and high capacity ether stats are configured during initialization.

5-189 rmon alarm

Set the RMON alarm entry in the RMON alarm MIB group.

No command deletes the RMON alarm entry.

rmon alarm *alarm number variable sample interval* **{absolute | delta} rising-threshold** *value* **[rising-event-index] falling-threshold** *value* **[falling-event-index] [startup {rising | falling | rising-falling}] [owner string]**

no rmon alarm *alarm number*

Parameters

Alarm Index	Unique index identifying an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
Alarm Variable	Variable object identifier to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
Alarm Interval	Data sampling and comparison (seconds) of the rising and falling threshold. The range is 1 to 2147483647. The default is 1.
Alarm Absolute Value	Statistical value during the sampling period. This object is a read-only, 32-bit signed value.
Alarm Rising Threshold	Rising threshold for the statistical sample. The range is 2147483648 to 2147483647. The default is 1.
Alarm Rising Event Index	Rising event index once threshold is crossed. The range is 1 to 65535. The default is 1.
Alarm Falling Threshold	Falling threshold for the statistical sample. The range is 2147483648 to 2147483647. The default is 1.
Alarm Falling Event Index	Falling event index once threshold is crossed. The range is 1 to 65535. The default is 2.
Alarm Startup Alarm	Designate alarm type. Possible values are rising, falling or both rising-falling. The default is rising-falling.
Alarm Owner	The owner string associated with the alarm entry. The default is monitor Alarm.

Default

The default is None.

Command Mode

Global Config

Example

The following is an output example.

```
(Routing)(Config)#rmon alarm 1 ifInErrors.2 30 absolute rising-threshold 100 1
falling-threshold 10 2 startup rising owner myOwner
```

The following is an output example.

```
(Routing)(Config)#no rmon alarm 1
```

5-190 rmon hcalarm

Set the RMON hcalarm entry for the High Capacity RMON alarm MIB group.

No command deletes the rmon hcalarm entry.

rmon hcalarm *aiarm number variable sample interval* **{absolute | delta} rising-threshold high** *value* **low** *value* **status {positive | negative} [***rising-event-index***] falling-threshold high** *value* **low** *value* **status {positive | negative} [***falling-event-index***] [startup {***rising* **|** *falling* **|** *rising-falling***}] [owner** *string***]**

no rmon hcalarm *aiarm number*

Parameters

High Capacity Alarm Index	Integer index value to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable	Identifier of the sampled variable.
High Capacity Alarm Interval	Interval sampling period in seconds used to compare with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	Sampling method to obtain variables used to compare against the thresholds. Possible types are **Absolute Value** or **Delta Value**. The default is **Absolute Value**.
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) for the hcAlarmVariable statistic during last completed sampling period. This object is a 64-bit read-only, unsigned value.
High Capacity Alarm Absolute Alarm Status	Indicates the validity and sign of the data for the high capacity alarm object, high value (hcAlarmAbsValueobject). Possible status types are **valueNotAvailable** (default), **valuePositive**, or **valueNegative**.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm for sending. Possible values are **rising**, **falling**, or **rising-falling** (default).
High Capacity Alarm Rising-Threshold Absolute Value Low	Threshold value: lower 32 bits of the absolute value, for the sampling. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	Threshold value: upper 32 bits of the absolute value, for sampling. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	Object indicates the data sign for the rising threshold, as defined by hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive** (default), or **valueNegative**.
High Capacity Alarm Falling-Threshold Absolute Value Low	Lower 32 bits of the value defining threshold sampling. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm	Upper 32 bits of the value for threshold sampling. The range is 0 to

Falling-Threshold Absolute Value High	4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	Indicates the falling threshold's data sign, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive** (default), or **valueNegative**.
High Capacity Alarm Rising Event Index	Index of the eventEntry used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	Index of the eventEntry used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
High Capacity Alarm Failed Attempts	Failed number of associated hcAlarmVariable was polled by hcAlarmEntry.. This object is a 32-bit counter value that is read-only.
High Capacity Alarm Owner	Alarm entry owner string. The default is **monitorHCAlarm**.
High Capacity Alarm Storage Type	The configured type of non-volatile storage. This object is read-only. The default is **volatile**.

Default

The default is None.

Command Mode

Global Config

Example

The following is an output example.

```
(Routing)(Config)#rmon hcalarm 1 ifInOctets.1 30 absolute rising-threshold high 1 low
100 status positive 1 falling-threshold high 1 low 10 status positive startup rising
owner myOwner
```

The following is an output example.

```
(Routing)(Config)#no rmon hcalarm 1
```

5-191 rmon event

Sets the RMON event entry in the RMON event MIB group.

No command deletes the rmon event entry.

rmon event *event number* **[description** *string* **| type** *log* **| owner** *string* **| trap** *community***]**

no enable password

Parameters

event *number*	Variable identifying an entry in the event table. An entry identifies a

	single event. The range is 1 to 65535.
description *string*	(Optional) A description for the event entry. The default is **alarmEvent**.
type *log*	(Optional) Event notification type. Possible values are **None** (default), **Log**, **SNMP Trap**, **Log and SNMP Trap**.
owner *string*	(Optional) String describing owner entry. The default is **monitorEvent**.
trap *community*	(Optional) Specified SNMP community by this octet string which is used to send an SNMP trap. The default is **public**.

Default

The default is None.

Command Mode

Global Config

Example

The following is an output example.

```
(Routing)(Config)#rmon event 1 log description test
```

The following is an example of the output.

```
(Routing)(Config)#no rmon event 1
```

5-192 show rmon

This command displays the entries in the RMON alarm table.

show rmon {alarms | alarm *alarm-index* **| collection | events | hcalarm | hcalarms | history | log | statistics }**

Parameters

alarms	Show RMON alarm entries.
alarm *alarm-index*	Display the alarm table.
collection	Displays the configured requested group of statistics.
events	Displays the RMON event table.
hcalarm	Show RMON high capacity alarm entries.
hcalarms	Displays the high capacity alarm table.
history	Displays the RMON history ethernet statistics.
log	Display the RMON logging table.
statistics	Display RMON ethernet statistics.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show rmon alarms

Index      OID                  Owner
-------    -----------------    -------------
1          alarmInterval.1      MibBrowser
2          alarmInterval.1      MibBrowser
```

The following is a CLI display output example.

```
(Routing)#show rmon alarm 1

Alarm 1
---------------
OID: alarminterval 1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold: 1
Falling Threshold: 1
Rising Event: 1
Falling Event: 2
Owner: DLBrowser
```

Display Parameters

Alarm	Unique index identifying an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
OID	Object ID to which the variable name is resolved. The format is x.x.x.x.
Last Sample Value	Object ID of the last event.
Interval	Interval (seconds) defining rising and falling thresholds sampling and comparison period. The range is 1 to 2147483647. The default is 1.
Sample Type Absolute	Statistical value during the last sampling period. This object is a read-only, 32-bit signed value.
Startup Alarm	Specified alarm to send. Possible values are **rising**, **falling** or both **rising-falling**. The default is **rising-falling**.
Rising Threshold	Rising threshold for the statistical sample. The range is 2147483648 to 2147483647. The default is 1.

Falling Threshold	Falling threshold of statistical sample. The range is 2147483648 to 2147483647. The default is 1.
Rising Event	Entry index used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Falling Event	Entry index used when a falling threshold is crossed. The range is 1 to 65535, default is 2.
Owner	String associated with the alarm entry. The default is **monitorAlarm**.

5-193 show rmon collection history

Displays the RMON history control table.

show rmon collection history [interfaces *slot/port***]**

Parameters

interfaces *slot/port*	(Optional) Display RMON interface information.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show rmon collection history

Index   Interface    Interval     Requested    Granted      Owner
                                  Samples      Samples
-----   ----------   ----------   ----------   ----------   ------------
1       0/1          30           10           10           myowner
2       0/1          1800         50           10           monitorHistoryControl
3       0/2          30           50           10           monitorHistoryControl
4       0/2          1800         50           10           monitorHistoryControl
5       0/3          30           50           10           monitorHistoryControl
6       0/3          1800         50           10           monitorHistoryControl
7       0/4          30           50           10           monitorHistoryControl
```

The following is a CLI display output example.

```
(Routing)#show rmon collection history interfaces 0/1

Index   Interface    Interval     Requested    Granted      Owner
```

```
                                    Samples      Samples
-----   ----------   ----------   ----------   ----------   ------------
1       0/1          30           10           10           myowner
2       0/1          1800         50           10           monitorHistoryControl
```

Display Parameters

Index	Unique index identifing an entry in the historyControl table. The entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
Interface	Displays the interface ID.
Interval	Defined interval period in seconds for data sampling. The range is 1 to 3600. The default is 1800.
Requested	Variable defining number of discrete time intervals for the saving of data. The range is 1 to 65535. The default is 50.
Granted Samples	Designated discrete sampling intervals for the saving of data. This object is read-only. The default is 10.
Owner	Owner string associated with the history control entry. The default is monitorHistoryControl.

5-194 show rmon events

Display entries listed in RMON event table.

show rmon events

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show rmon events

Index   Description  Type    Community    Owner      Last time sent
-----   -----------  -----   ----------   -----      -------------------
1       test         log     public       MIB        0 days 0 h:0 m:0 s
```

Display Parameters

Event Index	Unique index identifying an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
Event Description	Description of the event entry. The default is alarmEvent.
Event Type	Notification event type. Possible values are **None** (default), **Log**, **SNMP Trap**, **Log and SNMP Trap**.
Event Owner	String describing associated entry owner. The default is **monitorEvent**.
Event Community	SNMP community, specific the octet string, used to send an SNMP trap. The default is **public**.
Owner	Defined event owner for entry.
Last time sent	Defined period of last transmission of log or a SNMP trap message.

5-195 show rmon history

Display specified entry in the RMON history table.

show rmon history *index* **{errors [period** *seconds***] | other [period** *seconds***] | throughput [period** *seconds***]}**

Parameters

Index	Index of the entry.
errors [period *seconds***]**	(Optional) Display the error counter period in seconds.
other [period *seconds***]**	(Optional) Display the drop and collision counter period in seconds.
throughput [period *seconds***]**	(Optional) Display the throughput counter period in seconds.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show rmon history 1 errors

Sample set: 1                 Owner: myowner
Interface: 0/1                Interval: 30
Requested Samples: 10         Granted Samples: 10
Maximum table size: 1758
```

```
Time                    CRC Align   Undersize   Oversize    Fragments    Jabbers
----------------------  ---------   ---------   --------    ---------    --------
Jan 01 1970 21:41:43    0           0           0           0            0
Jan 01 1970 21:42:14    0           0           0           0            0
Jan 01 1970 21:42:44    0           0           0           0            0
Jan 01 1970 21:43:14    0           0           0           0            0
Jan 01 1970 21:43:44    0           0           0           0            0
Jan 01 1970 21:44:14    0           0           0           0            0
Jan 01 1970 21:44:45    0           0           0           0            0
Jan 01 1970 21:45:15    0           0           0           0            0
Jan 01 1970 21:45:45    0           0           0           0            0
Jan 01 1970 21:46:15    0           0           0           0            0
```

The following is a CLI display output example.

```
(Routing)#show rmon history 1 throughput

Sample set: 1               Owner: myowner
Interface: 0/1              Interval: 30
Requested Samples: 10       Granted Samples: 10
Maximum table size: 1758

Time                    Octets      Packets     Broadcast   Multicast    Util
----------------------  --------    --------    ---------   ---------    ------
Jan 01 1970 21:41:43    0           0           0           0            1
Jan 01 1970 21:42:14    0           0           0           0            1
Jan 01 1970 21:42:44    0           0           0           0            1
Jan 01 1970 21:43:14    0           0           0           0            1
Jan 01 1970 21:43:44    0           0           0           0            1
Jan 01 1970 21:44:14    0           0           0           0            1
Jan 01 1970 21:44:45    0           0           0           0            1
Jan 01 1970 21:45:15    0           0           0           0            1
Jan 01 1970 21:45:45    0           0           0           0            1
Jan 01 1970 21:46:15    0           0           0           0            1
```

```
(Routing)#show rmon history 1 other

Sample set: 1               Owner: myowner
Interface: 0/1              Interval: 30
Requested Samples: 10       Granted Samples: 10
Maximum table size: 1758

Time                    Dropped      Collisions
----------------------  ---------    -----------
Jan 01 1970 21:41:43    0             0
Jan 01 1970 21:42:14    0             0
Jan 01 1970 21:42:44    0             0
Jan 01 1970 21:43:14    0             0
Jan 01 1970 21:43:44    0             0
```

```
Jan 01 1970 21:44:14      0              0
Jan 01 1970 21:44:45      0              0
Jan 01 1970 21:45:15      0              0
Jan 01 1970 21:45:45      0              0
Jan 01 1970 21:46:15      0              0
```

Display Parameters

Control Index	Unique identifier in a historyControl table. Each entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
Control Data Source	The source interface for which historical data is collected.
Control Buckets Requested	Designated number of discrete time intervals for the saving of data. The range is 1 to 65535. The default is 50.
Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
Control Buckets Granted	Designated number of discrete sampling intervals for the saving of data. This object is read-only. The default is 10.
Control Interval.	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
Control Owner	Owner string associated with the history control entry. The default is monitorHistoryControl.
Maximum Table Size	Maximum number of entries that the history table can hold.
Time	Period stamp in seconds for collected sample.
CRC Align	Number of CRC align errors.
Undersize Packets	Number of undersized packets, less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Packets	Total number of oversized packets longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets--not integral number of octets in length or with a bad Frame Check Sequence (FCS)--less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets; longer than 1518 octets (excluding framing bits, including FCS octets), not integral number of octets in length or had a bad Frame Check Sequence (FCS).
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good broadcasted packets received on the interface.
Multicast	Total number of good Multicast packets received on the interface.
Dropped	Displays the total number of dropped collisions.
Collisions	Displays the total number of collisions on the interface.

5-196 show rmon log

Displays the entry list in the RMON log table.

show rmon log [*event-index***]**

Parameters

event-index	Enter a unique Event Index (1-65535)

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Maximum table size	Maximum allowed of log entries.
Event	Defined event index.
Description	Event entry comment.
Time	Event entry time stamp.

5-197 show rmon statistics interfaces

Displays the RMON statistics for the specified interfaces.

show rmon statistics interfaces *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show rmon statistics interfaces 0/1
```

```
Port: 0/1
Dropped: 0
Octets: 0                    Packets: 0
Broadcast: 0                 Multicast: 0
CRC Align Errors: 0          Collisions: 0
Undersize Pkts: 0            Oversize Pkts: 0
Fragments: 0                 Jabbers: 0
64 Octets: 0                 65 - 127 Octets: 0
128 - 255 Octets: 0          256 - 511 Octets: 0
512 - 1023 Octets: 0         1024 - 1518 Octets: 0
HC Overflow Pkts: 0 HC Pkts: 0
HC Overflow Octets: 0 HC Octets: 0
HC Overflow Pkts 64 Octets: 0              HC Pkts 64 Octets: 0
HC Overflow Pkts 65 - 127 Octets: 0        HC Pkts 65 — 127 Octets: 0
HC Overflow Pkts 128 - 255 Octets: 0       HC Pkts 128 - 255 Octets: 0
HC Overflow Pkts 256 - 511 Octets: 0       HC Pkts 256 - 511 Octets: 0
HC Overflow Pkts 512 - 1023 Octets: 0      HC Pkts 512 - 1023 Octets: 0
HC Overflow Pkts 1024 - 1518 Octets: 0     HC Pkts 1024 - 1518 Octets: 0
```

Display Parameters

Port	Indicates the interface in slot/port format.
Dropped	Total number of interface dropped events.
Octets	Total number of octets received.
Packets	Total number of packets received (including error packets).
Broadcast	Total number of good broadcast packets received.
Multicast	Total number of good multicast packets received.
CRC Align Errors	Total number of packets received from 64 to 1518 octets (excluding framing bits, including FCS octets) inclusive.
Collisions	Total number of collisions.
Undersize Pkts	Total number of undersize packets, less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Pkts	Total number of oversize packets, longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or without a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets; longer than 1518 octets (excluding framing bits, including FCS octets) and not an integral number of octets in length or contain a bad Frame Check Sequence (FCS).
64 Octets	Total number of packets, 64 octets in length (excluding framing bits, including FCS octets).
65-127 Octets	Total number of packets from 65 to 127 octets in length (excluding framing bits, including FCS octets).

128-255 Octets	Total number of packets from 128 to 255 octets in length (excluding framing bits, including FCS octets).
256-511 Octets	Total number of packets from 256 to 511 octets in length (excluding framing bits, including FCS octets).
512-1023 Octets	Total number of packets from 512 to 1023 octets in length (excluding framing bits, including FCS octets).
1024-1518 Octets	Total number of packets from 1024 to 1518 octets in length (excluding framing bits, including FCS octets).
HC Overflow Pkts	Total number of HC overflow packets.
HC Overflow Octets	Total number of HC overflow octets.
HC Overflow Pkts 64 Octets	Total number of HC overflow packets, 64 octets in length.
HC Overflow Pkts 65 – 127 Octets	Total number of HC overflow packets from 65 to 127 octets in length.
HC Overflow Pkts 128 - 255 Octets	Total number of HC overflow packets from 128 to 255 octets in length.
HC Overflow Pkts 256 – 511 Octets	Total number of HC overflow packets from 256 to 511 octets in length.
HC Overflow Pkts 512 – 1023 Octets	Total number of HC overflow packets from 512 to 1023 octets in length.
HC Overflow Pkts 1024 – 1518 Octets	Total number of HC overflow packets from 1024 to 1518 octets in length.

5-198 show rmon hcalarms

Displays the entries in the RMON high-capacity alarm table.

show rmon {hcalarms | hcalarm *alarm index***}**

Parameters

hcalarms	Displays the high capacity alarm table.
hcalarm *alarm index*	Show RMON high capacity alarm entries, index: 1-65535.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show rmon hcalarms

Index  OID                 Owner
-----  ----------------    ------------
1      alarmInterval.1     MibBrowser
2      alarmInterval.1     MibBrowser
```

```
(Routing)#show rmon hcalarm 1

Alarm 1
---------------
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold High: 0
Rising Threshold Low: 1
Rising Threshold Status: Positive
Falling Threshold High: 0
Falling Threshold Low: 1
Falling Threshold Status: Positive
Rising Event: 1
Falling Event: 2
Startup Alarm: Rising-Falling
Owner: MibBrowser
```

Display Parameters

Alarm	Object identifier of sampled variable. Only variables that resolve to an ASN.1 primitive type of integer.
AlarmInterval	Interval defining in seconds the sampling/comparing period of rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
Last Sample Value	Displays the value of the statistic during the last sampling period.
Interval	Displays the interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	Sampling method of selected variable and calculating the value to be compared against the thresholds. Possible types are Absolute Value or Delta Value. The default is **Absolute Value**.
Startup Alarm	The designated startup alarm to be sent. Possible values are **rising**, **falling**, or **rising-falling**. The default is **rising-falling**.
High Capacity Alarm Index	Integer index value identifying capacity alarm entry. The range is 1 to 65535.
Rising Threshold High	The upper 32 bits of the threshold's absolute value. The range is 0 to 4294967295. The default is 0.
Rising-Threshold Low	The lower 32 bits of the threshold's absolute value. The range is 0 to 4294967295. The default is 1.

Rising Threshold Status	This indicated data sign of the rising threshold, defined by hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh objects. Possible values are **valueNotAvailable**, **valuePositive** (default), or **valueNegative**.
Falling Threshold High	The upper 32 bits of the threshold's absolute value. The range is 0 to 4294967295. The default is 0.
Falling Threshold Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
Failling Threshold Staus	The indicated data sign for the falling threshold, defined by hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh objects. Possible values are **valueNotAvailable**, **valuePositive** (default), or **valueNegative**.
Rising Event	Entry index used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Falling Event	Entry index used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Startup Alarm	The designated startup alarm to be sent. Possible values are **rising**, **falling**, or **rising-falling**. The default is **rising-falling**.
Owner	String defining the associated owner for the alarm entry. The default is **monitorHCAlarm**.
High Capacity Alarm Absolute Value	The absolute value, unsigned, of the hcAlarmVariable statistic during last sampling period. The value during the current sampling period is available after the period is completed. This object is a 64-bit unsigned value (Read-Only).

5-199 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.**No** command enables a port.

shutdown

no shutdown

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

5-200 shutdown all

Disables all ports.

Note: Shutdown all is available for physical and port-channel (LAG) interfaces, but not for VLAN routing interfaces.

Use the **no** command to enable all ports.

shutdown all

no shutdown all

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

5-201 speed

Enable or disable auto-negotiation and set the advertised port speed. The duplex parameter allows for both half and full duplex speed configuration.

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, set the speed and duplex mode.

Note: The support speed depends on the model.

speed auto {10G|25G|40G|100G} [10G|25G|40G|100G] [half-duplex | full-duplex]

speed {10G|25G|40G|100G} {half-duplex | full-duplex}

Parameters

half-duplex	Set to half duplex.
full-duplex	Set to full duplex.

Default

The default is Auto-negotiation.

Command Mode

Interface Config

5-202 show port

Display port information.

show port {*intf-range* **| all}**

Parameters

intf-range	Enter interface(s) in slot/port format, use comma for a list and hyphen for ranges.
advertise	Show the auto negotiation advertisement information.
all	Enter 'all' for all interfaces.
description	Display interface description.
fpti	Display front panel tap interface information.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an output example of all port entries.

```
(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
```

The following command is a port range output example.

```
(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
```

Display Parameters

Interface	Slot/port.
Type	Define port type, values are as follows: • 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 (default) in order for it to be allowed into the network.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, the duplex mode and speed is determined by the auto-negotiation process. 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	Port speed and duplex mode.
Link Status	Up or down.
Link Trap	Determiner for send trap function if link status changes. The factory default is enabled.
LACP Mode	Enabled or disabled.
Actor Timeout	Displays the timeout value for the actor admin key. By default, ports are set to use a long timeout value (90 seconds).

5-203 show port description

This command displays the interface description.

show port description {*slot/port* **| lag** *lag-id* | **loopback** *loopback-id* | **tunnel** *tunnel-id* | **VLAN** *vlan-id* **}**

Parameters

slot/port	Enter an interface in slot/port format.
lag *lag-id*	Enter an interface in lag format.
loopback *loopback-id*	Configuration of Loopback Interface.
tunnel *tunnel-id*	Configure IPv6 Tunnel.
vlan *vlan-id*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Switching)#show port description 0/1

Interface..................................... 0/1
ifIndex....................................... 1
Description.....................................
MAC address................................... 00:10:18:82:0C:10
Bit offset ................................... 1
```

Display Parameters

Interface	Slot/port or LAG with the information.
ifIndex	Interface index number associated with the port.
Description	The alpha-numeric description of the interface created by the command.
MAC address	Port MAC address in the following format: 6 two-digit hexadecimal numbers separated by colons, for example 01:23:45:67:89:AB.
Bit Offset	The bit offset value.

5-204 hardware profile portmode

Configure a 40G QSFP+ port in either 4x10G mode, 1x40G mode or a 100G QSFP28 port in either 1x100G, 2x50G, or 4x25G mode.

The function is only available on interfaces supporting expandable ports.

Note: Not avialble in interface range mode.

No command returns the port to default.

hardware profile portmode *mode*

no hardware profile portmode

Parameters

mode	Modes are dependent on the platform. Possible modes are: • 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. • 1x100G: Configure the port as a single 100G port using four lanes. The 100G ports may be reconfigured as 40G ports using the interface speed command. • 2x50G: Configure the port as two 50G ports, each using two lanes. This mode requires the use of a suitable 1x100G to 2x50G pigtail cable. • 4x25g: Configure the port as a four 25G ports, each on a separate lane. This mode requires a 4x25G to 1x100G breakout cable--can be reconfigured as 4x10G ports.

Default

The default is Platform-specific.

Command Mode

Interface Config

5-205 show interfaces hardware profile

Display the hardware profile information for the ports supporting expandable features. Available displays are 40G interface with corresponding 10G interfaces, 100G interface with corresponding 25G or 50G interfaces.

A reboot is required for new configuration settings to take effect. The interface displays both the configured mode and the current operational mode of the interface.

show interfaces hardware profile [interface]

Parameters

interface	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
 (Routing)#show interfaces hardware profile

40G Interface       10G Interfaces      Configured Mode     Oper Mode
---------------     ---------------     ---------------     ---------------
0/1                 0/17-20             1x40G               4x10G
0/2                 0/21-24             1x40G               1x40G

(Routing)#show interfaces hardware profile 0/1

40G Interface       10G Interfaces      Configured Mode     Oper Mode
---------------     ---------------     ---------------     ---------------
0/1                 0/17-20             1x40G               4x10G
```

Additional information for platforms supporting expandable ports (high density ports that can be split into multiple lane modes).

```
(Routing)#show interfaces hardware profile

100G/40G     Configured   Operating    Expandable   Expanded
Interface    Mode         Mode         Option(s)    Interfaces
---------    -----------  -----------  -----------  -----------
0/81         1x40G        1x40G        4x10G        0/93-96
0/82         1x40G        1x40G        4x10G        0/97-100
0/83         1x40G        1x40G        4x10G        0/101-104
0/84         1x40G        1x40G        4x10G        0/105-108
0/85         1x100G       1x100G       4x25G        0/109-112
                                       2x50G        0/125-126
0/86         1x100G       1x100G       4x25G        0/113-116
                                       2x50G        0/127-128
0/87         1x100G       1x100G       4x25G        0/117-120
                                       2x50G        0/129-130
0/88         1x100G       1x100G       4x25G        0/121-124
                                       2x50G        0/131-132


(Routing) #show interfaces hardware profile 0/85

100G/40G     Configured   Operating    Expandable   Expanded
Spanning-tree vlan priority Interface   Mode         Mode         Option(s)
      Interfaces
---------    -----------  -----------  -----------  -----------
0/85         1x100G       1x100G       4x25G        0/109-112
                                       2x50G        0/125-126
```

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.

.

5-206 spanning-tree

Sets the spanning-tree operational mode to enabled.

No 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.

spanning-tree

no spanning-tree

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

5-207 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.

Use the **no** command to reset the auto-edge status of the port to the default value.

spanning-tree auto-edge

no spanning-tree auto-edge

Parameters

None

Default

The default is Enabled.

Command Mode

lnterface Config

5-208 spanning-tree backbonefast

Use this command to enable the detection of indirect link failures and accelerate spanning tree convergence on PVST 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.

Use the **no** command to disable 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.

spanning-tree backbonefast

no spanning-tree backbonefast

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-209 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.

Use the **no** command to reset the auto-edge status of the port to the default value.

spanning-tree cost {*cost* **| auto}**
no spanning-tree cost

Parameters

cost	Enter an integer in the range of 1 – 20000000.
auto	Set the external pathcost value automatically on the basis of Link Speed.

Default

The default is Auto.

Command Mode

Interface Config

5-210 spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

Use the **no** command to disable BPDU Filter on the interface or range of interfaces.

spanning-tree bpdufilter

no spanning-tree bpdufilter

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-211 spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Use the **no** command to disable BPDU Filter on all the edge port interfaces.

spanning-tree bpdufilter default

no spanning-tree bpdufilter default

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-212 spanning-tree bpduguard

Enable BPDU Guard on the switch.

No command disables BPDU Guard on the switch.

spanning-tree bpduguard

no spanning-tree bpduguard

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-213 spanning-tree bpdumigrationcheck

Force a rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs transmission. Use the *slot/port* parameter to transmit a BPDU from a specified interface, or use the **all** keyword to transmit

BPDUs from all interfaces. The command forces the BPDU transmission execution. It does not change the system configuration nor does it have a “no” version.

spanning-tree bpdumigrationcheck {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Force all the ports to transmit RST or MST BPDUs.

Default

The default is None.

Command Mode

Global Config

5-214 spanning-tree configuration name

Set the Configuration Identifier Name to identify the current configuration. The string uses up to 32 characters.

No command resets the Configuration Identifier Name to default.

spanning-tree configuration name *name*

no spanning-tree configuration name

Parameters

name	Enter a string of at most 32 characters.

Default

The default is MAC address in hexadecimal notation.

Command Mode

Global Config

5-215 spanning-tree configuration revision

Set the Configuration Identifier Revision Level for to identify the current configuration. The Configuration Identifier Revision Level range: 0 to 65535.

No command sets the Configuration Identifier Revision Level to identify the current configuration.

spanning-tree configuration revision *0-65535*

no spanning-tree configuration revision

Parameters

None

Default

The default is 0.

Command Mode

Global Config

5-216 spanning-tree forward-time

Sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value in seconds, range: 4 to 30.

No command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default.

spanning-tree forward-time *4-30*

no spanning-tree forward-time

Parameters

None

Default

The default is 15.

Command Mode

Global Config

5-217 spanning-tree max-age

Set the Bridge Max Age parameter to a defined value for common and internal spanning tree. The max-age value range is: 6 to 40, with the value being less than or equal to *2 x (Bridge Forward Delay - 1)*.

No command sets the Bridge Max Age parameter to default.

spanning-tree max-age *6-40*

no spanning-tree max-age

Parameters

None.

Default

The default is 20.

Command Mode

Global Config

5-218 spanning-tree max hops

Sets the MSTP Max Hops parameter to a defined value for the common and internal spanning tree, range 1 to 127.

No command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

spanning-tree max-hops *1-127*

no spanning-tree max-hops

Parameters

None

Default

The default is 20.

Command Mode

Global Config

5-219 spanning-tree mode

Configure global spanning tree mode per VLAN spanning tree, Rapid-PVST, MST, RSTP or STP. Only a single setting MSTP (RSTP), PVST or RPVST can be enabled on a switch.

Enabling PVSTP or rapid PVSTP (PVRSTP) disables MSTP/RSTP/STP. By default, MSTP is enabled.

No command globally configures the switch to the default spanning-tree mode, MSTP.

spanning-tree mode {mst | pvst | rapid-pvst | stp | rstp}

no spanning-tree mode

Parameters

mst	Configure spanning-tree mode as mst.
pvst	Configure spanning-tree mode as pvst.
rapid-pvst	Configure spanning-tree mode as rapid-pvst.
stp	Configure spanning-tree mode as pst.
rstp	Configure spanning-tree mode as rstp.

Default

The default is MST.

Command Mode

Global Config

5-220 spanning-tree mst

Set Path Cost or Port Priority for ports within the multiple or common and internal spanning tree instances. Specify an *mstid* parameter which corresponds to an existing multiple spanning tree instance, the corresponding settings are done for that multiple spanning tree instance. Specify 0 (defined as the default) as the mstid, the configurations are done for the common and internal spanning tree instance.

By specifying a cost for the path cost for the port is set within a multiple spanning tree instance or the common and internal spanning tree instance--dependent on the mstid parameter. The path cost range: 1 to 200000000 or **auto**. The **auto option defines** the path cost value based on Link Speed.

spanning-tree mst *mstid* **{cost** *1-200000000* **| auto} | port-priority** *0-240***}**

no spanning-tree mst mstid {cost | port-priority}

Parameters

mstid	Indicates a multiple spanning tree instance identifier.
cost *1-200000000*	Indicates the path cost range: 1 – 2000000000.
auto	Indicates the path cost value based on Link Speed.
port-priority *0-240*	Indicates the priority for the identified port interface.

Default

The default is as follows:

- cost – auto
- port-priority – 128

Command Mode

Global Config

5-221 spanning-tree mst instance

Add multiple spanning tree instances to the switch, *mstid* range: 1 to 4094. The range corresponds to the instance ID to be added. The maximum number of supported multiple instances is 4.

No command removes a multiple spanning tree instance and reallocates all VLANs corresponding instances to the common and internal spanning tree.

spanning-tree mst instance *mstid*

no spanning-tree mst instance *mstid*

Parameters

mstid	Enter a multiple spanning tree instance identifier.

Default

The default is None.

Command Mode

Global Config

5-222 spanning-tree mst priority

Sets the bridge priority for specific multiple spanning tree instances. The *mstid* parameter corresponds to the desired existing multiple spanning tree instances. The priority value range: 0 to 61440 in increments of 4096.

Specify 0 (default CIST ID) as the mstid to set the Bridge Priority parameter to a value for the common and internal spanning tree. The bridge priority range: 0 to 61440.

Note: The twelve least significant bits are masked, specified by 802.1s affecting the priority, which is rounded down to the next lower valid priority.

No command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance.

spanning-tree mst priority *mstid 0-61440*

no spanning-tree mst priority *mstid 0-61440*

Parameters

mstid	Enter a multiple spanning tree instance identifier (0 - 61440).

Default

The default is 32768.

Command Mode

Global Config

5-223 spanning-tree mst vlan

Adds an association between a multiple spanning tree instance and one or more VLANs disassociating the VLAN(s) from the common and internal spanning tree. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance.

No command disassociates a multiple spanning tree instance and one or more VLANs. In so doing, the VLAN(s) revert to the common and internal spanning tree association.

spanning-tree mst vlan *mstid vlanid*

no spanning-tree mst vlan *mstid vlanid*

Parameters

mstid	Enter a multiple spanning tree instance identifier.
vlanid	Enter VLAN IDs in range <1-4093>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Default

The default is None.

Command Mode

Global Config

5-224 spanning-tree port mode

Enable the Administrative Switch Port State for a port.

No command to set the Administrative Switch Port State for this port to disabled.

spanning-tree port mode

no spanning-tree port mode

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

5-225 spanning-tree port mode all

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

Use the **no** command to set the Administrative Switch Port State for all ports to disabled.

spanning-tree port mode all

no spanning-tree port mode all

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

5-226 spanning-tree transmit

Sets the Bridge Transmit Hold Count parameter, range: 1-10.

spanning-tree transmit *hold-count*

Parameters

hold-count	The Bridge Tx hold-count parameter, value 1 to 10.

Default

The default is 6.

Command Mode

Global Config

5-227 spanning-tree uplinkfast

Configures the rate at which gratuitous frames are sent (in packets per second) after switchover to an alternate PVSTP port and enables uplinkfast. The range is 0-32000 (default is 150). This command accelerates spanning-tree convergence after switchover to an alternate port.

Configur Uplinkfast even if the switch is configured for MST(RSTP) mode, only in PVST mode. Enabling FastUplink increases the priority by 3000. Path costing less than 3000 have an additional 3000 added when uplinkfast is enabled.

PVRSTP embeds support for backbonefast and uplinkfast, provisioning to enable or disable these features is not available.

No command disables uplinkfast on PVSTP configured switches. All switch priorities and path costs not modified from default values are set to default.

spanning-tree uplinkfast [max-update-rate *packets***]**

no spanning-tree uplinkfast [max-update-rate]

Parameters

max-update-rate	(Optional) Configure spanning tree directlink rapid convergence maximum update rate.
packets	(Optional) Indicates the rate.

Default

The default is 150.

Command Mode

Global Config

5-228 spanning-tree vlan

Enable/disable spanning tree on a VLAN.

spanning-tree vlan *vlan-list*

Parameters

vlan-list	The VLANs to which to apply this command.

Default

The default is None.

Command Mode

Global Config

5-229 spanning-tree vlan cost

Sets the path cost for a VLAN port. Values range: 1 to 200000000 or auto. If auto is selected, the path value is based on the link speed.

spanning-tree vlan *vlan-id* **cost {auto |** *1-200000000***}**

Parameters

vlan-id	Enter an integer in the range of 1 - 200000000.
auto	Set the pathcost value automatically on the basis of Link Speed.

Default

The default is None.

Command Mode

Interface Config

5-230 spanning-tree vlan forward-time

Configures the spanning tree forwarding delay time for a VLAN or a set of VLANs, default is 15 seconds.

Set value to a lower number to accelerate transition to forwarding.

Note: Consider 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.

spanning-tree vlan *vlan-list* **forward-time** *4-30*

Parameters

vlan-list	Enter the VLANs to apply.
forward-time *4-30*	Forward delay time for the spanning tree, range 4-30 seconds.

Default

The default is 15.

Command Mode

Global Config

5-231 spanning-tree vlan hello-time

Configure hello time (spanning-tree) for a specified or range of VLANs. The default is 2 seconds. Set this value to a lower number to accelerate the discovery of topology changes.

spanning-tree vlan *vlan-list* **hello-time** *1-10*

Parameters

vlan-list	ApplicableVLANs.
hello-time *1-10*	Forward hello time for spanning tree. The range is 1-10 seconds.

Default

The default is 2.

Command Mode

Global Config

5-232 spanning-tree vlan max-age

Configure the spanning tree maximum age time. The default is 20 seconds.

To accelerate the discovery of topology changes lower the value.

Note: Consider the end-to-end BPDU propagation delay and message age overestimate for the specific topology when configuring this value.

Default settings: 20 for a network of diameter 7; lost message value 3; transit delay 1; hello interval 2 seconds; overestimate per bridge 1 second; and BPDU delay 1 second. For a network of diameter 4, a setting of 16 seconds is appropriate if all other timers remain at their default values.

spanning-tree vlan *vlan-list* **max-age** *6-40*

Parameters

vlan-list	Applicable VLANs.
max-age *6-40*	Time for spanning tree forwarding hello time. The range is 1-10 seconds.

Default

The default is 20.

Command Mode

Global Config

5-233 spanning-tree vlan port-priority

Change VLAN port priority value of the VLAN port. Allows the selection of the relative importance of the VLAN port in the forwarding selection process when port is configured as point-to-point link. Set this value to a lower number to prefer a port for forwarding of frames.

spanning-tree vlan *vlan-list* **port-priority** *priority*

Parameters

vlan-id	The VLANs to which to apply this command.
priority	The VLAN port priority, range 0-240.

Default

The default is None.

Command Mode

Interface Config

5-234 spanning-tree vlan priority

Configure the bridge priority of a VLAN. The default value is 32768.

Configured values not among specified values are rounded off to the nearest valid value.

spanning-tree vlan *vlan-list* **priority** *priority*

Parameters

vlan-list	Applicable VLANs.
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.

Default

The default is 32768.

Command Mode

Global Config

5-235 spanning-tree vlan root

Modify the bridge priority from the default value of 32768 to a lower value as calculated to ensure the bridge is the root (or standby) and configure it to become the root bridge or standby root bridge.

spanning-tree vlan *vlan-list* **root {primary | secondary}**

Parameters

vlan-list	The VLANs to which to apply this command.
primary	Configure VLAN as primary.
secondary	Configure VLAN as secondary.

Default

The default is 32768.

Command Mode

Global Config

5-236 show spanning-tree

Displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

show spanning-tree

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show spanning-tree

Bridge Priority.................................. 32768
Bridge Identifier................................ 80:00:00:05:64:2F:0F:81
Time Since Topology Change....................... 4 day 4 hr 38 min 39 sec
```

```
Topology Change Count..... 0
Topology Change in progress..... False
Designated Root..... 80:00:00:05:64:2F:0F:81
Root Path Cost..... 0
Root Port Identifier..... 00:00
Bridge Max Age..... 20
Bridge Max Hops..... 20
Bridge Tx Hold Count..... 6
Bridge Forwarding Delay..... 15
Hello Time..... 2
Bridge Hold Time..... 6
CST Regional Root..... 80:00:00:05:64:2F:0F:81
Regional Root Path Cost..... 0

Associated FIDs      Associated VLANs
---------------      ----------------
1                    1
2                    2
3                    3
4                    4
5                    5
```

Display Parameters

Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). Value range: 0 and 61440, displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST, based on bridge priority and the base MAC address.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change	Boolean value of the Topology Change parameter. indicative of a topology change in progress on any port assigned to the common and internal spanning tree.
Designated Root	Root bridge bridge identifier, comprised of bridge's priority and base MAC address.
Root Path Cost	Root Path Cost parameter value for the common and internal spanning tree.
Root Port Identifier	Port identifier to access the Designated Root for the CST.
Root Port Max Age	Derived value.
Root Port Bridge Forward Delay	Derived value.
Hello Time	CST configured parameter value.
Bridge Hold Time	The Configuration Bridge Protocol Data Units (BPDUs) minimum time between transmission.
Bridge Max Hops	Bridge max-hops count for the device.

CST Regional Root	Bridge Identifier of the CST Regional Root, comprised of the bridge's priority and 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.

5-237 show spanning-tree active

Display the spanning tree values on active ports for the modes (xSTP and PV(R) STP).

show spanning-tree active

Parameters

None

Default

The default is None.

Command 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   Status       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 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

Name   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

Name   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 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

Name   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

Name   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
```

5-238 show spanning-tree backbonefast

Display spanning tree information for backbonefast.

show spanning-tree backbonefast

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an output example.

```
(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
```

Display Parameters

Transitions via Backbonefast	Backbonefast transition value.
Inferior BPDUs received (all VLANs)	Inferior BPDUs value received on all VLANs.
RLQ request PDUs received (all VLANs)	Root link query (RLQ) request value PDUs received on all VLANs.
RLQ response PDUs received (all VLANs)	RLQ response PDUs received values on all VLANs.
RLQ request PDUs sent (all VLANs)	RLQ request PDUs sent values on all VLANs.
RLQ response PDUs sent (all VLANs)	RLQ response PDUs sent values on all VLANs.

5-239 show spanning-tree brief

Display spanning tree settings for the bridge.

show spanning-tree brief

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a command example.

```
(Routing)# show spanning-tree brief

Bridge Priority.................................. 32768
Bridge Identifier................................ 80:00:00:05:64:2F:0D:E5
Bridge Max Age................................... 20
Bridge Max Hops.................................. 20
Bridge Hello Time................................ 2
Bridge Forward Delay............................. 15
Bridge Hold Time................................. 6
```

Display Parameters

Bridge Priority	Displays the specified bridge priority for both Common and Internal Spanning Tree (CST). Displayed in multiples of 4096, the value range is from 0 to 61440. It is displayed in multiples of 4096.
Bridge Identifier	Bridge identifier for the selected MST instance, composed of the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Displays the specified bridge max age for CST. The value is defined in seconds ranging from 6 to 40, less than or equal to 2 x (Bridge Forward Delay -1).
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Displays the bridge hello timer value between each bridge protocol data unit through a port. The value is defined as 2 seconds by default with a range between 1 and 10 seconds forward delay.
Bridge Forward Delay	Displays the specified bridge forward delay parameter for CST. The value is defined in seconds ranging from 4 to 30.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

5-240 show spanning-tree interface

Display the settings and parameters for a specific switch port within the common and internal spanning tree. The **{***slot/port* **| lag** *lag-id***}** is the displayed switch port or LAG. The following details are displayed:

show spanning-tree interface {*slot/port* **| lag** *lag-id***}**

Parameters

slot/port	Enter an interface in slot/port format.
lag *lag-id*	Enter into interface lag mode.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Hello Time	Port admin hello time.
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 propagation of received change notifications to topology and other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.
Auto Edge	To enable or disable auto edge feature: ports without an edge delay time BPDU transforming to a 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.

5-241 show spanning-tree mst detailed

The command displays the detailed settings for an MST instance.

show spanning-tree mst detailed *mstid*

Parameters

mstid	A multiple spanning tree instance identifier. The value is 0-4094.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show spanning-tree mst detailed 1

MST Instance ID.............................. 1
MST Bridge Priority.......................... 32768
MST Bridge Identifier........................ 80:01:00:05:64:2F:0F:81
Time Since Topology Change................... 4 day 4 hr 40 min 27 sec
Topology Change Count........................ 0
Topology Change in progress.................. False
Designated Root.............................. 80:01:00:05:64:2F:0F:81
Root Path Cost............................... 0
Root Port Identifier......................... 00:00

Associated FIDs   Associated VLANs
---------------   ----------------
10                10
```

5-242 show spanning-tree mst port detailed

Displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The **{***slot/port* **| lag** *lag-id***}** is the desired switch port or LAG.

show spanning-tree mst port detailed *mstid* **{***slot/port* **| lag** *lag-id***}**

Parameters

mstid	Enter a multiple spanning tree instance identifier.
slot/port	Enter an interface in slot/port format.
lag *lag-id*	Enter into interface lag mode.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

MST Instance ID	Existing MST instance ID.
Port Identifier	Port identifier for the specified port (selected MST instance), comprised of port priority and the interface number of the port.
Port Priority	Port priority within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Port role values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
Auto-Calculate Port Path Cost	Indicates if auto calculation is enabled.
Port Path Cost	Displays the path cost of the specified port. The value range is between 1 and 65535. The path cost is typically defined as 1000 ÷ /LAN speed in megabits per second.
Designated Root	Designated root identifier for the port.
Root Path Cost	The path cost to reach root bridge. The root path cost is zero if bridge is the root instance.
Designated Bridge	Designated Port bridge identifier.
Designated Port Identifier	Port on the Designated Bridge offering lowest LAN cost.
Loop Inconsistent State	If loop is in inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state places the port in a blocking state until subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times transitioned into a loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times transitioned out of loop inconsistent state.

If 0 (defined as the default CIST ID) is specified as the *mstid*, the command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The following display:.

Port Identifier	Port identifier within the CST.
Port Priority	Priority within the CST.
Port Forwarding State	Forwarding state within the CST.
Port Role	Role of the specified interface within the CST.
Auto-Calculate Port Path Cost	Indicates if auto calculation is enabled or not (disabled).
Port Path Cost	Configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.

External Port Path Cost	Cost across boundary region to reach to the root bridge of the CIST.
Designated Root	Identifier of the designated root within the CST.
Root Path Cost	Root path cost to reach the LAN.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port offering lowest cost to LAN on the Designated Bridge.
Topology Change Acknowledgement	If a topology change is in progress, this represents the value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission.
Hello Time	The designated hello time.
Edge Port	The value identifying an edge port.
Edge Port Status	Derived value of the edge port status. True if an edge port, false otherwise.
Point To Point MAC Status	Derived value indentifying a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	Internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop state. While loop guard is enabled, the port fails to receive BPDUs. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times transitioned into a loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

5-243 show spanning-tree mst port summary

Display the settings of one or all ports within the multiple spanning tree instance. The parameter *mstid* displays the particular MST instance. The parameter **{***slot/port* **| lag** *lag-id* **| all}** indicates the switch port, LAG, or all ports.

A 0 (defined as the default CIST ID) value for *mstid*, the status summary is displayed for one or all ports.

show spanning-tree mst port summary *mstid* **{***slot/port* **| active | lag** *lag-id* **| all)**

Parameters

mstid	Enter a multiple spanning tree instance identifier.
slot/port	Enter an interface in slot/port format.
active	Enter active to select all active interfaces.
lag *lag-id*	Enter into interface lag mode.
all	Enter all for all interfaces.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

MST Instance ID	The associated MST instance.
Interface	Enter an interface in slot/port format.
STP Mode	Indicates if spanning tree is enabled or disabled.
Type	Not in use.
STP State	The designated forwarding state of the port.
Port Role	The specified role of the port.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

5-244 show spanning-tree mst port summary active

Display active link settings for the ports within the specified multiple spanning tree instance.

show spanning-tree mst port summary *mstid* **active**

Parameters

mstid	Enter a multiple spanning tree instance identifier.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show spanning-tree mst port summary 1 active

Interface    STP         Type    STP         Port
             Mode                State       Role                  Desc
----------   ----------  -----   ----------  --------------------  ----------
0/1          Enabled             Mirror      Manual forwarding     Disabled
```

```
0/2          Enabled                        Manual forwarding      Disabled
```

Display Parameters

MST Instance ID	MST instance ID.
Interface	*slot/port*
Interface	Indicates spanning tree status: enabled or disabled on the port.
Type	Not in use.
STP State	The forwarding state of the port within the specified spanning tree instance.
Port Role	Role status of the specified port within the spanning tree.
Desc	Indicates the port status, loop inconsistent state or not. This field is blank if the loop guard feature is not available.

5-245 show spanning-tree mst summary

Displays summary information regarding all multiple spanning tree instances.

show spanning-tree mst summary

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show spanning-tree mst summary

MST Instance ID.............................. 1

Associated FIDs    Associated VLANs
---------------    ----------------
10                 10

MST Instance ID.............................. 2
```

```
Associated FIDs   Associated VLANs
---------------   ----------------
20                20

MST Instance ID.................................. 3

Associated FIDs   Associated VLANs
---------------   ----------------
30                30
```

Display Parameters

MST Instance ID List	List of current multiple spanning trees IDs.
For each MSTID:	• Associated FIDs: Forwarding database identifiers associated with this instance. • Associated VLANs: VLAN IDs associated with this instance.

5-246 show spanning-tree summary

Display spanning tree settings and parameters.

show spanning-tree summary

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing) #show spanning-tree summary

Spanning Tree Admin Mode....................... Disabled
Spanning Tree Version.......................... IEEE 802.1w
BPDU Guard Mode................................ Disabled
BPDU Filter Mode............................... Disabled
Configuration Name............................. DLINK
Configuration Revision Level................... 1
Configuration Digest Key....................... 0xaa07b4589430317683e50b5c456a0c69
```

```
Configuration Format Selector..................... 0
MST Instances..................................... 1,2,3
```

Display Parameters

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.

5-247 show spanning-tree uplinkfast

Display spanning tree information to uplinkfast.

show spanning-tree uplinkfast

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an output example.

```
(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
```

Display Parameters

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.

5-248 show spanning-tree vlan

Displays spanning tree information per VLAN and list the port roles, states and port cost. The *vlan-list* parameter is a list of VLANs or VLAN-ranges separated by commas and with no embedded blank spaces, ranging form “X-Y” where X and Y are valid VLAN identifiers and X<Y. The *vlanid* corresponds to an existing VLAN ID.

show spanning-tree vlan {*vlanid* **|** *vlan-list***}**

Parameters

vlanid	Enter a VLAN identifier.
vlan-list	Enter VLAN IDs in range <1-4093>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example.

```
(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           Status         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 includes VLAN configuration settings information.

5-249 vlan database

Configure VLAN settings through the VLAN Config mode.

vlan database

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-250 network mgmt_vlan

Configure the Management VLAN ID.

No command sets the Management VLAN ID to the default.

network mgmt_vlan *1-4093*

no network mgmt_vlan *1-4093*

Parameters

None

Default

The default is 1.

Command Mode

Privileged EXEC

5-251 vlan

Create a VLAN and assign an ID-- a valid VLAN identification number, range: 1-4093 (default: 1).

No command deletes existing VLAN identiers.

vlan *1-4093*

no vlan *1-4093*

Parameters

None

Default

The default is None.

Command Mode

VLAN Config

5-252 vlan acceptframe

Sets the frame acceptance mode on a single or range of interfaces. For VLAN Only mode, all received untagged frames or priority frames are discarded. For Admit All mode, all received untagged frames or priority frames the interface are accepted and assigned the value of the interface VLAN ID for the port. For admituntaggedonly mode, only untagged frames are accepted on the interface, while tagged frames are discarded.

No command resets the frame acceptance mode for the interface or range of interfaces to the default value.

vlan acceptframe {admituntaggedonly |vlanonly | all}

no vlan acceptframe

Parameters

admituntaggedonly	Set only untagged frames.
vlanonly	Admit only tagged frames.
all	Admit all frame types.

Default

The default is All.

Command Mode

Interface Config

5-253 vlan ingressfilter

Enable ingress filtering on a single or range of interfaces. When ingress filtering is disabled, any frames received with VLAN IDs not matching VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

No command disables ingress filtering. When ingress filtering is disabled, any frames received with VLAN IDs not matching VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

vlan ingressfilter

no vlan ingressfilter

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-254 vlan internal allocation

Configure VLAN IDs for port-based routing interfaces.

vlan internal allocation {base *vlan-id* **| policy ascending | policy decending}**

Parameters

base *vlan-id*	VLAN ID assigned to a port-based routing interface.
policy ascending	Policy assignment follows an ascending scale..
policy decending	Policy assignment follows a descending scale.

Default

The default is None.

Command Mode

Global Config

5-255 vlan makestatic

Change dynamically created VLANs to a static VLAN. The ID is a valid VLAN identification number, range: 1-4093.

vlan makestatic *1-4093*

Parameters

None

Default

The default is None.

Command Mode

VLAN Config

5-256 vlan name

Change VLAN name variable, alphanumeric string of up to 32 characters; range: 1-4093.

No command sets VLAN value to a blank string.

vlan name *1-4093 name*

no vlan name *1-4093*

Parameters

name	Indicates the name variable.

Default

The default is as follows:

- VLAN ID 1 – default
- Other VLANS – blank string

Command Mode

Global Config

5-257 vlan participation

Configures the participation state for a specific or range of interfaces in a VLAN.

vlan participation {exclude | include | auto} *1-4093*

Parameters

exclude	Does not include entry as a member of this VLAN.
include	Include the interface as a member of this VLAN.
auto	Dynamic registration of entry in VLAN, participation is available upon a join request.

Default

The default is None.

Command Mode

Interface Config

5-258 vlan participation all

Configures the participation status for all interfaces in a VLAN.

vlan participation all {exclude | include | auto} *1-4093*

Parameters

exclude	Does not include entry as a member of this VLAN.
include	Include the interface as a member of this VLAN.
auto	Dynamic registration of entry in VLAN, participation is available upon a join request.

Default

The default is None.

Command Mode

Global Config

5-259 vlan port acceptframe all

Set the frame acceptance mode for all interfaces.

No command sets the frame acceptance mode for Admit All (global). In Admit All mode, received untagged frames or priority frames on the interface are accepted and assigned the interface VLAN ID value for the port.

vlan port acceptframe all {admituntaggedonly | vlanonly | all}

no vlan port acceptframe all

Parameters

admituntaggedonly	Select to admit only untagged frames.
all	Select to admit all frame types.
vlanonly	Select to admit only tagged frames.

Default

The default is All.

Command Mode

Global Config

5-260 vlan port ingressfilter all

Enable ingress filtering for all ports. Disable ingress filtering to admit and forward frames not matching the VLAN membership of the received interface to member ports of the VLAN.

No command disables ingress filtering for all ports.

Disable ingress filtering to admit and forward frames not matching the VLAN membership of the received interface to member ports of the VLAN.

vlan port ingressfilter all

no vlan port ingressfilter all

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-261 vlan port pvid all

Change VLAN ID for all interface.

No command sets the VLAN ID for all interfaces to 1.

vlan port pvid all *1-4093*

no vlan port pvid all

Parameters

None

Default

The default is 1.

Command Mode

Global Config

5-262 vlan port tagging all

Enablee tagging behavior for all interfaces in a VLAN allowing the transmission of traffic as tagged frames. Disable tagging to transmit as untagged frames.

No command disables the tagging behavior for all interfaces in a VLAN.

vlan port tagging all *1-4093*

no vlan port tagging all

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-263 vlan pvid

Change the VLAN ID on a single or range of interfaces.

No command sets the VLAN ID on a single or range of interfaces to 1.

vlan pvid *1-4093*

no vlan pvid

Parameters

None

Default

The default is 1.

Command Mode

- Interface Config
- Interface Range Config

5-264 vlan tagging

Enable the tagging behavior for a specific interface or range of interfaces in a VLAN allowing the transmission of traffic as tagged frames. Disable tagging to transmit as untagged frames.

No command disables the tagging behavior for all interfaces in a VLAN.

vlan tagging *1-4093*

no vlan tagging *1-4093*

Parameters

None

Default

The default is None.

Command Mode

Interface Config

5-265 show vlan

Display configured private VLANs [including primary and secondary VLAN IDs, type (community, isolated, or primary) information] including ports which belong to a private VLAN.

show vlan {*vlanid* **| brief | internal | port [***slot/port* **| all]| private-vlan [***type***] remote span}**

Parameters

vlanid	Enter a VLAN ID.
brief	Display switch VLANs.
internal	Show VLANs assigned to port-based routing interfaces
port *slot/port*	Display 802.1Q port parameters.
all	Display all interfaces.
private-vlan	Display private VLAN configuration.
remote-span	Display RSPAN VLAN

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Primary	Primary identifier, range: 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	VLAN identifier (VID) associated with each VLAN: range 1 to 4093.
VLAN Name	String value given to identify VLAN, supports 32 alphanumeric characters long, including blanks (default is blank). VLAN ID 1 is named as the Default. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1), static, or Dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) when a RADIUS-assigned VLAN does not exist on the switch.
Interface	The associated physical port or LAG interface.
Current	Participation status: • **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	Participation status of a port in this VLAN, values include: • **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 defined tagging behavior. • **Tagged** – Transmit traffic for this VLAN as tagged frames. • **Untagged** – Transmit traffic for this VLAN as untagged frames.

5-266 show vlan internal usage

Display information about the VLAN ID allocation on the switch.

show vlan internal usage

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show vlan internal usage

Base VLAN ID:        4093
Allocation policy:   Descending
```

Display Parameters

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.

5-267 show vlan brief

Display a list of all configured VLANs.

show vlan brief

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show vlan brief

VLAN ID    VLAN Name     VLAN Type
-------    ----------    ---------------
1          default       Default
2          VLAN0002      Static
3          VLAN0003      Static
4          VLAN0004      Static
5          VLAN0005      Static
6          VLAN0006      Static
7          VLAN0007      Static
8          VLAN0008      Static
```

Display Parameters

VLAN ID	VLAN Identifier (vlanid) associated for each VLAN, range: S1-4093.
VLAN Name	String value given to identify VLAN, supports 32 alphanumeric characters long, including blanks (default is blank). VLAN ID 1 is named as the Default. This field is optional.

VLAN Type	Type of VLAN (default, VLAN ID = 1) static.

5-268 show vlan port

Displays VLAN port information.

show vlan port {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter 'all' for all interfaces.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing) #show vlan port all

Interface   Port        Port      Acceptable   Ingress      Ingress
            VLAN ID     VLAN ID   Frame Types  Filtering    Filtering    Default
            Configured  Current               Configured   Current      Priority
---------   ----------  --------- ----------   ----------   ----------   ----------
0/1         1           1         Admit All    Enable       Enable       0
0/2         5           5         Admit All    Enable       Enable       0
0/3         1           1         Admit All    Disable      Disable      0
0/4         1           1         Admit All    Disable      Disable      0
0/5         1           0         Admit All    Enable       Disable      0
0/6         1           0         Admit All    Enable       Disable      0
```

Display Parameters

Interface	Set the parameters for all slot/port.
Port VLAN ID Configured	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port, value for established (default: 1).
Port VLAN ID Current	Assigned VLAN ID to received untagged frames or priority tagged frames. The factory default is 1.

Acceptable Frame Types	Supported frame types, ‘VLAN only‘ and ‘Admit All‘. ‘VLAN only‘ discards received untagged or priority tagged frames. ‘Admit All‘ accepts received untagged or priority tagged frames and assigns a port VLAN ID.
Ingress Filtering Configured	Options: enable or disable. Enable to discard a frame if port is not a member of the associated VLAND is able to forward frames according to 802.1Q VLAN bridge specification (default: disabled).
Ingress Filtering Current	Displays the current ingress filtering configuration.
GVRP	Option: enable or disable.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.
Protected Port	False status indicates a non-protected port. True status indicates a protected port.
Switchport mode	The current switchport mode.
Operating parameters	The operating parameters: VLAN, name, egress rule, and type.
Static configuration	The static configuration: VLAN, name, and egress rule.
Forbidden VLANs	The forbidden VLAN configuration: VLAN and name.

Switch Ports

This section describes switch port mode settings.

5-269 switchport mode

Configure the switch port mode: access, trunk or general.

In Trunk mode, the port is configured as a member of all VLANs on switch unless specified in the allowed list in the **switchport trunk allowed vlan**. The PVID of the port is set to the Native VLAN as specified in the **switchport trunk native vlan**. Tagged packets received with a VLAN ID from non-member ports are discarded and MAC learning is not initiated.

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, while filtering is enabled.

In General mode, custom configuration of VLAN membership, PVID, tagging, ingress filtering is available. **No** command resets the switch port mode to default.

switchport mode {access | trunk | general | {private-vlan *host/promiscuous***}}**

no switchport mode {access | trunk | general | {private-vlan *host/promiscuous***}}**

Parameters

access	Untagged Layer 2 VLAN Interface.
trunk	Trunking Layer 2 VLAN interface.

general	Full 802.1q support VLAN Interface.
private-vlan	Set switchport mode as host or promiscuous port for the private VLAN.

Default

The default is General mode.

Command Mode

Interface Config

5-270 switchport trunk allowed vlan

Configure the allowed VLAN list configured to receive and send traffic in tagged format (trunking mode). The default is all.

VLANs lists can be modified through the add or remove options or replaced with another list using the vlan-list, all, or except options. Selecting all sets VLANs to the list of allowed VLAN. The except option provides an exclusion list.

Use the **no** command to reset the list of allowed VLANs on the trunk port to its default value.

switchport trunk allowed vlan {*vlan-list* **| all | {add** *vlan-list***} | {remove** *vlan-list***} | {except** *vlan-list***}}**

no switchport trunk allowed vlan

Parameters

vlan-list	Values: 1 to 4093, range is entered using two values separated by a hyphen. The lower value is entered first.
all	Specifies all VLANs from 1 to 4093. This option is not supported on commands that do not permit all VLANs in the list to be set at the same time.
add	Add VLANs to the current list.
remove	Removes VLANs from the current list.
except	Create an exception entry to the VLAN list.

Default

The default is All.

Command Mode

Interface Config

5-271 switchport trunk native vlan

Configure the Trunk port Native VLAN (PVID) parameter. Untagged ingress packets on the port are assigned a Native VLAN tag--native VLAN must be configured in the allowed VLAN list for tagging of received untagged packets. Otherwise, they are untagged packets are discarded. The default is 1.

No command resets the switch port trunk mode native VLAN to default.

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

Parameters

vlan-id	Enter VLAN ID.

Default

The default is VLAN.

Command Mode

Interface Config

5-272 switchport access vlan

Configure Access port VLAN, only a single can be assigned to the Access port. By default access ports are members of VLAN 1. Access ports may be assigned to a VLAN other than VLAN 1.

No command resets the switch port access mode VLAN to default.

switchport access vlan *vlan-id*

no switchport access vlan

Parameters

vlan-id	Enter VLAN ID.

Default

The default is 1.

Command Mode

Interface Config

5-273 show interfaces switchport

Display the switchport status for a single or all interfaces.

show interfaces switchport *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#show interfaces switchport 0/1

Port: 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: 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
```

5-274 show interfaces switchport

Display the Switch port configuration for a selected interface mode. All interfaces are displayed if there is not specific selection.

show interfaces switchport {access | err-disabled | trunk | general} [*slot/port***]**

Parameters

access	Display the switchport information for interfaces configured in access mode.
err-disabled	Display the error disable status of interfaces.
general	Display the switchport information for interfaces configured in general mode.
Trunk	Display the switchport information for interfaces configured in trunk mode.
slot/port	(Optional) Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Switching)#show interfaces switchport access 0/1

Intf    PVID
-----   -----
0/1          1
```

```
(Switching)#show interfaces switchport trunk 0/6

Intf    PVID       Allowed Vlans List
-----   -----      --------------------
0/6     1          All
```

```
(Switching)#show interfaces switchport general 0/5

Intf    PVID  Ingress      Acceptable   Untagged   Tagged     Forbidden  Dynamic
              Filtering    Frame Type   Vlans      Vlans      Vlans      Vlans
-----   --------------    ----------   --------   --------   --------   --------
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
-----   ----- ---------    ----------   --------   --------   ---------  --------
0/1     1     Enabled      Admit All    1,4-7      30-40,55   3,100-200  88,96
0/2     1     Disabled     Admit All    1          30-40,55   none       none
```

Double VLAN Commands

This section describes double VLAN (DVLAN) configuration. Double VLAN tagging uses a Metro Core to allow VLAN traffic from one customer domain to another.

5-275 dvlan-tunnel ethertype (Interface Config)

Configure the Ethertype for a specified interface. A two-byte hex ethertype is used to define the first 16 bits of the DVLAN tag. The Ethertype supports the following values **802.1Q**, **vman**, or **custom**. If the Ethertype with custom value must be set to a value range of 1 to 65535.

No command disassociates globally defined TPID(s) to its relevant interface.

dvlan-tunnel ethertype {802.1Q | vman | custom *1-65535***}**

no dvlan-tunnel ethertype {802.1Q | vman | custom *1-65535***}**

Parameters

802.1Q	Configure the Ethertype as 0x8100.
vman	Commonly used value: 0x88A8.
custom *1-65535*	Custom value range: 1 to 65535.

Default

The default is VMAN.

Command Mode

Interface Config

5-276 dvlan-tunnel ethertype primary-tpid

Create a TPID and associate it with the next available TPID register. A TPID registers slot must be available, otherwise the system returns an error to the user. The command **[default-tpid]** forces the TPID value as the default TPID at index 0.

No command resets the TPID register to 0. Initialization resets all TPID registers to default.

dvlan-tunnel ethertype {802.1Q | vman | custom *1-65535***} [primary-tpid]**

no dvlan-tunnel ethertype {802.1Q | vman | custom *1-65535***} [primary-tpid]**

Parameters

802.1Q	Configure the Ethertype as 0x8100.
vman	Commonly used value: 0x88A8.
custom *1-65535*	Custom tag value range: 1 to 65535.
primary-tpid	(Optional) Configure the TPID value to the default TPID at index 0

Default

The default is None.

Command Mode

Global Config

5-277 show dot1q-tunnel

Display all interfaces enabled for Double VLAN Tunneling. Any indicated optional parameters allow for the display of detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

show dot1q-tunnel [interface {*slot/port* **| all}]**

Parameters

interface	(Optional) Indicates the interface.
slot/port	(Optional) Indicates an interface in slot/port format.
all	(Optional) Enter all for all interfaces.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Interface	Represents the *slot/port* identifier.
Mode	Enabled or disable the mode, default: disabled.
EtherType	The first 16 bits of the DVLAN tunnel are defined by a 2-byte hexEtherType.

	Three different EtherType tags are available: 802.1Q, which represents the commonly used value of 0x8100; vMAN representing the commonly used value of 0x88A8; Custom representing a custom tunnel value with a range of 1 to 65535.

5-278 show dvlan-tunnel

Display all interfaces enabled for Double VLAN Tunneling.Any indicated optional parameters allow for the display of detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

show dvlan-tunnel [interface {*slot/port* **| all | lag}]**

Parameters

interface	(Optional) Indicates an interface.
slot/port	(Optional) Indicates an interface in slot/port format.
all	(Optional) Enter all for all interfaces.
lag	Enter into interface lag mode.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example.

```
(Routing)#show dvlan-tunnel

Primary TPID..................................... 0x8100
Secondary TPIDs Configured....................... 0x8100
Interfaces Enabled for DVLAN Tunneling........... None
```

```
(Routing)#show dvlan-tunnel interface 0/1

Interface     Mode          EtherType
----------    ----------    ----------
0/1           Disable       0x88a8
```

Display Parameters

Interface	Represents the *slot/port* identifier.

Mode	Enable or disable the mode, default: disabled.
EtherType	The first 16 bits of the DVLAN tunnel are defined by a 2-byte hexEtherType. Three different EtherType tags are available: 802.1Q, which represents the commonly used value of 0x8100; vMAN representing the commonly used value of 0x88A8; Custom representing a custom tunnel value with a range of 1 to 65535.

Provisioning (IEEE 802.1p) Commands

This section describes provisioning (IEEE 802.1p,) configuration for port prioritization.

5-279 vlan port priority all

Configure the port priority for untagged packets for all available ports; The priority range is 0-7.

vlan port priority all *priority*

Parameters

priority	Enter a priority value (0-7) for untagged frames received.

Default

The default is 0.

Command Mode

Global Config

5-280 vlan priority

Configures default 802.1p port priority assignments for untagged packets for a specified interface. Priority range is 0-7.

vlan priority *priority*

Parameters

priority	Enter a priority value (0-7) for untagged frames received.

Default

The default is 0.

Command Mode

Interface Config

Protected Ports Commands

This section describes protected port configuration. Protected ports are not designed to forward traffic to each other, even when configured on the same VLAN. However, forwarding to unprotected ports as long as the ports are in the same group. In as much, unprotected ports can forward traffic to both protected and unprotected ports. By default, ports are configured as unprotected.

5-281 switchport protected (Global Config)

Create a protected port group. The groupid parameter identifies the set of protected ports. Provide a name value pair to assign a name to the protected port group. Naming convention can use up to 32 alphanumeric characters, including blanks. The default is undefined.

Note: Port protection occurs within a devicve. Protected port configuration does not affect traffic between ports on two different switches. Traffic forwarding is not possible between two protected ports.

No command removes a protected port group.

switchport protected *groupid* **name** *name*

no switchport protected *groupid* **name** *name*

Parameters

groupid	Enter Group ID.
name ***name***	Enter a name up to 32 characters in length.

Default

The default is Unprotected.

Command Mode

Global Config

5-282 switchport protected (Interface Config)

Add an interface to a protected port group. Interfaces can only be configured as protected into a group.

Note: Port protection occurs within a devicve. Protected port configuration does not affect traffic between ports on two different switches. Traffic forwarding is not possible between two protected ports.

No command configures a port as unprotected.

switchport protected *groupid*

no switchport protected *groupid*

Parameters

groupid	Enter Group ID.

Default

The default is Unprotected.

Command Mode

Interface Config

5-283 show switchport protected

Display the status of all interfaces both protected and unprotected.

show switchport protected *groupid*

Parameters

groupid	Enter Group ID.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
 (Routing) #show switchport protected 0

Name.....................................
Member Ports :
```

Display Parameters

Group ID	Protected port group identifier.
Name	Given text string of group can be up to 32 alphanumeric characters including blank characters. The default is blank.

List of Physical Ports	List of configured ports as protected for the group identified with groupid. The field is blank if no port is configured as protected.

5-284 show interfaces switchport

Display the status of the interface (protected/unprotected) under the groupid.

show interfaces switchport *slot/port groupid*

Parameters

slot/port	Enter an interface in slot/port format.
groupid	Enter Group ID (0 – 2).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show interfaces switchport 0/1 0

Protected Port: False
```

Display Parameters

Name	Text string identifying group, value can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected	Indicates protected status (TRUE or FALSE). If a group is defined as a multiple groups then it displays TRUE.

Port-Based Network Access Control Commands

This section describes port-based network access control (IEEE 802.1X) configuration, which allows for network service control for authorized and authenticated devices.

5-285 aaa authentication dot1x default

Configure authentication for port-based access. Authentication function is available when an error has occurred.. Possible authentication methods include:

- ias. Internal authentication server database is used for authentication. This method can be used in conjunction with any one of the existing methods such as local, radius, etc.
- local. Local username database is used for authentication.
- none. No authentication applied.
- radius. RADIUS server is used for authentication.

aaa authentication dot1x default {[ias] | [method1 [method2 [method3]]]}

Parameters

ias	Select internal as the authentication method.
method #	(Optional) Indicates an alternative identification method: local, none, or radius.

Default

The default is None.

Command Mode

Global Config

Example

The following is an example of the command.

```
(Routing)#
(Routing)#configure
(Routing)(Config)#aaa authentication dot1x default ias none
(Routing)(Config)#aaa authentication dot1x default ias local radius none
```

5-286 clear dot1x statistics

Resets the 802.1X statistics for the specified or for all ports.

clear dot1x statistics {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter all to specify all ports.

Default

The default is None.

Command Mode

Privileged EXEC

5-287 clear dot1x authentication-history

Clear the authentication history table of successful and unsuccessful authentication events on all or specified interface.

clear dot1x authentication-history [*slot/port***]**

Parameters

slot/port	(Optional) Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

5-288 clear radius statistics

Clear all RADIUS statistics.

clear radius statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-289 dot1x eapolflood

Enable EAPOL flood support on the switch.

No command disables EAPOL flooding on the switch.

dot1x eapolflood

no dot1x eapolflood

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-290 dot1x dynamic-vlan enable

Enable the creation of VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

No command prevents from the creation of VLANs when a RADIUS-assigned VLAN does not exist in the switch.

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-291 dot1x port-control

Set the authentication mode for the specified interface or range of interfaces. The**Force-unauthorized** configures the authenticator PAE sets the controlled port to unauthorized. The **force-authorized** configures the authenticator PAE unconditionally sets the controlled port to authorized. While the **auto** parameter specify the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. lf a **mac-based** option is specified, the MAC-based dot1x authentication is enabled.

No command sets the 802.1X port control mode on the specified port to default.

dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}

no dot1x port-control

Parameters

force-unauthorized	Enter force-unauthorized to deny all access through the interface.
force-authorized	Enter force-authorized to disable authentication check.
auto	Enter auto - for default auto mode.
mac-based	Enter mac-based to enable MAC-based 802.1X authentication for this interface.

Default

The default is Auto.

Command Mode

Interface Config

5-292 dot1x port-control all

Set the authentication mode on all ports. The**Force-unauthorized** configures the authenticator PAE sets the controlled port to unauthorized. The **force-authorized** configures the authenticator PAE unconditionally sets the controlled port to authorized. While the **auto** parameter specify the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If **mac-based** option is specified, then MAC-based dot1x authentication is enabled on the port.

No command sets the authentication mode on all ports todefault.

dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}

no dot1x port-control all

Parameters

force-unauthorized	Enter force-unauthorized to deny all access through this interface.
force-authorized	Enter force-authorized to disable authentication check.
auto	Enter auto - for default auto mode.
mac-based	Enter mac-based to enable MAC-based 802.1X authentication for this interface.

Default

The default is Auto.

Command Mode

Global Config

5-293 dot1x system-auth-control

Enable the dot1x authentication support. While disabled, the dot1x configuration is retained and can be configured when disabled.

No command disables the dot1x authentication support.

dot1x system-auth-control

no dot1x system-auth-control

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-294 dot1x system-auth-control monitor

Enable the 802.1X monitor mode to help troubleshoot port-based authentication configuration issues--network access to connected hosts is not disrupted. While in Monitor mode, a host is granted network access to an 802.1X-enabled port even if authentication has failed.

No command disables 802.1X Monitor mode.

dot1x system-auth-control monitor

no dot1x system-auth-control monitor

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-295 dot1x user

Add specific users to the current list providing access to the specified port or all ports. The specified user must be a configured user.

No command removes the user from the list of users.

dot1x user user {*slot/port* **| all}**

no dot1x user user {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter all for access to all ports.

Default

The default is None.

Command Mode

Global Config

5-296 show authentication methods

Display the ordered authentication methods for all authentication login lists.

show authentication methods

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an authentication configuration example.

```
(Routing)#show authentication methods

Login Authentication Method Lists
-----------------------------------------
defaultList         :      local
networkList         :      local
```

```
Enable Authentication Method Lists
---------------------------------------
enableList          :      enable none
enableNetList       :      enable deny

Line          Login Method List          Enable Method List
--------      --------------------       --------------------
Console       defaultList                enableList
Telnet        networkList                enableNetList
SSH           networkList                enableNetList

DOT1X         :
```

Display Parameters

Authentication Login List	Listname of authentication list.
Method 1	First defined method in the specified authentication login list, if any.
Method 2	Second defined method in the specified authentication login list, if any.
Method 3	Third defined method in the specified authentication login list, if any.

5-297 show dot1x

Display a summary of the following: global dot1x configuration, the dot1x configuration for a single specified or all ports, the detailed dot1x configuration for a specified port, and the dot1x statistics for a specified port.

show dot1x [{summary {*slot/port* **| all} | detail** *slot/port* **| statistics** *slot/port***]**

Parameters

summary *slot/port*	(Optional) Display the configuration summary for the specified port or all ports.
authentication-history	Display the Dot1x authentication history log for the specified port or all ports.
detail *slot/port*	(Optional) Display the details of the configuration for the specified port.
clients	Display client information.
statistics *slot/port*	(Optional) Display the statistics for the specified port.
users	Display user information for locally configured users.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example for the command **show dot1x summary 0/1**.

```
(Routing)#show dot1x summary 0/1

Interface     Control Mode         Operating Control Mode     Port Status
----------    ---------------      ------------------------   -------------
0/1           auto                 auto                       Authorized
```

The following shows example CLI display output for the command.

```
(Routing)#show dot1x detail 0/1

Port.......................................... 0/1
Protocol Version.............................. 1
PAE Capabilities.............................. Supplicant
Control Mode.................................. auto
Supplicant PAE State.......................... Initialize
Supplicant Backend Authentication............. Initialize
Maximum Start trails.......................... 3
Start Period (secs)........................... 30
Held Period (secs)............................ 60
Authentication Period (secs).................. 30
EAP Method.................................... MD5-Challenge
```

Display Parameters

Global dot1x, VLAN Assignment, and Dynamic VLAN Creation mode are displayed if optional slot/port or vlanid parameters are defined.

Administrative Mode	Display enabled or disabled status.
VLAN Assignment Mode	Display enabled or disabled status for an authorized port to a RADIUS-assigned VLAN.
Dynamic VLAN Creation Mode	Indicates support for dynamic creation of RADIUS-assigned VLAN.
Monitor Mode	Displays Dot1x Monitor mode status: enabled or disabled.

By using the **summary** parameter **{***slot/port* **| all}**, the dot1x configuration for the specified port or all ports is displayed.

Interface	The displayed interface.
Control Mode	Configured control mode, values: force-unauthorized, force-authorized, auto, mac-based, authorized, and unauthorized.
Operating Control Mode	Displays operating control mode, values: authorized or unauthorized.

Reauthentication Enabled	Indicates reauthentication status: enabled.
Port Status	Indicates authorized or unauthorized status, values: authorized or unauthorized.

The optional parameter 'detail slot/port‘ provides detailed dot1x configuration for the specified port.

Port	The identified interface.
Protocol Version	The associated protocol version. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The associated port access entity (PAE) functionality, values: Authenticator or Supplicant.
Control Mode	The configured control mode for this port, values: force-unauthorized, force-authorized, auto, or mac-based.
Authenticator PAE State	Current state of the authenticator PAE function, possible values include: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. Enabling MAC-based authentication disapproves the parameter on the port.
Backend Authentication State	Current state of the backend authentication state machine, values include: Request, Response, Success, Fail, Timeout, Idle, and Initialize. Enabling MAC-based authentication disapproves the parameter.
Quiet Period	The defined period of time without a supplicant query. The value is expressed in seconds and will be in the range 0 and 65535.
Transmit Period	The defined period of time to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier.
Guest VLAN Peflod	The defined period of time in seconds to authorize and place the port in the Guest VLAN if EAPOL packets are not detected on that port.
Supplicant Timeout	The defined period of time before timing out the supplicant. The value is expressed in seconds, range: 1to 65535.
Server Timeout	The defined period of time to timeout the authentication server. The value is expressed in seconds, range: 1 to 65535.
Maximum Requests	The defined maximum number of times an EAPOL EAP Request/Identity is submitted before timing out the supplicant. The value range: 1 to 10.
Configured MAB mode	The dot1x MAC Authentication bypass configuration status.
Operational MAB mode	The dot1x MAC Authentication bypass operational status.
VLAN ID	The VLAN assigned to the port by the RADIUS server if port control mode is not MAC-based.
VLAN Assigned Reason	Identified reason the VLAN is assigned to the port. Possible values include: RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. If a VLAN Assigned Reason is not available, the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The defined period of time to determine when reauthentication of the

	supplicant takes place. The value is expressed in seconds, range: 1 to 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are “True” or “False”.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values: both, in.
Maximum Users	The maximum number of clients that can obtain authentication. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates if VLAN configuration is authenticated. This value is valid only when the port control mode is not MAC-based.
Session Timeout	Indicates the valid period of time for the given session. The time period in seconds is returned by the RADIUS server once authenticated. This value is valid only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the proceeding action once the session times out. Possible values: Default, Radius-Request. This value is valid only when the port control mode is not MAC-based.

For each client authenticated on the port, the **show dot1x detail** *slot/port* command displays the following MAC-based dot1x parameters (port-control mode must be MAC-based).

Supplicant MAC-Address	MAC-address of the supplicant.
Authenticator PAE State	Current state. Possible values: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend. Possible values: Request, Response, Success, Fail, Timeout, Idle, and Initialize.
VLAN-Assigned	The VLAN assigned by the RADIUS server to the client.
Logical Port	The logical port number associated with the client.

The optional parameter **statistics** *slot/port* provides the following dot1x statistics for a specified port.

Port	The specified interface.
EAPOL Frames Received	The number of valid received EAPOL frames of any type.
EAPOL Frames Transmitted	The number of transmitted EAPOL frames of any type.
EAPOL Start Frames Received	The number of received EAPOL start frames.
EAPOL Logoff Frames Received	The number of received EAPOL logoff frames.
Last EAPOL Frame Version	The protocol version number carried by the most recent EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recent EAPOL frame.

EAP Response/Id Frames Received	The number of received EAP response/identity frames.
EAP Response Frames Received	The number of valid received EAP response frames (other than resp/id frames).
EAP Request/Id Frames Transmitted	The number of transmitted EAP request/identity frames that have been transmitted.
EAP Request Frames Transmitted	The number of transmitted EAP request frames (other than request/identity frames).
Invalid EAPOL Frames Received	The number of received EAPOL frames without a recognized frame type.
EAP Length Error Frames Received	The number of received EAPOL frames without a recognized frame type.

5-298 show dot1x authentication-history

Displays 802.1X authentication events and information during successful and unsuccessful Dot1x authentication attempts for specific or all interfaces.

show dot1x authentication-history {*stot/port* **| all [failed-auth-only | detail]}**

Parameters

stot/port	Enter an interface in slot/port format.
all	Enter all to specify all ports.
detail	(Optional) Display the details of the Dot1x authentication history log events.
failed-auth-only	(Optional) Display the Dot1x failed authentication events from the Dot1x history log.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Time Stamp	Time stamp for event occurance
Interface	Physical Port of event.
Mac-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port upon authentication.
VLAN assigned Reason	The type of VLAN ID assigned, values: Guest VLAN, Unauth, Default,

	RADIUS Assigned, or Montior Mode VLAN ID.
Auth Status	The authentication status.
Reason	The specified reason for a successful or failed authentication attempt.

5-299 show dot1x clients

Display 802.1X client information as well as information regarding the number of clients that are authenticated.

show dot1x clients {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter all to specify all ports.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show dot1x clients all

Clients Authenticated using Monitor Mode..... 0
Clients Authenticated using Dot1x............... 0
```

Display Parameters

Clients Authenticated using Monitor Mode	The number of the Dot1x authenticated clients using Monitor mode.
Clients Authenticated using Dot1x	The number of authenticated Dot1x clients using 802.1X authentication process.
Logical Interface	The logical port number.
Interface	The physical port associated to the supplicant.
User Name	The user name used for authenticate to the server.
Supplicant MAC Address	The supplicant device’s MAC address.
Session Time	The period of time for the logged in session.

Filter ID	The Filter ID as defined by the RADIUS server authenticating the client. This is a configured DiffServ policy name on the switch.
VLAN ID	The assigned VLAN.
VLAN Assigned	The assigned VLAN identified, values include: RADIUS, Unauthenticated VLAN, Monitor Mode, or Default.
Session Timeout	The value indicating the valid session time. The time period in seconds is returned by the RADIUS server on authentication of the port.
Session Termination Action	Defined action following the timeout period. Possible values are Default and RADIUS -Request.

5-300 show dot1x users

Display 802.1X port security user information for locally configured users.

show dot1x users *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show dot1x users 0/1

Users
-----------------
admin
guest
```

Display Parameters

Users	Users configured locally with access to the specified port.

802.1X Supplicant Commands

D-Link OS supports 802.1X (dot1x) supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

5-301 dot1x dynamic-vlan

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

No command sets the dot1x dynamic-vlan to default.

dot1x dynamic-vlan {*enable***}**

no dot1x dynamic-vlan

Parameters

enable	Enable dot1x dynamic vlan creation configuration.

Default

The default is None.

Command Mode

Global Config

5-302 dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

dot1x eapolflood

no dot1x eapolflood

Parameters

None

Default

The default is Auto.

Command Mode

Interface Config

5-303 dot1x supplicant max-start

Configure the number of defined attempts before ending authenticator request to find the authenticator.

No command sets the max-start value to default.

dot1x supplicant max-start *1-10*

no dot1x supplicant max-start

Parameters

None

Default

The default is 3.

Command Mode

Interface Config

5-304 show dot1x statistics

Displays the dot1x port statistics in detail.

show dot1x statistics *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example.

```
(Routing)#show dot1x statistics 0/1

Port..................................... 0/1
EAPOL Frames Received.................... 0
EAPOL Frames Transmitted................. 0
EAPOL Start Frames Transmitted........... 3
EAPOL Logoff Frames Received............. 0
```

```
EAP Resp/Id frames transmitted.................. 0
EAP Response frames transmitted................. 0
EAP Req/Id frames transmitted................... 0
EAP Req Frames transmitted...................... 0
Invalid EAPOL frames received................... 0
EAP length error frames received................ 0
Last EAPOL Frame Version........................ 0
Last EAPOL Frame Source......................... 00:00:00:00:02:01
```

Display Parameters

EAPOL Frames Received	Displays the number of valid EAPOL frames received on the port.
EAPOL Frames Transmitted	Displays the number of EAPOL frames transmitted via the port.
EAPOL Start Frames Transmitted	Displays the number of EAPOL Start frames transmitted via the port.
EAPOL Logoff Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.
EAP Resp/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
EAP Response Frames Received	Displays the number of valid EAP Respond frames received on the port.
EAP Req/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.
EAP Req Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
EAP Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
Last EAPOL Frames Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frames Source	Displays the source MAC Address attached to the most recently received EAPOL frame.

Task-based Authorization

Task-based authorization configures specific permission levels (read, write, execute, debug) at a per-component level. The function defines permission for commands for a given user, locally authenticated through CLI interface

Users are assigned to User Groups which are then associated with Task Groups. Each Task Group is then associated with one or more tasks/components supporting AAA, BGP and OSPF components.

5-305 usergroup

Create a user group with the specified name and enters user group configuration mode.

No command removes the user group with the specified name.

usergroup *usergroup-name*

no usergroup *usergroup-name*

Parameters

usergroup-name	Enter usergroup name.

Default

The default is None.

Command Mode

Global Config

5-306 taskgroup

Create a task group and enter task group configuration mode.

No command removes the task group.

taskgroup *taskgroup-name*

no taskgroup *taskgroup-name*

Parameters

taskgroup-name	Enter taskgroup name.

Default

The default is None.

Command Mode

Global Config

5-307 username usergroup

Assign the specified user to a user group.

No command removes the specified user from the specified user group.

username *username* **usergroup** *usergroup-name*

no username *username* **usergroup** *usergroup-name*

Parameters

username	Indicates the username to assign.
usergroup-name	Configure participated usergroup.

Default

The default is None.

Command Mode

Global Config

5-308 description (User Group Mode)

Sets a description for the user group.

No command removes the description from the user group.

description *description*

no description

Parameters

description	Enter description for this usergroup.

Default

The default is None.

Command Mode

User Group

5-309 inherit usergroup (User Group Mode)

Set the parent group for the current user group. The user group acquires the permissions of the parent group.

No command removes the specified user-parent group relationship.

inherit usergroup *usergroup-name*

no inherit usergroup *usergroup-name*

Parameters

usergroup-name	Inherit to this usergroup.

Default

The default is None.

Command Mode

User Group

5-310 taskgroup (User Group Mode)

Associate a user group with a specified task group.

No command removes the user group's relationship with the associated task group.

taskgroup *taskgroup-name*

no taskgroup *taskgroup-name*

Parameters

taskgroup-name	Enter taskgroup name.

Default

The default is None.

Command Mode

User Group

5-311 description (Task Group Mode)

Sets a description for the task group.

No command removes the description from the task group.

description *description*

no description

Parameters

description	Enter description for this usergroup.

Default

The default is None.

Command Mode

Task Group

5-312 inherit taskgroup (Task Group Mode)

Set the parent task group of the current task group. The task group acquires the permissions of the specified parent task group.

No command removes the specified parent-user group relationship.

inherit taskgroup *taskgroup-name*

no inherit taskgroup *taskgroup-name*

Parameters

taskgroup-name	Enter taskgroup name.

Default

The default is None.

Command Mode

Task Group

5-313 task [read] [write] [debug] [execute]

Associate the task group with specified set of task permissions.

No command removes all associated relationships.

task [read] [write] [debug] [execute] {aaa | ospf | bgp}

no task (aaa | ospf | bgp}

Parameters

read	(Optional) Set read permission.
write	(Optional) Set write permission.
debug	(Optional) Set debug permission.
execute	(Optional) Set execute permission.

aaa	Authentication, Authorization and Accounting.
ospf	Open Shortest Path First.
bgp	Border Gateway Protocol.

Default

The default is No Permissions.

Command Mode

Task Group

Example

The following example gives all users in the task group tg1 read-only permissions for AAA and read, write, execute, and debug permissions for OSPF.

```
(Routing)#configure

(Routing)(ConFig)#taskgroup tg1

(Routing)(ConFig-taskgroup)#task read aaa

(Routing)(ConFig-taskgroup)#task read write execute debug ospf
```

5-314 show aaa usergroup

Displays a list of user groups and their configuration.

show aaa usergroup [*usergroup-name***]**

Parameters

usergroup-name	(Optional) Enter usergroup name.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show aaa usergroup group1

User group “group1”
```

```
Description: “Example”
Parent user groups: “”
Contained task groups:
task group#1: “tg1”

Operational permissions:
Task: aaa    : READ    WRITE   EXECUTE    DEBUG
Task: ospf   : READ    WRITE   EXECUTE    DEBUG
Task: bgp    : READ    WRITE   EXECUTE    DEBUG
```

5-315 show aaa taskgroup

Display a list of task groups and their configuration.

show aaa taskgroup [*taskgroup-name***]**

Parameters

taskgroup-name	(Optional) Enter taskgroup name.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show aaa taskgroup

Task group “default-taskgroup-name”

Description: “”
Parent taskgroups: “”

Configured permissions:
Task: aa     : READ    WRITE   EXECUTE    DEBUG
Task: ospf   : READ    WRITE   EXECUTE    DEBUG
Task: bgp    : READ    WRITE   EXECUTE    DEBUG

Operational permission:
Task: aa     : READ    WRITE   EXECUTE    DEBUG
Task: ospf   : READ    WRITE   EXECUTE    DEBUG
Task: bgp    : READ    WRITE   EXECUTE    DEBUG

Task group “task1”
```

```
Description: “”
Parent taskgroups: “”

Configured permissions:
Task: aa     : READ     WRITE    EXECUTE    DEBUG
Task: ospf   : READ
Task: bgp    : READ

Operational permission:
Task: aa     : READ     WRITE    EXECUTE    DEBUG
Task: ospf   : READ
Task: bgp    : READ
```

5-316 show aaa userdb

Display user and group lists a user is participating.

show aaa userdb [*username***]**

Parameters

username	Enter user name.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show aaa userdb admin

User “admin”

Contained user groups:
user group#1: “D-LINK OS-Root”

Operational permissions:
Task: aa     : READ     WRITE    EXECUTE    DEBUG
Task: ospf   : READ     WRITE    EXECUTE    DEBUG
Task: bgp    : READ     WRITE    EXECUTE    DEBUG
```

Asymmetric Flow Control Commands

Configure settings for symmetric, asymmetric or no flow control. Asymmetric flow control allows the switch to respond to received PAUSE frames—port is unable to generate PAUSE frames. Symmetric flow control allows the switch to respond and generate MAC control PAUSE frames.

5-317 flowcontrol

Enable or disable symmetric or asymmetric flow control. Asymmetric disables Tx Pause, enabling only Rx Pause.

No command disables the symmetric and asymmetric flow control.

flowcontrol {symmetric | asymmetric}

no flowcontrol

Parameters

symmetric	Enable Symmetric flow control.
asymmetric	Enable Asymmetric flow control.

Default

The default is Disabled.

Command Mode

Global Config

5-318 show flowcontrol

Display the IEEE 802.3 Annex 31B flow control settings and status for all or specific interfaces. In addition, it displays 802.3 Tx and Rx pause counts.

show flowcontrol [*slot/port***]**

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show flowcontrol

Admin Flow Control: Symmetric

Port    Flow Control Oper    RxPause    TxPause
-----   ------------------   --------   --------
0/1     Active               310        611
0/2     Inactive             0          0
--More-- or (q)uit
```

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

Admin Flow Control: Symmetric

Port    Flow Control Oper    RxPause    TxPause
-----   ------------------   --------   --------
0/1     Active               310        611
```

Display Parameters

Admin Flow Control	The administrative mode of flow control.
Port	The port associated with the rest of the data in the row.
Flow Control Oper	The operational mode of flow control.
RxPause	The received pause frame count.
TxPause	The transmitted pause frame count.

Storm-Control Commands

This section provides storm-control configuration information. When incoming packets flood the LAN, it is defined as a traffic storm condition leading to network performance degradation. Storm-Control features prevents the occurance of such events.

To configure storm-control, enable the feature for all or specific interfaces. Once enabled the threshold (storm-control level) can be set — this is the limit used to drop broadcast or unicast traffic. The Storm-Control allows for the definition of rate limits of specific types of packets through the switch on a per-port, per-type, basis.

Note: The incoming packet size as well as the hard-coded packet size (512 bytes) is used to calculate the actual rate of ingress traffic required to activate storm-control. As an example, if a configured limit is assumed to be 10%, it can be converted to ~25000 pps. The arrived pps limit is set in the forwarding

plane (hardware). Based on the figure, the approximate desired output when 512bytes packets are used can be calculated.

5-319 storm-control broadcast

Enable broadcast storm recovery mode for all or specific interfaces (Global Config mode/Interface Config mode). If enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

No command disables broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

storm-control broadcast

no storm-control broadcast

Parameters

None

Default

The default is Disabled.

Command Mode

- Global Config
- Interface Config

5-320 storm-control broadcast action

This command configures the broadcast storm recovery action to either shutdown or trap for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to **shutdown**, the interface that receives the broadcast packets at a rate above the threshold is diagnostically disabled. If set to **trap**, the interface sends trap messages approximately every 30 seconds until broadcast storm control recovers.

Use the **no** command to configure the broadcast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (lnterface Config mode).

storm-control broadcast action {shutdown | trap}

no storm-control broadcast action

Parameters

shutdown	Enter the storm-control action to shutdown.
trap	Enter the storm-control action to trap.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

5-321 storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Use the **no** command to set the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

storm control broadcast level *0-100*

no storm control broadcast level

Parameters

None

Default

The default is 5.

Command Mode

- Global Config
- Interface Config

5-322 storm-control broadcast rate

Configure the broadcast storm recovery threshold for all or specific interfaces (Global Config mode/Interface Config mode) in packets per second. Enabled the mode to activate broadcast storm recovery. Once the L2 broadcast traffic ingressing rate on an interface surpasses the configured threshold, the traffic is dropped.

No command sets the broadcast storm recovery threshold to the default value for all or specific interfaces (Global Config mode/Interface Config mode) and disables broadcast storm recovery.

storm-control broadcast rate *0-14880000*

no storm-control broadcast rate

Parameters

None

Default

The default is 0.

Command Mode

- Global Config
- Interface Config

5-323 storm-control multicast

Enable multicast storm recovery mode for all or specific interfaces (Global Config mode/Interface Config mode). Enable the mode to activate multicast storm recovery . Once the L2 multicast traffic rate ingress surpasses configured threshold, the traffic is dropped.

No command disables multicast storm recovery mode for all or specific interfaces (Global Config mode /Interface Config mode).

storm control multicast

no storm control multicast

Parameters

None.

Default

The default is Disabled.

Command Mode

- Global Config
- Interface Config

5-324 storm-control multicast action

Configure the multicast storm recovery action to **shutdown** or **trap** for all or specific interfaces (Global Config mode/Interface Contig mode). The **shutdown** configuration allows interface that receive multicast packets at a rate above the threshold are diagnostically disabled. While the **trap** function sends trap messages approximately every 30 seconds until multicast storm control event is over.

No command returns the multicast storm recovery action option to default for all or specific interfaces (Global Config mode/Interface Config mode).

storm-control multicast action {shutdown | trap}

no storm-control multicast action

Parameters

shutdown	Enter the storm-control action to shutdown.
trap	Enter the storm-control action to trap.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

5-325 storm-control multicast level

Configure the multicast storm recovery threshold for all or specific interfaces (Global Config mode/Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode. Enable the mode to activate multicast storm recovery. If the L2 multicast traffic rate ingressing on an interface surpasses the configured threshold, the traffic is dropped.

No command set the multicast storm recovery threshold to default for all or specific interfaces (Global Config mode/Interface Config mode) and disables multicast storm recovery.

storm-control multicast level *0-100*

no storm-control multicast level *0-100*

Parameters

None

Default

The default is 5.

Command Mode

- Global Config
- Interface Config

5-326 storm-control multicast rate

Configure the multicast storm recovery threshold for all or specific interfaces (Global Config mode/Interface Config mode) in packets per second. Enable the mode to activate multicast storm recovery. If the L2 broadcast traffic rate ingressing on an interface surpasses the configured threshold, the traffic is dropped.

Use the **no** command to set the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

storm-control multicast rate *0-14880000*

no storm-control multicast rate

Parameters

None

Default

The default is 0.

Command Mode

- Global Config
- Interface Config

5-327 storm-control unicast

Enable unicast storm recovery mode for all or specific interfaces (Global Config mode/Interface Config mode) Enable the mode to activate unicast storm recovery. If the unknown L2 unicast (destination lookup failure) traffic rate ingressing on an interface surpasses the configured threshold, the traffic is dropped.

No command disables unicast storm recovery mode for all or specified interfaces (Global Config mode/Interface Config mode).

storm-control unicast

no storm-control unicast

Parameters

None.

Default

The default is Disabled.

Command Mode

- Global Config
- Interface Config

5-328 storm-control unicast action

Configure the unicast storm recovery action to **shutdown** or **trap** for all or specific interfaces (Global Config mode/Interface Config mode) If configured to **shutdown**, the interface that receives unicast packets exceeding the threshold is diagnostically disabled. The option **trap** sends trap messages at a rate of every 30 seconds until unicast storm control is recovered.

No command returns the unicast storm recovery action option to default for all or specified interfaces (Global Config mode/Interface Config mode).

storm-control unicast action {shutdown | trap}

no storm-control unicast action

Parameters

shutdown	Enter the storm-control action to shutdown.
trap	Enter the storm-control action to trap.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

5-329 storm-control unicast level

Configure the unicast storm recovery threshold for all or specific interfaces (Global Config mode/Interface Config mode) as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active. If the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface surpasses the configured threshold, the traffic will be dropped. In which case, the rate of unknown unicast traffic is limited to the configured threshold.

No command sets the unicast storm recovery threshold to default for all and specific interfaces (Global Config mode/Interface Config mode) and disables unicast storm recovery.

storm-control unicast level *0-100*

no storm-control unicast level

Parameters

None

Default

The default is 5.

Command Mode

- Global Config
- Interface Config

5-330 storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, trate of unicast traffic is limited to the configured threshold.

Use the **no** command to set the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

storm-control unicast rate *0-14880000*

no storm-control unicast rate

Parameters

None

Default

The default is None.

Command Mode

- Global Config
- Interface Config

5-331 show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

Use the **all** keyword to display the per-port configuration parameters for all interfaces, or specify the ***slot/port*** to display information about a specific interface.

show storm-control [all I *slot/port***]**

Parameters

all	(Optional) Display storm-control information for all ports.
slot/port	(Optional) Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an output example.

```
(Routing)#show storm-control

Broadcast Storm Control Mode..................... Disable
Broadcast Storm Control Level.................... 5 percent
Broadcast Storm Control Action................... None
Multicast Storm Control Mode..................... Disable
Multicast Storm Control Level.................... 5 percent
Multicast Storm Control Action................... None
Unicast Storm Control Mode....................... Disable
Unicast Storm Control Level...................... 5 percent
Unicast Storm Control Action..................... None
```

The following is an output example.

```
(Routing)#show storm-control 0/1

Intf    Bcast     Bcast    Bcast     Mcast    Mcast   Mcast    Ucast     Ucast    Ucast
        Mode      Level    Action    Mode     Level   Action   Mode      Level    Action
------  ------    ------   ------    ------   ------  ------   ------    ------   ------
0/1     Disable   5%       None      Disable  5%      None     Disable   5%       None
```

The following is an output example.

```
(Routing)#show storm-control all

Intf    Bcast     Bcast    Bcast     Mcast    Mcast   Mcast    Ucast     Ucast    Ucast
        Mode      Level    Action    Mode     Level   Action   Mode      Level    Action
------  ------    ------   ------    ------   ------  ------   ------    ------   ------
0/1     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/2     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/3     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/4     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/5     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/6     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/7     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/8     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/9     Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/10    Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/11    Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/12    Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/13    Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/14    Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/15    Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/16    Enable    50       Trap      Disable  5%      None     Disable   5%       None
0/17    Enable    50       Trap      Disable  5%      None     Disable   5%       None
```

```
0/18    Enable    50        Trap      Disable 5%      None     Disable    5%        None
0/19    Enable    50        Trap      Disable 5%      None     Disable    5%        None
```

Display Parameters

Bcast Mode	Displays broadcast storm control mode. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Bcast Action	Enables broadcast traffic storm control on the interface.
Mcast Mode	Displays the multicast storm control mode.
Mcast Level	The multicast storm control level.
Mcast Action	Enables multicast traffic storm control levels.
Ucast Mode	Displays the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode.
Ucast Level	Displays the Unknown Unicast or DLF (Destination Lookup Failure) storm control level.
Ucast Action	Displays the storm-control action setting for unicast traffic.

Link Dependency Commands

The following commands configure link dependency. Link dependency allows specified ports to be link-status dependent of selected ports. Consequently, if a port link dependency is lost, the port is equally affected.

5-332 link state group

Indicate whether the downstream interfaces of the group should mirror or invert the status of the upstream interfaces (default configuration for a group is down). The action up option causes the downstream interfaces to be up when no upstream interfaces are down.

No command restores the link state to down for the group.

link state group *group-id* **action {up | down}**

no link state group *group-id* **action**

Parameters

group-id	Enter the link dependency group number.
action up	Link UP the group downstream interface list when upstream link goes down (link is down otherwise)
action down	Link DOWN the group downstream interface list when upstream link goes down (link is up othewise).

Default

The default is Down.

Command Mode

Global Config

5-333 link state group downstream

Add interfaces to the downstream interface list. The addition of an interface to a downstream list brings the interface down until an upstream interface is added to the group. To avoid the unexpected disconnection of an interface, enter the upstream command prior to entering the downstream command.

No command removes the selected interface from the downstream list.

link state group *group-id* **downstream**

no link state group *group-id* **downstream**

Parameters

group-id	Enter the link dependency group number (1 – 48).

Default

The default is None.

Command Mode

Interface Config

5-334 link state group upstream

Add interfaces to the upstream interface list--interfaces defined as upstream interfaces cannot be defined downstream interfaces in the same link state group or as a downstream interface.

No command removes the selected interfaces from upstream list.

link state group *group-id* **upstream**

no link state group *group-id* **upstream**

Parameters

group-id	Enter the link dependency group number (1 – 48).

Default

The default is None.

Command Mode

Interface Config

5-335 show link state group

Display information for a specified or all configured link-dependency groups.

show link state group *group-id*

Parameters

group-id	Enter the link dependency group number (1 – 48).

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a configured link-dependency groups example.

```
(Switching)#show link-state group

GroupId    Downstream Interfaces      Upstream Interfaces     Link Action  Group State
--------   ----------------------     ----------------------  -----------  ------------
1          0/3-0/7,0/12-0/17          0/12-0/32,3/5           Link Up      Up
4          0/18,0/27                  0/22-0/33,3/1           Link Up      Down
```

Thefollowing is a specified link-dependency groups.

```
(Switching)#show link-state group 1

GroupId    Downstream Interfaces      Upstream Interfaces     Link Action  Group State
--------   ----------------------     ----------------------  -----------  ------------
1          0/3-0/7,0/12-0/17          0/12-0/32,3/5           Link Up      Up
```

Display Parameters

GroupID	Indicates the group ID for each displayed set.
Downstream Interfaces	Indicates a tracking of the port's inclusion to the Downstream set.
Upstream Interfaces	Indicates a tracking of the port's inclusion to the Upstream set.
Link Action	Indicates the current state of the specified link-dependency group.

Group State	Indicates the current state of the link-dependency group.

5-336 no link state track

This command is used to disable the link state track feature.

no link state track *group-id*

Parameters

group-id	Enter the link dependency group number (1 – 48).

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a configured link-dependency groups example.

```
(Switching)#configure
(Switching)(Config)#no link state track 1
```

5-337 show link state group detail

Display detailed information regarding upstream and downstream interface states for selected link-dependency group.

show link state group *group-id* **detail**

Parameters

group-id	Enter the link dependency group number (1 – 48).

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Switching)#show link state group 1 detail

GroupId:      1
Link Action:  Up
Group State:  Up

Downstream Interface State:
Link Up:      0/3
Link Down:    0/4-0/7,0/12-0/17

Upstream Interface State:
Link Up:      -
Link Down:    0/12-0/32,3/5

Group Transitions: 0
Last Transition Time: 00:52:35 (UTC+0:00) Jan 1 1970
```

5-338 show llpf interface all

Display Link Layer Packet Filtering (LLPF) rule status.

show llpf interface [all | *slot/port*]

Parameters

all	(Optional) Display link-level protocol filtering complete configuration.
slot/port	(Optional) Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show llpf interface all

Intf    Block       Block       Block      Block      Block      Block       Block
        Protocol    Protocol    Protocol   Protocol   Protocol   Protocol    Protocol
        ISDP        VTP         DTP        UDLD       PAGP       SSTP        All
------  --------    --------    --------   --------   --------   --------    --------
0/1     Enabled     Disabled    Disabled   Enabled    Disabled   Disabled    Disabled
```

0/2	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/3	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/4	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/5	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/6	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/7	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/8	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/9	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/10	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/11	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/12	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/13	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/14	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/15	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/16	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/17	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/18	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/19	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/20	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/21	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/22	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/23	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/24	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/25	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/26	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/27	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/28	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/29	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/30	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/31	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/32	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/33	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/34	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/35	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/36	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/37	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/38	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/39	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/40	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0/41	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled

Display Parameters

Block ISDP	Shows whether the port blocks IPTV Service Delivery Platform (ISDP) PDUs.
Block VTP	Shows whether the port blocks VLAN Trunking Protocol (VTP) PDUs.
Block DTP	Shows whether the port blocks Dynamic Trunking Protocol (DTP) PDUs.
Block UDLD	Shows whether the port blocks Unidirectional Link Detection (UDLD)

	PDUs.
Block PAGP	Shows whether the port blocks Port Aggregation Protocol (PAgP) PDUs.
Block SSTP	Shows whether the port blocks Secure Socket Tunneling Protocol (SSTP) PDUs.
Block All	Shows whether the port blocks all proprietary PDUs available for the LLDP feature.

MVR Commands

Lists the Multicast VLAN Registration (MVR) commands.

5-339 mvr

Enable MVR, default: disabled.

No command disables MVR.

mvr

no mvr

Parameters

None

Default

The default is Disable.

Command Mode

- Global Config
- Interface Config

5-340 mvr group

Use this command to add an MVR membership group.

Use the **no** command to disable an MVR membership group.

mvr group

no mvr group

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-341 mvr immediate

Enable MVR Immediate Leave mode. When an interface configured as a source ports, MVR immediate cannot be enabled.

No command disables MVR Immediate Leave mode.

mvr immediate

no mvr immediate

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-342 mvr mode

Change the Multicast VLAN Registration (MVR) mode type (default: compatible).

No command sets the MVR mode type to compatible (default).

mvr mode [compatible | dynamic]

no mvr mode

Parameters

compatible	(Optional) Enable MVR compatible mode. While in compatible mode, multicast data received by MVR hosts is forwarded to all data ports (MVR), regardless of MVR host membership on those ports. The multicast data is forwarded only to receiver ports if MVR hosts have already joined them, either by IGMP reports or by MVR static configuration.
dynamic	(Optional) Enable MVR dynamic mode. While in dynamic mode,

	multicast data received by MVR hosts on the switch is forwarded from only joined, either by IGMP reports or by MVR static configuration, MVR data and client ports.

Default

The default is None.

Command Mode

Global Config

5-343 mvr querytime

Set the MVR query response time (1/10 sec.). The query time is the maximum waiting time for an IGMP membership report on a receiver port before removing it from the multicast group.

No command sets the MVR query response time to the default.

mvr querytime *1-100*

no mvr querytime

Parameters

None

Default

The default is 5.

Command Mode

Global Config

5-344 mvr type

Set the MVR port type, default is none.

No command resets the MVR port type to None.

mvr type [receiver | source]

no mvr type

Parameters

receiver	(Optional) Set the MVR Receiver port type.
source	(Optional) Set the MVR Source port type.

Default

The default is None.

Command Mode

Interface Config

5-345 mvr vlan

Set the MVR multicast VLAN.

No command sets the MVR multicast VLAN to default.

mvr vlan *1-4093*

no mvr vlan

Parameters

None

Default

The default is 1.

Command Mode

Global Config

5-346 mvr vlan group

Configure a port to participate in a specific MVR group. The default value is None.

No command removes port participation in the specific MVR group.

mvr vlan *mvlan* **group** *A.B.C.D*

no mvr vlan *mvlan* **group** *A.B.C.D*

Parameters

mvlan	Indicates the multicast VLAN ID (1 – 4093).
A.B.C.D	IP multicast address.

Default

The default is None.

Command Mode

Interface Config

5-347 show mvr

Display global MVR settings.

show mvr

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Switching)#show mvr

MVR Disabled.
```

```
(Switching)#show mvr

MVR Running..................................... TRUE
MVR multicast VLAN.............................. 1
MVR Max Multicast Groups........................ 256
MVR Current multicast groups.................... 0
MVR Global query response time.................. 5 (tenths of sec)
MVR Mode........................................ compatible
```

5-348 show mvr members

Display the allocated MVR membership groups.

show mvr members [*A.B.C.D***]**

Parameters

A.B.C.D	(Optional) Indicates the MVR Group IP.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Switching)#show mvr members

MVR Group IP      Status          Members
-------------     ----------      -------------------------
224.1.1.1         INACTIVE        0/1, 0/2, 0/3
```

```
(Switching)#show mvr members 224.1.1.1

MVR Group IP      Status          Members
-------------     ----------      -------------------------
224.1.1.1         INACTIVE        0/1, 0/2, 0/3
```

5-349 show mvr interface

Display the cgnfiguration of MVR-enabled interfaces.

show mvr interface [*interface-id* **[members [vlan** *vlan-id***]]]**

Parameters

interface-id	(Optional) Enter an interface in slot/port format.
members	(Optional) Multicast group members on this port.
vlan *vlan-id*	(Optional) MVR multicast VLAN.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Switching)#show mvr interface

Port    Type            Status               Immediate Leave
------  ----------      ---------------      --------------------
0/9     RECEIVER        ACTIVE/inVLAN        DISABLED
```

```
(Switching)#show mvr interface 0/4

Type: NONE    Status: INACTIVE/InVLAN    Immediate Leave: DISABLED
```

```
(Switching)#show mvr interface 0/23 members

235.0.0. 1    STATIC ACTIVE
```

```
(Switching)#show mvr interface 0/23 members vlan 12

235.0.0.1     STATIC ACTIVE
235.1.1.1     STATIC ACTIVE
```

5-350 show mvr traffic

Display global MVR statistics.

show mvr traffic

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Switching)#show mvr traffic

IGMP Query Received.............................. 0
IGMP Report V1 Received.......................... 0
IGMP Report V2 Received.......................... 0
IGMP Leave Received.............................. 0
IGMP Query Transmitted........................... 0
IGMP Report V1 Transmitted....................... 0
```

```
IGMP Report V2 Transmitted..................... 0
IGMP Leave Transmitted......................... 0
IGMP Packet Receive Failures................... 0
IGMP Packet Transmit Failures.................. 0
```

5-351 debug mvr trace

Enable MVR debug tracing, default is disabled

No command disables MVR debug tracing.

debug mvr trace

no debug mvr trace

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

5-352 debug mvr packet

Enable MVR receive/transmit packets debug tracing. Without argument specification both receive and transmit packets debugging is enabled (default).

No command disables MVR receive/transmit packet debug tracing.

debug mvr packet [receive | transmit]

no debug mvr packet [receive | transmit]

Parameters

receive	(Optional) Turn on MVR receive packet debug trace.
transmit	(Optional) Turn on MVR transmit packet debug trace.

Default

The default is Enabled.

Command Mode

Privileged EXEC

Port-Channel/LAG (802.3ad) Commands

This section describes port-channel configuration , also known as link aggregation groups (LAGs). Link aggregation allows multiple full-duplex Ethernet link combinations into a single logical link. Network devices treat the aggregation as a single link allowing for increased fault tolerance and load sharing.

A port-channel (LAG) interface can be designated as static or dynamic. All members within the same port channel are designated same protocols.

Note: Configuring the maximum number of supported dynamic port-channels (LAGs) will configure additional port-channels as static.

5-353 port-channel

Configure a new port-channel (LAG) and generate logical *slot/port* number for a port-channel. Use the **show port-channel** command to display the *slot/port* number for the logical interface.

Note: Set port physical mode before including a port in a port-channel.

Note: *Name* fields support alphanumberic and characters string, such as dashes "-".

port-channel {adminmode [all] | linktrap [*slot/port* **| all | lag** *lag-group-id***] | load-balance [1|2|3|4|5|6|7] {***slot/port* **| all} | name [***slot/port* **| lag** *lag-group-id***]** *name* **| resilient-hashing | system priority** *0-65535***}**

Parameters

adminmode	Enable/Disable the port-channel's administrative Mode.
linktrap	Enable/Disable Link Up/Down traps for this port.
load-balance	Configures port-channel load balance.
name	Configure a name for the interface port-channel.
resilient-hashing	Enable the resilient hashing in the port-channel.
***system* priority**	Configure port channel system priority (LAG).

Default

The default is None.

Command Mode

Global Config

5-354 port-channel adminmode

This command enables all configured port-channels with the same administrative mode setting.

Use the **no** command to disable all configured port-channels wit the same administrative mode setting.

port-channel adminmode all

no port-channel adminmode all

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-355 port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical *slot/port* for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Use the **no** command to disable link trap notifications for the port-channel (LAG). The interface is a logical *slot/port* for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

port-channel linktrap {*logical slot/port* **| all | lag** *lag-group-id***}**

no port-channel linktrap {*logical slot/port* **| all | lag** *lag-group-id***}**

Parameters

slot/port	Enter permissible interface.
all	Enables/Disables link traps for all configured port-channels.
lag *lag-group-id*	Enter an interface in lag format.

Default

The default is Enabled.

Command Mode

Global Config

5-356 port-channel load-balance

Select the load-balancing option used on a port-channel (LAG). Select a channel link to transmit balanced traffic on a port-channel (LAG)

Configuration is available for single, a range, or all interfaces.

No command reverts load balancing configuration to default.

port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7} {*slot/port* **| all}**

no port-channel load-balance {*slot/port* **| all}**

Parameters

1	Source: MAC, VLAN, EtherType, and incoming port associated with the packet.
2	Destination: MAC, VLAN, EtherType, and incoming port associated with the packet.
3	Source/Destination: MAC, VLAN, EtherType, and incoming port associated with the packet.
4	Source IP and Source TCP/UDP fields of the packet.
5	Destination IP and Destination TCP/UDP Port fields of the packet.
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
7	Enhanced hashing mode.
slot/port **| all**	For Global Config Mode only: The interface is defined as a logical *slot/port* number of a configured port-channel. **All** configuration to all currently configured port-channels.

Default

The default is 3.

Command Mode

- Global Config
- Interface Config

5-357 port-channel min-links

Configures the port-channel's minimum links for lag interfaces.

port-channel min-links *1-32*

Parameters

None

Default

The default is 1.

Command Mode

Interface Config

5-358 port-channel name

Define a name for the port-channel (LAG). The interface is defined as a logical *slot/port* for a configured port-channel. The term *name* is defined as an alphanumeric string of up to 15 characters.

port-channel name {*logical slot/port***}** *name*

Parameters

slot/port	Enter permissible interface.
lag	Configure a name for the interface port-channel.

Default

The default is None.

Command Mode

Global Config

5-359 port-channel system priority

Configure port-channel system prioritis.

No command configures the port-channel system priority to default.

port-channel system priority *0-65535*

no port-channel system priority

Parameters

None

Default

The default is 0x8000.

Command Mode

Global Config

5-360 addport (Interface Config)

Add a port to the port-channel (LAG). The first interface is a logical *slot/port* number of a configured port-channel. To add a port range, specify the range in the Interface Config mode, example: **interface 0/1-0/4**.

Note: The physical mode of the port must be first set before adding a port to a port-channel.

addport *slot/port* **{lag** *lag-group-id* **}**

Parameters

slot/port	Enter permissible interface.
lag	Add this port to a port-channel.
lag-group-id	Enter a valid LAG group ID.

Default

The default is None.

Command Mode

Interface Config

5-361 deleteport (Interface Config)

Deletes a port or a range of ports from the port-channel (LAG). The interface is the logical *slot/port* number of the configured port or range of port channel.

deleteport *slot/port*

Parameters

slot/port	Enter permissible interface.
lag	Delete this port from a port-channel.

Default

The default is None.

Command Mode

Interface Config

5-362 deleteport (Global Config)

Delete all configured ports from the port-channel (AG). The interface is the logical *slot/port* number of the configured port or range of port channel.

deleteport {*slot/port* **| all}**

Parameters

logical slot/port	Enter permissible interface.
all	Sets every configured port-channel with the same administrative mode setting.

Default

The default is None.

Command Mode

Global Config

5-363 interface lag

Enter Interface configuration mode for a specified LAG.

interface lag *lag-interface-number*

Parameters

lag-interface-number	Enter LAG interface number.

Default

The default is None.

Command Mode

Global Config

5-364 ip resilient-hashing

Enable resilient hashing on all ECMP objects (default: enabled).

No command disables resilient hashing on all the ECMP objects.

Note: The device requires a reboot after changes to the configuration.

ip resilient-hashing

no ip resilient-hashing

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-365 port lacpmode

Enable Link Aggregation Control Protocol (LACP) on a port or range of ports.

No command disables Link Aggregation Control Protocol (LACP) on selected port.

port lacpmode

no port lacpmode

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

5-366 port lacpmode enable all

Enable Link Aggregation Control Protocol (LACP) on all ports.

No command disables Link Aggregation Control Protocol (LACP) on all ports.

port lacpmode enable all

no port lacpmode enable all

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-367 port lacptimeout (Interface Config)

Set timeout function on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Use the **no** command to set the timeout back to its default value on a physical interface of a particular device type (actor or partner).

Note: Both the **no portlacptimeout** and the **no lacp actor admin state** commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands Will display in **show running-config**.

port lacptimeout {actor} {long | short}

no port lacptimeout {actor}

Parameters

actor	Enter actor LACP device type.
long	Enter long timeout setting (90 seconds).
short	Enter short timeout setting (3 seconds).

Default

The default is Long.

Command Mode

Interface Config

5-368 port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Use the **no** command to set the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

Note: Both the **no portlacptimeout** and the **no lacp actor admin state** commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands Will display ih **show running-config**.

port lacptimeout {actor} {long | short}

no port lacptimeout {actor}

Parameters

actor	Enter actor LACP device type.
long	Enter long timeout setting (90 seconds).
short	Enter short timeout setting (3 seconds).

Default

The default is Long.

Command Mode

5-369 Global Configshow ip resilient-hashing

Displays the resilient hashing property for the ECMP.

show ip resilient-hashing

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Routing)#show ip resilient-hashing

Resilient Hashing.............................. Enabled

(Routing)#
```

Display Parameters

Resilient Hashing	Resilient hashing mode for the system.

5-370 show lacp actor

Display the LACP actor attributes.

show lacp actor {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter all for all interfaces.

Default

The default is None.

Command Mode

Global Config

Example

The following shows an example of the command.

```
(Routing)#show lacp actor all

Intf    Sys Priority    Admin Key    Port Priority     Admin State
-----   -------------   ----------   ---------------   ---------------
0/1     32768           0            128               ACT|AGG|LTO
0/2     32768           0            128               ACT|AGG|LTO
0/3     32768           0            128               ACT|AGG|LTO
0/4     32768           0            128               ACT|AGG|LTO
0/5     32768           0            128               ACT|AGG|LTO
0/6     32768           0            128               ACT|AGG|LTO
0/7     32768           0            128               ACT|AGG|LTO
0/8     32768           0            128               ACT|AGG|LTO
0/9     32768           0            128               ACT|AGG|LTO
0/10    32768           0            128               ACT|AGG|LTO
0/11    32768           0            128               ACT|AGG|LTO
0/12    32768           0            128               ACT|AGG|LTO
0/13    32768           0            128               ACT|AGG|LTO
0/14    32768           0            128               ACT|AGG|LTO
0/15    32768           0            128               ACT|AGG|LTO
0/16    32768           0            128               ACT|AGG|LTO
0/17    32768           0            128               ACT|AGG|LTO
0/18    32768           0            128               ACT|AGG|LTO
0/19    32768           0            128               ACT|AGG|LTO
0/20    32768           0            128               ACT|AGG|LTO
0/21    32768           0            128               ACT|AGG|LTO
0/22    32768           0            128               ACT|AGG|LTO
0/23    32768           0            128               ACT|AGG|LTO
0/24    32768           0            128               ACT|AGG|LTO
0/25    32768           0            128               ACT|AGG|LTO
0/26    32768           0            128               ACT|AGG|LTO
0/27    32768           0            128               ACT|AGG|LTO
```

0/28	32768	0	128	ACT|AGG|LTO
0/29	32768	0	128	ACT|AGG|LTO
0/30	32768	0	128	ACT|AGG|LTO
0/31	32768	0	128	ACT|AGG|LTO
0/32	32768	0	128	ACT|AGG|LTO
0/33	32768	0	128	ACT|AGG|LTO
0/34	32768	0	128	ACT|AGG|LTO
0/35	32768	0	128	ACT|AGG|LTO
0/36	32768	0	128	ACT|AGG|LTO
0/37	32768	0	128	ACT|AGG|LTO
0/38	32768	0	128	ACT|AGG|LTO
0/39	32768	0	128	ACT|AGG|LTO
0/40	32768	0	128	ACT|AGG|LTO
0/41	32768	0	128	ACT|AGG|LTO
0/42	32768	0	128	ACT|AGG|LTO
0/43	32768	0	128	ACT|AGG|LTO
0/44	32768	0	128	ACT|AGG|LTO
0/45	32768	0	128	ACT|AGG|LTO
0/46	32768	0	128	ACT|AGG|LTO
0/47	32768	0	128	ACT|AGG|LTO
0/48	32768	0	128	ACT|AGG|LTO
0/49	32768	0	128	ACT|AGG|LTO
0/50	32768	0	128	ACT|AGG|LTO
0/51	32768	0	128	ACT|AGG|LTO
0/52	32768	0	128	ACT|AGG|LTO
0/53	32768	0	128	ACT|AGG|LTO
0/54	32768	0	128	ACT|AGG|LTO
0/55	32768	0	128	ACT|AGG|LTO
0/56	32768	0	128	ACT|AGG|LTO
0/57	32768	0	128	ACT|AGG|LTO
0/58	32768	0	128	ACT|AGG|LTO
0/59	32768	0	128	ACT|AGG|LTO
0/60	32768	0	128	ACT|AGG|LTO
0/61	32768	0	128	ACT|AGG|LTO
0/62	32768	0	128	ACT|AGG|LTO
0/63	32768	0	128	ACT|AGG|LTO
0/64	32768	0	128	ACT|AGG|LTO
0/65	32768	0	128	ACT|AGG|LTO
0/66	32768	0	128	ACT|AGG|LTO
0/67	32768	0	128	ACT|AGG|LTO
0/68	32768	0	128	ACT|AGG|LTO
0/69	32768	0	128	ACT|AGG|LTO
0/70	32768	0	128	ACT|AGG|LTO
0/71	32768	0	128	ACT|AGG|LTO
0/72	32768	0	128	ACT|AGG|LTO
0/73	32768	0	128	ACT|AGG|LTO
0/74	32768	0	128	ACT|AGG|LTO
0/75	32768	0	128	ACT|AGG|LTO
0/76	32768	0	128	ACT|AGG|LTO
0/77	32768	0	128	ACT|AGG|LTO

```
0/78    32768           0            128              ACT|AGG|LTO
```

Display Parameters

System Priority	The value of the system priority Key.
Actor Admin Key	The value of the actor administrative Key.
Port Priority	The value assigned to the Aggregation (priority) Port.
Admin State	The values of the administrative state as transmitted by the Actor in LACPDUs.

5-371 show lacp partner

Display LACP partner attributes.

show lacp actor (*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter all for all interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)#show lacp partner all

          Sys     System              Admin   Prt     Prt     Admin
Intf      Pri     ID                  Key     Pri     Id      State
-----     -----   ------------------  ------  ------  ------  ---------------
0/1       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
0/2       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
0/3       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
0/4       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
0/5       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
0/6       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
0/7       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
0/8       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
0/9       0       00:00:00:00:00:00   0       0       0       PSV|IND|LTO
```

0/10	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/11	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/12	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/13	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/14	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/15	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/16	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/17	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/18	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/19	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/20	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/21	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/22	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/23	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/24	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/25	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/26	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/27	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/28	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/29	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/30	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/31	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/32	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/33	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/34	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/35	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/36	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/37	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/38	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/39	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/40	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/41	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/42	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/43	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/44	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/45	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/46	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/47	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/48	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/49	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/50	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/51	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/52	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/53	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/54	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/55	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/56	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/57	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/58	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO
0/59	0	00:00:00:00:00:00	0	0	0	PSV|IND|LTO

```
0/60        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/61        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/62        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/63        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/64        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/65        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/66        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/67        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/68        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/69        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/70        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/71        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/72        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/73        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/74        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/75        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/76        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/77        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
0/78        0       00:00:00:00:00:00    0       0       0       PSV|IND|LTO
```

Display Parameters

System Priority	The administrative value of priority associated with the Partner System ID.
System-ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The parameter assigned within the LACP packet to group channels containing ports assigned the same admin key.
Port Priority	The value assigned to the Aggregation (priority) Port.
Port-ID	The value of the administrative port number for the protocol Partner.
Admin State	The values of the administrative actor state for the protocol Partner.

5-372 show port-channel brief

Display the static capability of all port-channel (LAG) interfaces as well as a summary of individual port-channel interfaces.

show port-channel brief

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show port-channel brief

Logical      Port-Channel Min Link State  Trap   Type        Mbr Ports    Active Ports
Interface    Name                         Flag
----------   -----------  --------------  -----  --------    ----------   -------------
3/1          ch1          1               Down   Enabled     Static       0/5,0/6
3/2    ch2    1      Down   Enabled      Static 0/7,0/8
3/3    ch3    1      Down   Enabled      Static 0/9,0/10
3/4    ch4    1      Down   Enabled      Static
3/5    ch4    1      Down   Enabled      Static
3/6    ch4    1      Down   Enabled      Static
3/7    ch4    1      Down   Enabled      Static
3/8    ch4    1      Down   Enabled      Static
3/9    ch4    1      Down   Enabled      Static
3/10   ch4    1      Down   Enabled      Static
3/11   ch4    1      Down   Enabled      Static
3/12   ch4    1      Down   Enabled      Static
3/13   ch4    1      Down   Enabled      Static
3/14   ch4    1      Down   Enabled      Static
3/15   ch4    1      Down   Enabled      Static
3/16   ch4    1      Down   Enabled      Static
3/17   ch4    1      Down   Enabled      Static
3/18   ch4    1      Down   Enabled      Static
3/19   ch4    1      Down   Enabled      Static
3/20   ch4    1      Down   Enabled      Static
3/21   ch4    1      Down   Enabled      Static
3/22   ch4    1      Down   Enabled      Static
3/23   ch4    1      Down   Enabled      Static
3/24   ch4    1      Down   Enabled      Static
3/25   ch4    1      Down   Enabled      Static
3/26   ch4    1      Down   Enabled      Static
3/27   ch4    1      Down   Enabled      Static
3/28   ch4    1      Down   Enabled      Static
3/29   ch4    1      Down   Enabled      Static
3/30   ch4    1      Down   Enabled      Static
3/31   ch4    1      Down   Enabled      Static
3/32   ch4    1      Down   Enabled      Static
3/33   ch4    1      Down   Enabled      Static
3/34   ch4    1      Down   Enabled      Static
3/35   ch4    1      Down   Enabled      Static
3/36   ch4    1      Down   Enabled      Static
3/37   ch4    1      Down   Enabled      Static
3/38   ch4    1      Down   Enabled      Static
3/39   ch4    1      Down   Enabled      Static
```

```
3/40   ch4    1      Down   Enabled      Static
3/41   ch4    1      Down   Enabled      Static
3/42   ch4    1      Down   Enabled      Static
3/43   ch4    1      Down   Enabled      Static
3/44   ch4    1      Down   Enabled      Static
3/45   ch4    1      Down   Enabled      Static
3/46   ch4    1      Down   Enabled      Static
3/47   ch4    1      Down   Enabled      Static
3/48   ch4    1      Down   Enabled      Static
3/49   ch4    1      Down   Enabled      Static
3/50   ch4    1      Down   Enabled      Static
3/51   ch4    1      Down   Enabled      Static
3/52   ch4    1      Down   Enabled      Static
3/53   ch4    1      Down   Enabled      Static
3/54   ch4    1      Down   Enabled      Static
3/55   ch4    1      Down   Enabled      Static
3/56   ch4    1      Down   Enabled      Static
3/57   ch4    1      Down   Enabled      Static
3/58   ch4    1      Down   Enabled      Static
3/59   ch4    1      Down   Enabled      Static
3/60   ch4    1      Down   Enabled      Static
3/61   ch4    1      Down   Enabled      Static
3/62   ch4    1      Down   Enabled      Static
3/63   ch4    1      Down   Enabled      Static
3/64   ch4    1      Down   Enabled      Static
```

Display Parameters

Logical Interface	The slot/port of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

5-373 show port-channel

Displays an overview of all port-channels (LAGs). The LAG interface can be specified by through *slot/port* or **lag** *lag-intf-num*. Where *lag-intf-num* is expressed as a number, **lag** *lag-intf-num* can be used to specify the LAG interface.

show port-channel {*lag-intf-num* **|** *slot/port* **| all | brief | resilient hashing | system}**

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(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 Ports     Device/Timeout              Port Speed      Port Active
----------    ------------------------    ----------      ---------------
0/1           actor/long partner/long     Auto            True
0/2           actor/long partner/long     Auto            True
0/3           actor/long partner/long     Auto            False
0/4           actor/long partner/long     Auto            False
```

Display Parameters

Logical Interface	The valid slot/port number.
Port-Channel Name	The name of this port-channel (LAG), supports up to 15 alphanumeric characters.
Link State	Indicates the Link status (up or down).
Admin Mode	Enabled (default) or disabled, .
Type	Designates a port-channel (LAG) status: static or dynamic.
Load Balance Option	The load balance option associated with this LAG.
Load Preference Mode	Indicates whether the local preference mode is **enabled** or **disabled**.
Mbr Ports	Listing of member ports of this port-channel (LAG), in slot/port notation. A maximum of eight ports can be 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).

5-374 show port-channel counter

Display port-channel counters for the specified port.

show port-channel *slot/port* **counters**

Parameters

slot/port	Enter permissible interface.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Switch)#show port-channel 3/1 counters

Local Interface.................................. 3/1
Channel Name..................................... ch1
Link State....................................... Down
Admin Mode....................................... Enabled
Port Channel Flap Count.......................... 0

Mbr Ports    Mbr Flap 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
```

Display Parameters

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.

5-375 show port-channel resilient-hashing

Display the resilient hashing property for the port channel interface

show port-channel resilient-hashing

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Routing)#show port-channel resilient-hashing

Resilient Hashing.............................. Enabled

(Routing)#
```

Display Parameters

Resilient Hashing	Resilient hashing mode for the system.

5-376 show port-channel system priority

Display the port-channel system priority.

show port-channel system priority

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show port-channel system priority

System Priority................................ 32768
```

Display Parameters

System Priority	The administrative value of priority associated with the Partner System ID.

5-377 clear port-channel counters

Clear and reset counters for port-channels and member flaps for the specified interface.

clear port-channel {*lag-intf-num* **|** *slot/port* | *all***} counters**

Parameters

lag-intf-num	Enter LAG interface number.
slot/port	Enter permissible interface.
all	Enter 'all' for all interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

5-378 clear port-channel all counters

Clear and reset counters for all port-channels and member flaps for the specified interface.

clear port channel all counters

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

VPC Commands

Virtual private cloud (VPC), also known as MLAG, enables the creation of a LAG to across two independent switches for the purpose of allowing member ports of a VPC to reside on one switch while others can reside on a different switch.

5-379 vpc domain

Enter into VPC configuration mode and create a VPC domain with the specified domain-id. Only a single VPC domain can be created on a given device. The domain-id of the VPC domain must be equal to the one configured on the related VPC peer attempting the VPC pairing. The configured VPC domain-ids are exchanged during role election. If the configuration does not match, the VPC does not become operational.

No command deletes the VPC domain.

vpc domain *1-255*

no vpc domain *1-255*

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-380 feature vpc

Enable VPC globally which occurs if both VPC and the keepalive state machine are enabled. Peer link must be configured for role election to occur.

No command disables VPC.

feature vpc

no feature vpc

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-381 peer detection enable (VPC Config)

Start the Dual Control Plane Detection Protocol (DCPDP). The peer VPC switch's IP address must be configured for the DCPDP to start.

No command disables the dual control plane (DCPDP) detection protocol on the VPC switch.

peer detection enable

no peer detection enable

Parameters

None

Default

The default is None.

Command Mode

VPC Config

5-382 peer detection interval (VPC Config)

Configure the DCPDP transmission interval and reception timeout.
Configurable interval range: 200 ms – 4000 ms (default: 1000 ms). Configurable reception timeout range: 700 ms – 14000 ms (default: 3500 ms).

No command resets the DCPDP transmission interval and reception timeout to default.

peer detection interval *msecs* **timeout** *seconds*

no peer detection interval *msecs* **timeout** *seconds*

Parameters

msecs	Enter the transmission interval (200 – 400 in seconds).
timeout *seconds*	Enter the reception timeout (700 – 14000 in seconds).

Default

The default is as follows:

- Transmission interval: 1000 ms
- Reception timeout: 3500 ms

Command Mode

VPC Config

5-383 peer-keepalive destination (VPC Config)

Configures the IP address of the peer VPC switch, which is the destination IP address of the DCPDP on the peer VPC switch. This configuration is used by the DCPDP on the VPC switches. The source IP address of the DCPDP message is also configured with the function, which is the self IP on the VPC switch.

No command removes the self IP address, peer IP address, and the UDP port configuration (range: port 1 to 65535, default: 60000).

peer-keepalive destination *ipaddress* **source** *ipaddress* **[***udp-port port***]**

no peer-keepalive destination *ipaddress* **source** *ipaddress* **[***udp-port port***]**

Parameters

ipaddress	IP address of the peer VPC switch.
source *ipaddress*	Configures DCPDP source parameters.

Default

The default is None.

Command Mode

VPC Config

5-384 peer-keepalive enable

Start the keepalive state machine on the VPC device, if globally enabled.

No command stops the keepalive state machine of the VPC switch.

peer-keepalive enable

no peer-keepalive enable

Parameters

None

Default

The default is Disabled.

Command Mode

VPC Config

5-385 peer-keepalive timeout

Configure the peer keepalive timeout value (in seconds). If a VPC switch does not receive a keepalive message from the peer for the duration of the timeout value, it transitions its role.

No command resets the keepalive timeout to default (5 seconds).

Note: Keepalive state machine is not restarted if the priority is modified post election.

peer-keepalive timeout *2-15*

no peer-keepalive timeout

Parameters

None

Default

The default is 5.

Command Mode

VPC Config

5-386 role priority

Configure VPC switch priority for VPC role election. The priority value is sent to the peer in the VPC keepalive messages. A VPC switch with lowered priority is converted to the Primary while the switch with the higher priority is converted as the Secondary.

No command resets the keepalive priority and timeout to default (100).

role priority *1-255*

no role priority

Parameters

None

Default

The default is 100.

Command Mode

VPC Config

5-387 system-mac

Manually configure the MAC address for the VPC domain. The VPC MAC address should carry the same configuration both peer devices.

The specified MAC address must be a unicast MAC address <aa:bb:cc:dd:ee:ff> format. The address assigned must not use the primary VPC nor the secondary VPC device. The configured VPC MAC address is exchanged during role election and if configured differently on the peer devices, VPC is not initiated.

No command removes the manually configured VPC MAC address for the VPC domain.

system-mac *mac-address*

no system-mac

Parameters

mac-address	Enter MAC address.

Default

The default is None.

Command Mode

VPC Domain

5-388 system-priority

Manually configure a system priority for the VPC domain. System-priority configuration must be identical on both VPC peers. If the configured VPC system priority is different on VPC peers, the VPC does not come up.

The system-priority is used in the LACP PDUs sent out on VPC member ports, VPC system priorities must be configured to allow for primary device election.

The configurable range is 1 to 65535 (default: 32767).

No command restores the VPC system priority to default.

system-priority *1-65535*

no system-priority

Parameters

None

Default

The default is 32767.

Command Mode

VPC Domain

5-389 vpc

Configure a port-channel (LAG) as part of an VPC. Upon issuing this command, the port-channel is down pending port-channel to VPC peer switch member authentication.

No command removes a port-channel from VPC.

vpc *id*

no vpc *id*

Parameters

id	Enter the VPC domain configuration mode.

Default

The default is None.

Command Mode

LAG Interface

5-390 show running-config vpc

Display running configuration information for virtual port channels (VPC).

show running-config vpc

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Switching)#show running-config vpc

feature vpc
vpc domain 1
role priority 120
system-mac 00:10:18:82:1A:A0
system-priority 32767
peer-keepalive destination 1.1.1.1 source 1.1.1.2
peer detection interval 2000 timeout 6000
```

5-391 show vpc

Display information about a VPC. The configuration and operational modes of the VPC are displayed. Once all preconditions are met, the VPC is operationally enabled.

show vpc *id*

Parameters

id	Display VPC keepalive status and parameters.

Default

The default is None.

Command Mode

User EXEC

Example

The following is a command example.

```
(Switching)#show vpc 10

VPC id#10
---------------
Config mode..................................... Enabled
Operational mode................................ Enabled
Port channel.................................... 3/1

Local Members        Status
-----------------    ----------
0/2                  UP
0/6                  DOWN

Peer members         Status
-----------------    ----------
0/8                  UP
```

5-392 show vpc brief

Display the VPC global status and current VPC operational mode. In addition, peerlink and keepalive status including the number of configured and operational VPCs, and system MAC and roles are also displayed.

show vpc brief

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Switching)#show vpc brief
```

```
VPC config Mode................................ Enabled
Keepalive config mode.......................... Enabled
VPC operational Mode........................... Enabled
Self Role...................................... Primary
Peer Role...................................... Secondary
Peer detection................................. Disabled

Peer-Link details
--------------------
Interface...................................... 3/2
Peer link status............................... UP
Peer-link STP Mode............................. Disabled
Configured Vlans............................... 1
Egress tagging................................. none

VPC Details
--------------------
Number of VPCs configured...................... 1
Number of VPCs operational..................... 1

VPC id# 1
--------------------
Interface...................................... 3/1
Configured Vlans............................... 1
VPC Interface State............................ Active

Local MemberPorts    Status
-----------------    ----------
0/19                 UP
0/20                 UP
0/21                 UP
0/22                 UP

Peer MemberPorts     Status
-----------------    ----------
0/27                 UP
0/28                 UP
0/29                 UP
0/30                 UP
```

5-393 show vpc consistency-parameters

Display global and LAG interface consistency parameters for virtual port channels (VPC).

show vpc consistency-parameters {global | interface *id***}**

Parameters

global	Display VPC global consistency parameters.
interface *id*	Display VPC consistency parameters of a lag interface.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Switch)#show vpc consistency-parameters global

Parameter
Name                        Value
--------------------        --------------------
STP Mode                    Enabled
STP Version                 IEEE 802.1s
BPDU Filter Mode            Enabled
BPDU Guard Mode             Enabled
MST Instances               1,2,4
FDB Aging Time              300 seconds
VPC system MAC address      <AA:BB:CC:DD:EE:FF>
VPC system priority         32767
VPC Domian ID               1
MST VLAN Configuration

Instance     Associated VLANS
----------   --------------------
7,8,10,20
2               4,5,40-50
4               30,32,34-38

PV(R)STP Configuration:

PV(R)STP Mode                           Enabled/Disabled
PV(R)STP Version                        PVST/Rapid-PVST
FastUplinkfast                          Enabled/Disabled
FastUpLinkfast max-update-rate          <0-32000>
FastBackbone                            Enabled/Disabled

VLAN    Mode       STP Root   Hello Time   Forward Time    MaximumAge Time    Priority
-----   --------   ---------  ----------   -------------   ---------------    ---------
4       Enabled    Primary    2            15              15                 0
```

```
(Switch)#show vpc consistency-parameters interface lag 2
```

```
Parameter
Name                          Value
--------------------          --------------------
Port Channel Mode             Enabled
STP Mode                      Enabled
BPDU Filter Mode              Enabled
BPDU Flood Mode               Enabled
Auto-edge                     FALSE
TCN Guard                     True
Port Cost                     2
Edge Port                     True
Root Guard                    True
Loop Guard                    True
Hash Mode                     3
Minimum Links                 1
Channel Type                  Static
Configured VLANs              4,5,7,8
MTU                           1518

Active Port     Speed         Duplex
------------    --------      --------
0/1             100           Full
0/2             100           Full

MST VLAN Configuration

Instance     Associated VLANS
----------   --------------------
1            7,8
2            4,5

PV(R)STP Configuration:
STP port-priority   <0-240>

VLAN    port-priority      cost
-----   ---------------    ----------
<ID>    <0-240>            auto | <1- 200000000>
```

5-394 show vpc peer-keepalive

Display the peer VPC switch IP address used by the dual control plane detection protocol. In addition, the command displays enabled peer detection. If enabled, the detection status displays. The DCPDP message transmission interval and reception timeout are also displayed.

show vpc peer-keepalive

Parameters

None

Default

The default is None.

Command Mode

User EXEC

Example

The following is a command example.

```
(Switching)#show vpc peer-keepalive

Peer IP address.................................. 10.130.14.55
Source IP address................................ 10.130.14.55
UDP port......................................... 50000
Peer detection admin status...................... Enabled
Peer detection operational status................ Down
Peer is detected................................. True
Configured Tx interval........................... 1000 milliseconds
Configured Rx timeout............................ 3500 milliseconds
Operational Tx interval.......................... 500 milliseconds
Operational Rx timeout........................... 2000 milliseconds
```

5-395 show vpc role

Displays keepalive status and parameter information. The role of the VPC switch as well as the system MAC address and priority are displayed.

show vpc role

Parameters

None

Default

The default is None.

Command Mode

User EXEC

Example

The following is a command example.

```
(Switching)#show vpc role

Self
```

```
----------
VPC domain ID..................................... 1
Keepalive config mode............................. Enabled
Keepalive operational mode........................ Enabled
Role Priority..................................... 100
Configured VPC MAC................................ AA:BB:CC:DD:EE:FF>
Operational VPC MAC............................... AA:BB:CC:DD:EE:FF>
Configured VPC system priority.................... 32767
Operational VPC system priority................... 32767
Local System MAC.................................. 00:10:18:82:18:63
Timeout........................................... 5
VPC State......................................... Primary
VPC Role.......................................... Primary

Peer
----------
VPC Domain ID..................................... 1
Role Priority..................................... 100
Configured VPC MAC................................ AA:BB:CC:DD:EE:FF>
Operational VPC MAC............................... AA:BB:CC:DD:EE:FF>
Configured VPC system priority.................... 32767
Operational VPC system priority................... 32767
Role.............................................. Secondary
Local System MAC.................................. 00:10:18:82:1b:ab
```

5-396 show vpc statistics

Display keepalive message counters transmitted and received by the VPC switch.

show vpc statistics {peer-keepalive | peer-link}

Parameters

peer-keepalive	Display VPC peer keepalive statistics.
peer-link	Display VPC peer link statistics.

Default

The default is None.

Command Mode

User EXEC

Example

The following is a command example.

```
(Switching)#show vpc statistics peer-keepalive
```

```
Total transmitted.............................. 123
Tx successful.................................. 118
Tx errors...................................... 5
Total received................................. 115
Rx successful.................................. 108
Rx Errors...................................... 7
Timeout counter................................ 6
```

The following shows examples of the command.

```
(Switching)#show vpc statistics peer-link

Peer link control messages transmitted........... 123
Peer link control messages Tx errors............. 5
Peer link control messages Tx timeout............ 4
Peer link control messages ACK transmitted....... 34
Peer link control messages ACK TX erorrs......... 5
Peer link control messages received.............. 115
Peer link data messages transmitted.............. 123
Peer link data messages Tx errors................ 5
Peer link data messages Tx imeout................ 4
Peer link data messages ACK transmitted.......... 34
Peer link data messages ACK Tx erorrs............ 5
Peer link data messages received................. 115
Peer link BPDU’s tranmsitted to peer............. 123
Peer link BPDU’s Tx error........................ 9
Peer link BPDU’s received from peer.............. 143
Peer link BPDU’s Rx error........................ 1
Peer link LACPDU’s tranmsitted to peer........... 123
Peer link LACPDU’s Tx error...................... 9
Peer link LACPDU’s received from peer............ 143
Peer link LACPDU’s Rx error...................... 1
```

5-397 clear vpc statistics

Clear all the keepalive statistics.

clear vpc statistics {peer-keepalive | peer-link}

Parameters

peer-keepalive	Clears all VPC peer-keepalive statistics.
peer-link	Clears all VPC peer link statistics.

Default

The default is None.

Command Mode

User EXEC

Example

The following is a command example.

```
(Switching)#clear vpc statistics peer-keepalive

(Switching)#clear vpc statistics peer-link
```

5-398 debug vpc peer-keepalive

Enable debug traces of the keepalive state machine transitions.

debug vpc peer-keepalive

Parameters

None

Default

The default is None.

Command Mode

User EXEC

5-399 debug vpc peer-link data-message

Enable debug traces for the control messages exchanged between the VPC devices on the peer link.

debug vpc peer-link data-message

Parameters

None

Default

The default is None.

Command Mode

User EXEC

5-400 debug vpc peer-link control-message async

Enable debug traces for the asynchronous reliable control messages exchanged between the MLAG devices on the peer link. For **error**, only the communication errors are traced. Exchanged control messages can be traced through msg.

debug vpc peer-link control-message async {error | msg [receive | transmit] | normal | verbose}

Parameters

error	Error Tracing Level.
msg receive	(Optional) Trace Messages exchanged.
normal	(Optional) Normal Tracing Level.
verbose	Verbose Tracing Level.

Default

The default is None.

Command Mode

User EXEC

5-401 debug vpc peer-link control-message bulk

Enable debug traces for the periodic control messages exchanged between the MLAG devices on the peer link. . For **error**, only the communication errors are traced. Exchanged control messages can be traced through msg.

debug vpc peer-link control-message bulk { error | msg | receive [receive | transmit] | normal | verbose }

Parameters

error	Error Tracing Level.
msg receive	(Optional) Trace Messages exchanged.
receive	Enter trace Received Messages.
transmist	Enter trace Transmitted Messages.
normal	(Optional) Normal Tracing Level.
verbose	Verbose Tracing Level.

Default

The default is None.

Command Mode

User EXEC

5-402 debug vpc peer-link control-message ckpt

Enable debug traces for the checkpointing control messages exchanged between the MLAG devices on the peer link. . For **error**, only the communication errors are traced. Exchanged control messages can be traced through msg.

debug vpc peer-link control-message ckpt {error | msg [receive | transmit] | normal | verbose }

Parameters

error	Error Tracing Level.
msg	(Optional) Trace Messages exchanged.
receive	Enter trace Received Messages.
transmist	Enter trace Transmitted Messages.
normal	(Optional) Normal Tracing Level.
verbose	Verbose Tracing Level.

Default

The default is None.

Command Mode

User EXEC

5-403 debug vpc peer detection

Enable debug traces for the dual control plane detection protocol. Traces are available when the DCPDP transmits or receives detection packets to or from the peer VPC switch.

debug vpc peer detection

Parameters

None

Default

The default is None.

Command Mode

User EXEC

Port Mirroring

Port mirroring (port monitoring) selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

5-404 monitor session source

Configure the source interface for a selected monitor session. Use the **source interface** *slot/port* parameter to specify the interface to monitor. **Rx** monitors only ingress packets while **tx** monitors only egress packets. If **{rx | tx}** options are not specified, the destination port monitors both ingress and egress packets.

Note: The source and destination cannot be configured as remote on the same device.

Note: If an interface is configured as a VLAN and is a LAG member, the VLAN cannot be designated as a source VLAN for a Monitor session. In the same manner, if an interface is configured in a VLAN and assigned as a source VLAN for a monitor session, the interface can be designated as a LAG member.

No command removes the specified mirrored port from the selected port mirroring session.

monitor session *session-id* **source {interface {***slot/port* **| cpu | lag } | vlan** *vlan-id* **| remote vlan** *vlan-id***} [{rx | tx}]**

no monitor session *session-id* **source {interface {***slot/port* **| cpu | lag } | vlan | remote vlan}**

Parameters

session-id	Indicates the session number.
slot/port	Enter an interface in slot/port format.
cpu	Monitor CPU port packets.
lag	Configure interface.
vlan *vlan-id*	Configure monitoring on the VLAN.
remote vlan *vlan-id*	Configure source as remote.
rx	(Optional) Select to monitor only ingress packets.
tx	(Optional) Select to monitor only egress packets.

Default

The default is None.

Command Mode

Global Config

5-405 monitor session destination

Configures the probe interface for a selected monitor session. This command configures a probe port and a monitored port for monitor session (port monitoring). R**x** monitors only ingress packets, while **tx** monitors only egress packets. If not specified **{rx | tx}**, the destination port monitors both ingress and egress packets.

Note: The source and destination cannot be configured as remote on the same device.

The **reflector-port** is configured at the source switch along with the destination RSPAN VLAN. The **reflector-port** forwards the mirrored traffic towards the destination switch.

Note: This port must be configured with RSPAN VLAN membership.

To receive monitored traffic, configure the destination interface slot/port to specify the interface.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

Note: If an interface is configured as a VLAN and is a LAG member, the VLAN cannot be designated as a source VLAN for a Monitor session. In the same manner, , if an interface is configured in a VLAN and assigned as a source VLAN for a monitor session, the interface can designated as a LAG member.

No command removes the specified probe port from the selected port mirroring session.

monitor session *session-id* **destination {interface** *slot/port* **| remote vlan** *vlan-id* **reflector-port** *slot/port***}**

no monitor session *session-id* **destination {interface** *slot/port* **| remote vlan** *vlan-id* **reflector-port** *slot/port***}**

Parameters

session-id	Indicates the session number.
interface *slot/port*	Enter an interface in slot/port format.
remote vlan *vlan-id*	Enter VLAN ID.
reflector-port *slot/port*	Configure the reflector port.

Default

The default is None.

Command Mode

Global Config

5-406 monitor session filter

Attach an IP/MAC ACL to a selected monitor session to configure a probe port and a monitored port for monitor session (port monitoring).

An IP/MAC ACL can be attached to a session by giving the access list number/name.

Filtering for a specified access group by IP address or MAC address is also available through the command.

Note: Source and destination cannot be configured as a remote on the same device.

Note: IP/MAC ACL can be attached to a session by providing designated list number/name access. Platforms not supporting both IP and MAC ACLs assignment on the same Monitor session, an error displays during ACL configuration.

No command removes the specified IP/MAC ACL from the selected monitoring session.

monitor session *session-id* **filter {ip access-group** *acl-id/aclname* **| mac access-group** *acl-name***}**

no monitor session session-id filter {ip access-group | mac access-group}

Parameters

session-id	Indicates the session number.
ip access-group *acl-id/aclname*	Indicates the IP ACL include in the access group list. Enter an integer specifying an IP ACL number.
mac access-group *acl-name*	Indicates the MAC ACL to include in the access group list.
Ip-acl-name *acl-name*	Enter access-list name up to 31 characters in length.

Default

The default is None.

Command Mode

Global Config

5-407 monitor session mode

Enable the selected port mirroring session to configure a probe and monitored port for monitor session (port monitoring).

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured through RSPAN VLAN ID. On the source switch, the destination can be configured as the RSPAN VLAN. On a destination switch, the source is configured as the RSPAN VLAN.

Note: The source and destination cannot be configured as remote on the same device.

The commands described below add a mirrored port (source port) to a session--identified by *session-id*. The *session-id* parameter is an integer value used to identify the session. The maximum number of sessions that can be configured stated as L7_MIRRORING_MAX_SESSIONS.

R**x** monitors only ingress packets, while **tx** monitors only egress packets. If not specified **{rx | tx}**, the destination port monitors both ingress and egress packets.

Note: Interfaces participating in VLAN and also LAG members, the VLAN cannot be assigned as a source VLAN for a Monitor session.

Remote port mirroring is configured through the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

Note: Source and destination cannot be configured as a remote on the same device.

No command disables the selected port mirroring session.

monitor session *session-id* **mode**

no monitor session *session-id* **mode**

Parameters

session-id	Indicates the session ID number (1 – 4).

Default

The default is None.

Command Mode

Global Config

5-408 no monitor session

Configure the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once removed from the VLAN, a port must be added manually to the desired VLAN. Use the **source interface** *slot/port* parameter or **destination interface** to remove the specified interface from the port monitoring session. Use the **mode** parameter to disable the administrative mode of the session.

no monitor session *session-id* **{ destination[interface** *slot/port***] | remote vlan} | filter {ip | mac } | mode | source }**

Parameters

session-id	Indicates the session number (1 – 4).
destination	Configure the probe interface.
interface *slot/port*	Enter an interface in slot/port format.
remote	Configure source as remote.
vlan	Configure monitoring on the VLAN.
Filter *ip / mac*	Configure filter.
mode	Enable/Disable port mirroring session.
source	Configure the source interface.

Default

The default is None.

Command Mode

Global Config

5-409 no monitor

Removes all the source and destination ports and restores the default for mirroring session mode for all the configured sessions.

no monitor

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

5-410 remote-span

Identified the VLAN as the RSPAN VLAN.

No command clears the RSPAN information for the VLAN.

remote-span

no remote-span

Parameters

None

Default

The default is None.

Command Mode

VLAN Config

5-411 show monitor session

Display the Port monitoring information for a particular mirroring session.

Note: The *session-id* parameter is depicted by an integer value, the *session-id* parameter is always one (1).

show monitor {session *session-id* **| all}**

Parameters

session *session-id*	Indicates the session ID number.
all	Show all sessions.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Switch)#show monitor session 1

Session   Admin   Probe   Src     Mirrored   Ref     Src     Dst     Type    IP    MAC
ID        Mode    Port    VLAN    Port       Port    RVLAN   RVLAN           ACL   ACL
--------  ------  ------  ------  ---------  ------  ------  ------  -----   ----  -----
1         Enable  0/8             0/10                               Rx,Tx
```

```
(Switch)#show monitor session all

Session   Admin   Probe   Src     Mirrored   Ref     Src     Dst     Type    IP    MAC
ID        Mode    Port    VLAN    Port       Port    RVLAN   RVLAN           ACL   ACL
--------  ------  ------  ------  ---------  ------  ------  ------  -----   ----  -----
1         Enable  0/8             0/10                               Rx,Tx
2         Disable         6                  0/4             10              4
3         Disable 0/11                                       10                    101
4         Enable  0/11            0/7                                Tx
```

```
(Switch)#show monitor session all

Session   Admin   Probe   Src     Mirrored   Ref     Src     Dst     Type    IP    MAC
ID        Mode    Port    VLAN    Port       Port    RVLAN   RVLAN           ACL   ACL
--------  ------  ------  ------  ---------  ------  ------  ------  -----   ----  -----
1         Enable  0/8             0/10                               Rx
2         Enable          6                                          Rx      4
3         Disable         10                                         Tx            101
4         Disable 0/11            0/7                                Tx
```

```
(Switch)#show monitor session all

Session   Admin   Probe   Src     Mirrored   Ref     Src     Dst     Type    IP    MAC
ID        Mode    Port    VLAN    Port       Port    RVLAN   RVLAN           ACL   ACL
--------  ------  ------  ------  ---------  ------  ------  ------  -----   ----  -----
1         Enable                  0/15       0/4             11      Tx      4
2         Enable  0/3             0/15                               Tx
3         Enable                  0/15       0/20            10      Rx
4         Enable  0/11            0/15                               Rx            10
```

```
(Switch)#show monitor session all

Session   Admin   Probe   Src     Mirrored   Ref     Src     Dst     Type    IP    MAC
ID        Mode    Port    VLAN    Port       Port    RVLAN   RVLAN           ACL   ACL
--------  ------  ------  ------  ---------  ------  ------  ------  -----   ----  -----
1         Disable
2         Disable
3         Enable  0/16    3
4         Enable  0/11            0/16                               Rx,Tx         10
```

```
(Switch)#show monitor session all

Session   Admin   Probe   Src     Mirrored   Ref     Src     Dst     Type    IP    MAC
ID        Mode    Port    VLAN    Port       Port    RVLAN   RVLAN           ACL   ACL
--------  ------  ------  ------  ---------  ------  ------  ------  -----   ----  -----
1         Enable          1                  0/4             15              4
2         Enable  0/15    2
3         Enable          3                  0/20            10
4         Enable  0/11            0/16                               Rx,Tx         10
```

Display Parameters

Session ID	Integer identifying the session.
Admin Mode	Indicates Port Mirroring status: enabled or disabled for the session identified with session-id.
Probe Port	Identified probe port (destination port) for the session-id.
Src VLAN	Indicates mirrored status of all member ports
Mirrored Port	Identifies configured port as a mirrored (source port) for the session identified with session-id.
Ref. Port	Identifies the port carrying all the mirrored traffic at the source switch.
Src RVLAN	The configured source VLAN for the destination switch.
Dst RVLAN	Identifies the configured destination VLAN for the source switch.
Type	The configured direction of the source port for mirroring.
IP ACL	The IP access-list ID or name attached to the port mirroring session.

MAC ACL	The MAC access-list name attached to the port mirroring session.

5-412 show vlan remote-span

Display the configured RSPAN VLAN.

show vlan remote-span

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an output example.

```
(Switch)#show vlan remote-span

Remote SPAN VLAN
----------------------------------------------------
100,102,201,303
```

Static MAC Filtering

This section describes static MAC filtering configuration. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

5-413 macfilter

Add a static MAC filter entry for the *macaddr* (MAC address) on the VLAN *vlanid*. The value of the *macaddr* parameter is defined as a 6-byte hexadecimal number with the following format b1:b2:b3:b4:b5:b6. The following are restricted MAC Addresses: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The *vlanid* parameter must identify a valid VLAN.

For current platforms, the following configurations are supported:

- Unicast MAC and source port
- Multicast MAC and source port
- Multicast MAC and destination port (only)

- Multicast MAC and source ports and destination ports

No command removes all filtering restriction and the static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

macfilter *macaddr vlanid*

no macfilter *macaddr vlanid*

Parameters

macaddr	Indicates the MAC address.
vlanid	Enter a VLAN ID. (1-4093)

Default

The default is None.

Command Mode

Global Config

5-414 macfilter adddest

Add a single or range of interfaces to the destination filter with *macaddr* (MAC filter) and *vlanid* (VLAN). The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

No command removes a port from the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

macfilter adddest *macaddr vlanid*

no macfilter adddest *macaddr vlanid*

Parameters

macaddr	Enter MAC address.
vlanid	Enter a VLAN ID (1-4093).

Default

The default is None.

Command Mode

Interface Config

5-415 macfilter adddest all

Add all interfaces to the destination filter with *macaddr* (MAC filter) and *vlanid* (VLAN). The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify as a valid VLAN.

No command removes all ports defined by *macaddr* and *vlanid* from the destination filter. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify as a valid VLAN.

macfilter adddest all *macaddr vlanid*

no macfilter adddest all *macaddr vlanid*

Parameters

macaddr	Enter MAC address.
vlanid	Enter a VLAN ID (1-4093).

Default

The default is None.

Command Mode

Global Config

5-416 macfilter addsrc

Add a single or range of interfaces to the source destination filter with *macaddr* (MAC filter) and *vlanid* (VLAN).. The *macaddr* parameter is defined by a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify as a valid VLAN.

No command removes a port from the source destination filter with *macaddr* (MAC filter) and *vlanid* (VLAN).. The *macaddr* parameter is defined by a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify as a valid VLAN.

macfilter addsrc *macaddr vlanid*

no macfilter addsrc *macaddr vlanid*

Parameters

macaddr	Enter MAC address.

vlanid	Enter a VLAN ID (1-4093).

Default

The default is None.

Command Mode

Interface Config

5-417 macfilter addsrc all

Add all interfaces using *macaddr* and *vlanid* to the source filter. The *macaddr* parameter must be defined as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must be identified as a valid VLAN.

No command removes all interfaces from the source filter as set by the MAC filter using the MAC address (*macaddr*) and VLAN (*vlanid*). You must specify the *macaddr* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

macfilter addsrc all *macaddr vlanid*

no macfilter addsrc all *macaddr vlanid*

Parameters

macaddr	Enter MAC address.
vlanid	Enter a VLAN ID (1-4093).

Default

The default is None.

Command Mode

Global Config

5-418 show mac-address-table static

Display the Static MAC Filtering information for all Static MAC Filters. By specifying **all**, all Static MAC Filters in the system are displayed. Both *macaddr* and *vlanid* require a specified value for the system to display Static MAC Filter information only for that MAC address and VLAN.

Note: Only multicast address filters have destination port lists.

show mac-address-table static {*macaddr vlanid* **| all}**

Parameters

macaddr	Enter MAC address.
vlanid	Enter a VLAN ID (1-4093).
all	Enter all for all Static MAC Filter entries.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)(Interface 0/2)#show mac-address-table static all

MAC Address             VLAN ID      Source Port(s)     Destination Port(s)
--------------------    ----------   ---------------    --------------------
01:00:5E:00:00:01       1                               0/1
01:00:5E:00:00:02       1            0/2
AA:BB:CC:DD:EE:FF       1
```

Display Parameters

MAC Address	The static MAC filter entry address.
VLAN ID	The static MAC filter entry VLAN ID.
Source Port(s)	Displays the defined slot and port(s) for the source port filter sets.
Destination Port(s)	Displays the defined slot and port(s) for the destination port for this rule.

5-419 show mac-address-table staticfiltering

Display the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

show mac-address-table staticfiltering

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)#show mac-address-table staticfiltering

VLAN ID    MAC Address                 Type          Description     Interfaces
--------   -------------------------   ----------    ----------      ---------------
           00:01:01:00:5E:00:00:01     Static        Mgmt Config     Fwd: 0/1
           00:01:01:00:5E:00:00:02     Static        Mgmt Config
```

Display Parameters

VLAN ID	The identifier for the VLAN for obtaining the MAC address.
MAC Address	The unicast MAC address designated for forwarding and or filtering information. The format is identified as 6 two-digit hexadecimal numbers separated by colons.
Type	Describes the type of entry: Static or Dynamic. Static entries are configured by the end user, while dynamic entries are added to the table as a result of a learned process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces designated for forwarding (Fwd:) and filtering (Flt:).

DHCP L2 Relay Agent Commands

Enable operation as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server.

5-420 dhcp l2relay

Enable the DHCP Layer 2 Relay agent for a single or interface a range of interfaces in, or all interfaces. The function is only available if the DHCP L2 relay is enabled.

No command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

dhcp l2relay

no dhcp l2relay

Parameters

None

Default

The default is None.

Command Mode

- Global Config
- Interface Config

5-421 dhcp l2relay trust

Configure a single or range of interfaces as trusted for Option-82 reception.

No command configures an interface to default (untrusted for Option-82 reception).

dhcp l2relay trust

no dhcp l2relay trust

Parameters

None

Default

The default is Untrusted.

Command Mode

Interface Config

5-422 show dhcp l2relay all

Display the DHCP L2 Relay configuration summary.

show dhcp l2relay all

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Switching)#show dhcp l2relay all

DHCP L2 Relay is Enabled.

Interface    L2RelayMode     TrustMode
----------   ------------    ------------
0/1          Enabled         untrusted
0/2          Enabled         untrusted
0/4          Disabled        trusted
…
3/64         Enabled         untrusted

VLAN Id      L2 Relay     CircuitId    RemoteId
----------   ----------   ----------   ----------
```

5-423 show dhcp l2relay circuit-id vlan

Display DHCP circuit-id vlan configuration.

show dhcp l2relay circuit-id vlan *vlan-list*

Parameters

vlan-list	Enter a VLAN ID identifier, range: 1-4093. A dash (-)specifies a range while a comma (,)separates VLAN IDs within a list.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)#show dhcp l2relay circuit-id vlan 1

DHCP L2 Relay is  Enabled.

DHCP Circuit-Id option is enabled on the following VLANs:
1
```

5-424 show dhcp l2relay interface

Displays DHCP L2 relay configuration specific to interfaces.

show dhcp l2relay interface {all | *slot/port***}**

Parameters

all	Display DHCP L2 Relay configuration for all interfaces.
slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Switching)#show dhcp l2relay interface all

DHCP L2 Relay is Enabled.

Interface     L2RelayMode   TrustMode
----------    ------------ ----------
0/2           Enabled      untrusted
0/4           Disabled     trusted
```

5-425 show dhcp l2relay remote-id vlan

Displays DHCP Remote-id vlan configuration.

show dhcp l2relay remote-id vlan *vlan-list*

Parameters

vlan-list	Enter VLAN ID identifiers, range: 1 to 4093. A dash (-) specifies a range while a comma (,) separates VLAN IDs within a list.

Default

The default is None.

Command Mode

Privileged EXEC

5-426 show dhcp l2relay stats interface

Display statistics specific to DHCP L2 Relay configured interface.

show dhcp l2relay stats interface {all | *slot/port***}**

Parameters

all	Display DHCP L2 Relay statistics for all interfaces.
slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Switching)#show dhcp l2relay stats interface all

DHCP L2 Relay is Enabled.

Interface    UntrustedServer      UntrustedClient    TrustedServer      TrustedClient
             MsgsWithOpt82        MsgsWithOpt82      MsgsWithOpt82      MsgsWithOpt82
----------   ---------------      ---------------    ---------------    ---------------
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
0/10         0                    0                  0                  0
```

5-427 show dhcp l2relay agent-option vlan

Display the DHCP L2 Relay Option-82 configuration for a specific VLAN.

show dhcp l2relay agent-option vlan *vlan-range*

Parameters

vlan-range	Display configuration for DHCP circuit-id VLAN range.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Switching)#show dhcp l2relay agent-option vlan 5-10

DHCP L2 Relay is Enabled.

VLAN Id      L2 Relay     Circuitld       RemoteID
----------   ----------   ----------      ---------------
5            Enabled      Enabled         --NULL--
6            Enabled      Enabled         --NULL--
7            Enabled      Disabled        --NULL--
8            Enabled      Disabled        --NULL--
9            Enabled      Disabled        --NULL--
10           Enabled      Disabled        --NULL--
```

5-428 show dhcp l2relay vlan

Displays DHCP vlan configuration.

show dhcp l2relay vlan *vlan-list*

Parameters

vlan-list	Enter VLAN ID identifier, range: 1 to 4093. A dash (-)specifies a range while a comma (,)separates VLAN IDs within a list.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)#show dhcp l2relay vlan 2
```

```
DHCP L2 Relay is  Enabled.

DHCP L2 Relay is enabled on the following VLANs:
2
```

5-429 clear dhcp l2relay statistics interface

Reset the DHCP L2 relay counters to zero. Specify a single or all port counters to clear.

clear dhcp l2relay statistics interface {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Clears DHCP L2 Relay statistics for all enabled interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

DHCP Client Commands

5-430 dhcp client vendor-id-option

Enable the inclusion of DHCP Option-60 and Vendor Class Identifier in the DHCP server transmitted requests.

No command disables the inclusion of DHCP Option-60 and Vendor Class Identifier in DHCP server.

dhcp client vendor-id-option *string*

no dhcp client vendor-id-option

Parameters

string	Vendor-id suboption string of length <0 - 128> characters.

Default

The default is None.

Command Mode

Global Config

5-431 dhcp client vendor-id-option-string

Set the DHCP Vendor Option-60 string to include requests transmitted to the DHCP server by the DHCP client.

No command clears DHCP Vendor Option-60 string.

dhcp client vendor-id-option-string *string*

no dhcp client vendor-id-option-string

Parameters

string	Vendor-id suboption string of length <0 - 128> characters.

Default

The default is None.

Command Mode

Global Config

5-432 show dhcp client vendor-id-option

Display the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in DHCP requests.

show dhcp client vendor-id-option

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Switching)#show dhcp client vendor-id-option
```

```
DHCP Client Vendor Identifier Option.............. Enabled
DHCP Client Vendor Identifier Option String...... D-LINK OSClient.
```

DHCP Snooping Configuration Commands

This section describes DHCP Snooping configuration.

5-433 ip dhcp snooping

Enable DHCP Snooping globally.

No command to disable DHCP Snooping globally.

ip dhcp snooping

no ip dhcp snooping

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-434 ip dhcp snooping vlan

Enable DHCP Snooping on a list of comma-separated VLAN ranges.

No command disables DHCP Snooping on VLANs.

ip dhcp snooping vlan *vlan-list*

no ip dhcp snooping vlan *vlan-list*

Parameters

vlan-list	Indicates the VLAN list or list range.

Default

The default is Disabled.

Command Mode

Global Config

5-435 ip dhcp snooping verify mac-address

Enable verification of the source MAC address with the client hardware address in the received DCHP message.

No command disables verification of the source MAC address with the client hardware address.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

5-436 ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

ip dhcp snooping database {local | tftp://hostIP/filename | write delay}

Parameters

local	Configure DHCP snooping binding URL in the form local.
tftp://hostIP/filename	Configure DHCP snooping binding URL in the form tftp://host/filename.
write delay	Configure DHCP snooping bindings store interval in <15> to <86400> seconds range.

Default

The default is Local.

Command Mode

Global Config

5-437 ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

Use the **no** command to set the write delay value to the default value.

ip dhcp snooping database write-delay *15-86400*

no ip dhcp snooping database write-delay

Parameters

None.

Default

The default is 300 seconds.

Command Mode

Global Config

5-438 ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Use the **no** command to remove the DHCP static entry from the DHCP Snooping database.

ip dhcp snooping binding *mac-address* **vlan** *vlan-id ip address* **interface** *interface-id*

no ip dhcp snooping binding *mac-address* **vlan** *vlan-id ip address* **interface** *interface-id*

Parameters

mac-address	Enter MAC address.
vlan *vlan-id*	Indicates the VLAN ID.
ip address	Indicates the IP address for the location.
interface *interface-id*	Indicates the interface to specify.

Default

The default is None.

Command Mode

Global Config

5-439 ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Use the **no** command to remove the IPSG static entry from the IPSG database.

ip verify binding *mac-address* **vlan** *vlan-id ip address* **interface** *interface-id*

no ip verify binding *mac-address* **vlan** *vlan-id ip address* **interface** *interface-id*

Parameters

mac-address	Enter MAC address.
vlan *vlan-id*	Indicates the VLAN ID.
ip address	Indicates the IP address for the location.
interface *interface-id*	Indicates the interface to specify.

Default

The default is None.

Command Mode

Global Config

5-440 ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second. The burst level range is 1 to 15 seconds.

Use the **no** command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

ip dhcp snooping limit {rate *pps* **[burst interval** *seconds***]}**

no ip dhcp snooping limit

Parameters

pps	Enter rate in the range <0-300> pps.
seconds	(Optional) Enter burst interval in the range <1-15> seconds.

Default

The default is Disabled (no limit).

Command Mode

Interface Config

5-441 ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Use the **no** command to disable the logging DHCP messages filtration by the DHCP Snooping application.

ip dhcp snooping log-invalid

no ip dhcp snooping log-invalid

Parameters

None.

Default

The default is Disabled.

Command Mode

Interface Config

5-442 ip dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Use the **no** command to configure the port as untrusted.

ip dhcp snooping trust

no ip dhcp snooping trust

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-443 ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the “port-security” option, the data traffic will be filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

Use the **no** command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

ip verify source {port-security}

no ip verify source

Parameters

port-security	Filter incoming packets by source MAC address.

Default

The default is None.

Command Mode

Interface Config

5-444 show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

show ip dhcp snooping

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip dhcp snooping
```

```
DHCP snooping is Enabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40

Interface    Trusted      Log Invalid Pkts
----------   ----------   ---------------
0/1          Yes          No
0/2          No           Yes
0/3          No           Yes
0/4          No           No
```

Display Parameters

Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP Snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP Snooping application logs invalid packets on the specified interface.

5-445 show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

show ip dhcp snooping binding [{static | dynamic}] [interface *slot/port***] [vlan** *id***]**

Parameters

static	(Optional) Restrict the output based on static entries.
dynamic	(Optional) Restrict the output based on DHCP snooping.
interface *slot/port*	(Optional) Restrict the output based on a specific interface.
vlan *id*	(Optional) Restrict the output based on VLAN.

Default

The default is None.

Command Mode

- Privileged EXEC

- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip dhcp snooping binding

Total number of bindings: 2

MAC Address         IP Address    VLAN   Interface     Type   Lease time (Secs)
------------------- ------------ -----  ------------ -----  --------------------
00:02:B3:06:60:80   210.1.1.3     10     0/1                 86400
00:0F:FE:00:13:04   210.1.1.4     10     0/1                 86400
```

Display Parameters

MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IP Address	Displays the valid IP address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease time (sec)	The remaining lease time for the entry.

5-446 show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

show ip dhcp snooping database

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip dhcp snooping database
```

```
agent url:    /10.131.13.79:/sai1.txt

write-delay: 5000
```

Display Parameters

Agent URL	Bindings database agent URL.
Write Delay	The maximum waiting period in seconds before writing to the DHCP Snooping database. The value range: 15 – 86400 seconds (default: 300).

5-447 show ip dhcp snooping interfaces

Use this command to show the DHCP Snooping status of the interfaces.

show ip dhcp snooping interfaces

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip dhcp snooping interfaces

Interface     Trust State   Rate Limit (pps)    Burst Interval (seconds)
----------    ------------  -----------------   -------------------------------
0/1           No            15                  1
0/2           No            15                  1
0/3           No            15                  1

(Routing)#show ip dhcp snooping interfaces ethernet 0/15

Interface     Trust State   Rate Limit (pps)    Burst Interval (seconds)
----------    ------------  -----------------   -------------------------------
0/15          Yes           15                  1
```

5-448 show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

show ip dhcp snooping statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip dhcp snooping statistics

Interface    MAC Verify Failures     Client Ifc Mismatch     DHCP Server Msgs Rec'd
----------   --------------------    --------------------    --------------------------
0/2          0                       0                       0
0/3          0                       0                       0
0/4          0                       0                       0
0/5          0                       0                       0
0/6          0                       0                       0
0/7          0                       0                       0
0/8          0                       0                       0
0/9          0                       0                       0
0/10         0                       0                       0
0/11         0                       0                       0
0/12         0                       0                       0
0/13         0                       0                       0
0/14         0                       0                       0
0/15         0                       0                       0
0/16         0                       0                       0
0/17         0                       0                       0
0/18         0                       0                       0
0/19         0                       0                       0
0/20         0                       0                       0
```

Display Parameters

Interface	The IP address identifier for the interface (slot/port).
MAC Verify Failures	Failed message list for MAC and client HW address mismatch.

Client Ifc Mismatch	List of DHCP release and denial messages from varying ports.
DHCP Server Msgs Rec'd	List of DHCP server messages from untrusted ports.

5-449 clear ip dhcp snooping binding

Clear all DHCP Snooping bindings on a single or all interfaces.

clear ip dhcp snooping binding [interface *slot/port***]**

Parameters

interface *slot/port*	(Optional) Restrict clear to a specific interface.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

5-450 clear ip dhcp snooping statistics

Clear all DHCP Snooping statistics.

clear ip dhcp snooping statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

5-451 show ip verify source

Display IPSG configurations on all ports.

show ip verify source

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example.

```
(Routing)#show ip verify source

Interface     Filter Type   IP Address    MAC Address                Vlan
----------    ------------ -----------   --------------------       -----
0/1           ip-mac        210.1.1.3     00:02:B3:06:60:80          10
0/1           ip-mac        210.1.1.4     00:0F:FE:00:13:04          10
```

Display Parameters

Interface	Interface address in slot/port format.
Filter Type	List one of two value types: • ip-mac: User has configured MAC address filtering on this interface. • ip: Only IP address filtering on this interface.
IP Address	IP address of the interface.
MAC Address	Configure MAC address filtering to display the parameter. Disabling port security sets MAC Address to “permit-all” setting.
VLAN	The VLAN for the binding rule.

5-452 show ip verify interface

Display the IPSG filter type for a specific interface.

show ip verify interface *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

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

Interface    Filter Type
----------   ---------------
0/1          N/A
```

Display Parameters

Interface	Interface address identifier (slot/port format)
Filter Type	Two values are available: • ip-mac: User has configured MAC address filtering on this interface. • ip: Only IP address filtering on this interface.

5-453 show ip source binding

Display the IPSG bindings.

show ip source binding [{static | dynamic}] [interface *slot/port***] [vlan** *id***]**

Parameters

static	Restrict the output based on static entries.
dhcp-snooping	Restrict the output based on DHCP snooping.
interface *slot/port*	Restrict the output based on a specific interface.
vlan *id*	Restrict the output based on VLAN.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example.

```
(Routing)#show ip source binding

MAC Address          IP Address   Type              Vlan    Interface
-------------------  ----------   ---------------   -----   ----------
00:00:00:00:00:08    1.2.3.4      dhcp-snooping     2       0/1
00:00:00:00:00:09    1.2.3.4      dhcp-snooping     3       0/1
00:00:00:00:00:0A    1.2.3.4      dhcp-snooping     4       0/1
```

Display Parameters

MAC Address	The MAC address for the added entry.
IP Address	The IP address of the added entry.
Type	Entry type definition, static or dynamic.
VLAN	List entry VLAN identifier.
Interface	IP address identifier (slot/port format).

Dynamic ARP Inspection Commands

The Dynamic ARP Inspection (DAI) feature is designed to reject invalid and malicious ARP packets. The DAI function prevents class of man-in-the-middle attacks.

DAI relies on DHCP snooping, which relies on DHCP message exchanges and builds a binding database of settings ({MAC address, IP address, VLAN, and interface}.

When enabled, the MAC and sender IP addresses of ARP packets not matching entry in the DHCP snooping bindings database are dropped.

5-454 ip arp inspection vlan

Enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

N**o** command disables Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

ip arp inspection vlan *vlan-list*

no ip arp inspection vlan *vlan-list*

Parameters

vlan-list	Enter VLAN IDs in range <1-4093>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Default

The default is Disabled.

Command Mode

Global Config

5-455 ip arp inspection vlan logging

Enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

No command disables logging of invalid ARP packets on a list of comma-separated VLAN ranges.

ip arp inspection vlan *vlan-list* **{logging}**

no ip arp inspection vlan *vlan-list* **{logging}**

Parameters

vlan-list	Enter VLAN IDs in range <1-4093>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.
logging	Enable Logging of invalid ARP packets.

Default

The default is Disabled.

Command Mode

Global Config

5-456 ip arp inspection validate

Enable additional validation checks, such as source-mac validation, destination-mac validation, and ip address validation on the received ARP packets.

The latest command settings override current configuration.

No command disables the additional validation checks on the received ARP packets.

ip arp inspection validate {[src-mac] [dst-mac] [ip]}

no ip arp inspection validate {[src-mac] [dst-mac] [ip]}

Parameters

src-mac	(Optional) Configure Source MAC validation.
dst-mac	(Optional) Configure Destination MAC validation.
ip	(Optional) Configure IP address validation.

Default

The default is Disabled.

Command Mode

Global Config

5-457 ip arp inspection trust

Configure a single or range of interfaces as trusted for Dynamic ARP Inspection.

No command configures an interface as untrusted for Dynamic ARP Inspection.

ip arp inspection trust

no ip arp inspection trust

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-458 ip arp inspection filter

Configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static setting is identified, no matching packets a permit statement are dropped without consulting the DHCP snooping bindings.

No command unconfigures the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

ip arp inspection filter *name* **vlan** *vlan-list* **[static]**

no ip arp inspection filter *name* **vlan** *vlan-list* **[static]**

Parameters

name	Enter arp access-list name <1-31> alphanumeric characters in length.

vlan *vlan-list*	Configure ARP ACL filter for a VLAN List.
static	(Optional) Configure if ARP ACL filter is static on a VLAN.

Default

The default is None.

Command Mode

Global Config

5-459 arp access-list

Create an ARP ACL.

No command deletes a configured ARP ACL.

arp access-list *name*

no arp access-list *name*

Parameters

name	Enter arp access-list name <1-31> alphanumeric characters in length.

Default

The default is None.

Command Mode

Global Config

5-460 permit ip host mac host (ARP Access-list Config)

Configure valid IP and MAC address combination rules used in ARP packet validation.

No command deletes a rule for a valid IP and MAC combination.

permit ip host *sender-ip* **mac host** *sender-mac*

no permit ip host *sender-ip* **mac host** *sender-mac*

Parameters

sender-ip	Enter IP address in the ARP ACL rule.
sender-mac	Enter MAC address in the ARP ACL rule.

Default

The default is None.

Command Mode

ARP Access-list Config

5-461 show ip arp inspection

Display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. To display the global and VLAN configuration the VLAN-list can be designated. The global configuration includes the **source mac validation**, **destination mac validation** and **invalid IP validation** information.

show ip arp inspection [interfaces *slot/port* **| statistics | vlan** *vlan-list***]**

Parameters

interfaces *slot/port*	Display Dynamic ARP Inspection Interface configuration.
statistics	Display Dynamic ARP Inspection Statistics.
vlan *vlan-list*	Display Dynamic ARP Inspection VLAN configuration.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example.

```
(Routing) #show ip arp inspection vlan 10-12

Source Mac Validation             : Disabled
Destination Mac Validation        : Disabled
IP Address Validation             : Disabled

Vlan    Configuration     Log Invalid     ACL Name     Static Flag
-----   ---------------   ------------    ----------   ---------------
10      Enabled           Enabled         H2           Enabled
11      Disabled          Enabled
12      Enabled           Disabled
```

Display Parameters

Source MAC Validation	Displays status of Source MAC Validation of ARP frame: enabled or disabled.
Destination MAC Validation	Displays status of Destination MAC Validation: enabled or disabled.
IP Address Validation	Displays status of IP Address Validation: enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.
Log Invalid	Displays whether logging of invalid ARP packet is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

5-462 show ip arp inspection statistics

Display the statistics of the ARP packets processed by Dynamic ARP Inspection.

show ip arp inspection statistics [vlan *vlan-list***]**

Parameters

vlan *vlan-list*	(Optional) Display Dynamic ARP Inspection Statistics on a VLAN List.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example for the command **show ip arp inspection statistics** which lists the summary of forward and dropped ARP packets on all DAI-enabled VLANs.

```
(Routing)#show ip arp inspection statistics

VLAN   Forwarded    Dropped
-----  ----------   ----------
10     90           14
20     10           3
```

The following is a CLI display output example for the command **show ip arp inspection statistics vlan** *vlan-list*.

```
(Routing)#show ip arp inspection statistics vlan 1
```

```
VLAN    DHCP    ACL     DHCP       ACL        Bad Src    Bad Dest   Invalid
        Drops   Drops   Permits    Permits    MAC        MAC        IP
-----   -----   -----   --------   --------   --------   --------   -------
10      11      1       65         25         1          1          0
20      1       0       8          2          0          1          1
```

Display Parameters

VLAN	The VLAN ID identifier.
Forwarded	The total number of valid ARP packets forwarded through VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped resulting from DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped resulting from ARP ACL rule match failure.
DHCP Permits	The number of packets permitted resulting from DHCP snooping binding database match.
ACL Permits	The number of packets permitted resulting from ARP ACL rule match.
Bad Src MAC	The number of packets dropped resulting from Source MAC validation failure.
Bad Dest MAC	The number of packets dropped resulting from Destination MAC validation failure.
Invalid IP	The number of packets dropped resulting from invalid IP checks.

5-463 clear ip arp inspection statistics

Reset Dynamic ARP Inspection statistics for all VLANs.

clear ip arp inspection statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-464 show ip arp inspection interfaces

Display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An enabled interface is defined as having at least one DAI enabled VLAN. Given a *slot/port* interface argument, the command displays the values for that interface.

show ip arp inspection interfaces [*slot/port***]**

Parameters

slot/port	(Optional) Enter an interface in slot/port format.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example.

```
(Routing)#show ip arp inspection interfaces

Interface       Trust State     Rate Limit      Burst Interval
----------      ------------    ------------    ---------------
0/1             Untrusted       15              1
0/2             Untrusted       10              10
```

Display Parameters

Interface	The interface identifier.
Trust State	Displays state: trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

5-465 show arp access-list

Display the configured ARP ACLs - the rules name ARP ACL.

show arp access-list [*acl-name***]**

Parameters

acl-name	(Optional) Display ARP Access list configuration.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is a CLI display output example.

```
(Routing)#show arp access-list

ARP access list H2
       permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
       permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
ARP access list H3
ARP access list H4
       permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```

IGMP Snooping Configuration Commands

This section IGMP snooping configuration. The supported IGMP Versions are 1, 2, and 3. The feature conserves bandwidth allowing IP multicast traffic forwarding to connected hosts that request multicast traffic.

5-466 set igmp

Enable IGMP Snooping on the system (Global Config Mode), a single or a range of interfaces. Configuration is also available to enable IGMP snooping on a single or all part participating VLANs.

The IGMP application supports the following:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintain forwarding table, MAC address to the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

No command disables IGMP Snooping, a single or a range of interfaces, or a VLAN.

set igmp [*vlan_id***]**

no set igmp [*vlan_id***]**

Parameters

vlan_id	(Optional) Indicates the VLAN identifier.

Default

The default is Disabled.

Command Mode

VLAN Config

5-467 set igmp header-validation

Enable header validation for IGMP messages.

When header validation is enabled, IGMP Snooping scans:

- The time-to-live (TTL) field in the IGMP header and drops packets where TTL does not equal 1. The TTL field should always be set to 1 in the headers of IGMP reports and queries.
- Router alert option (9404) in the IP packet header of the lGMPv2 message and drops packets that do not include this option.
- Router alert option (9404) and ToS Byte = 0xC0 (Internet Control) in the IP packet header of IGMPv3 message and drops packets that do not include these options.

No command disables header validation for IGMP messages.

set igmp header-validation

no set igmp header-validation

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-468 set igmp interfacemode

Enable IGMP Snooping on all interfaces. When IGMP Snooping is enabled and the interface routing is enabled or if it is a member of a port-channel (LAG) the IGMP Snooping functionality is disabled.

No command disables IGMP Snooping on all interfaces.

set igmp interfacemode

no set igmp interfacemode

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-469 set igmp fast-leave

Enable or disable IGMP Snooping fast-leave admin mode on a single or range interfaces or a VLAN. Enable fast-leave to allow for the immediate remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

No command disables IGMP Snooping fast-leave admin mode on selected interfaces.

set igmp fast-leave [*vlan_id***]**

no set igmp fast-leave [*vlan_id***]**

Parameters

vlan_id	(Optional) Indicates the VLAN identifiations.

Default

The default is Disabled.

Command Mode

- Interface Config
- VLAN Config

5-470 set igmp groupmembership-interval

Set the IGMP Group Membership Interval time on a VLAN, one interface, a range of interfaces, or all interfaces. The Group Membership Interval time is the amount of time in seconds for a report from a group on a particular interface before deleting the interface from the entry. The value must be greater than the lGMPv3 Maximum Response time value, range: 2 to 3600 seconds.

No command sets the IGMPv3 Group Membership Interval time to the default value.

set igmp groupmembership-interval [*vlan_id***]** *2-3600*

no set igmp groupmembership-interval [*vlan_id***]**

Parameters

vlan_id	(Optional) Indicates the VLAN identifiations.

Default

The default is 260 seconds.

Command Mode

- Interface Config
- Global Config
- VLAN Config

5-471 set igmp maxresponse

Sets the IGMP Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. The Maximum Response time is the waiting period in seconds after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

No command sets the max response time (on the interface or VLAN) to the default value.

set igmp maxresponse [*vlan_id***]** *1-25*

no set igmp maxresponse [*vlan_id***]**

Parameters

vlan_id	(Optional) Indicates the VLAN identification.

Default

The default is 10 seconds.

Command Mode

- Interface Config
- Global Config
- VLAN Config

5-472 set igmp mcrtrexpiretime

Set the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. The range is 0 to 3600 seconds, whereas a value of 0 indicates no expiration time.

No command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

set igmp mcrtrexpiretime [*vlan_id***]** *0-3600*

no set igmp mcrtrexpiretime [*vlan_id***]**

Parameters

vlan_id	(Optional) Indicates the VLAN identification.

Default

The default is 0.

Command Mode

- Interface Config
- Global Config
- VLAN Config

5-473 set igmp mrouter

Configures the VLAN ID (*vlan_id*) that has the multicast router mode enabled.

No command disables multicast router mode for a particular VLAN ID (*vlan_id*).

set igmp mrouter *vlan_id*

no set igmp mrouter *vlan_id*

Parameters

vlan_id	(Optional) Indicates the VLAN identification.

Default

The default is None.

Command Mode

Interface Config

5-474 set igmp mrouter interface

Configures the interface or range of interfaces as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

No command disables the status of the interface as a statically configured multicast router interface.

set igmp mrouter interface

no set igmp mrouter interface

Parameters

None.

Default

The default is Disabled.

Command Mode

Interface Config

5-475 set igmp report-suppression

Suppress the IGMP reports on a given VLAN ID. In order to optimize the number of reports traversing the network with no added benefits, a Report Suppression mechanism is implemented. When more than one client responds to an MGMD query for the same Multicast Group address within the max-response-time, only the first response is forwarded to the query and others are suppressed at the switch.

No command returns the system to default.

set igmp report-suppression *vlan_id*

no set igmp report-suppression

Parameters

vlan_id	(Optional) Indicates the VLAN identification. Range is 1 to 4093.

Default

The default is Disabled.

Command Mode

VLAN Config

Example

The following is a command example.

```
(Routing)#vlan database

(Routing)(Vlan)#set igmp report-suppression 1
```

5-476 show igmpsnooping

Display IGMP Snooping information for a given slot/port or VLAN. Configured information is displayed whether or not IGMP Snooping is enabled.

show igmpsnooping [*slot/port* **|** *vlan_id***]**

Parameters

slot/port	Enter an interface in slot/port format.
vlan_id	(Optional) Indicates the VLAN identification. Range is 1 to 4093.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a CLI display output example.

```
(Routing)#show igmpsnooping 1

VLAN ID..................................... 1
IGMP Snooping Admin Mode.................... Enabled
Fast Leave Mode............................. Disabled
Group Membership Interval (secs)............ 260
Maximum Response Time (secs)................ 10
Multicast Router Expiry Time (secs)......... 0
Report Suppression Mode..................... Enabled
```

Display Parameters

When the optional argument slot/port or vlan_id are not used, the command displays the following information:

Admin Mode	Indicates active status for IGMP Snooping.
Multicast Control Frame Count	The number of multicast control frames processed by the CPU.
Interface Enabled for IGMP Snooping	The list of enabled interfaces on IGMP Snooping.
VLANS Enabled for IGMP Snooping	The list of enabled VLANs on IGMP Snooping.

When you specify the slot/port values, the following information appears:

IGMP Snooping Admin Mode	Indicates active status of IGMP Snooping.
Fast Leave Mode	Indicates active status of IGMP Snooping Fast-leave.
Group Membership Interval	The waiting period in seconds a report from a particular group on a particular interface before deleting the interface from the entry. This value may be configured.
Maximum Response Time	The waiting period after it sends a query on an interface because it did not receive a report for a particular group on that interface. The value is configurable.
Multicast Router Expiry Time	The waiting period before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. The value is configurable.

When you specify a value for vlan_id, the following information appears:

VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval (secs)	The waiting period for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Maximum Response Time (secs)	The waiting period after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time (secs)	The waiting period before removing an interface that is participating in the VLAN from the list of interface with multicast routers attached. The interface is removed if a query is not received. This value may be configured.
Report Suppression Mode	Indicates whether IGMP reports (set by the command "set igmp report-suppression") in enabled or not.

5-477 show igmpsnooping mrouter interface

Display information about statically configured ports

show igmpsnooping mrouter interface *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

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

Slot/Port..................................... 0/1
Multicast Router Attached..................... Disable
```

Display Parameters

Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

5-478 show igmpsnooping mrouter vlan

Display statically configured port information.

show igmpsnooping mrouter vlan *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show igmpsnooping mrouter vlan 0/1

Slot/Port..................................... 0/1
VLAN ID....................................... 1
```

Display Parameters

Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

5-479 show igmpsnooping ssm

Display information about Source Specific Multicasting (SSM) by entry, group, or statistics. SSM delivers multicast packets to receivers that originated from a source address specified by the receiver SSM is only available with IGMPv3 and MLDv2.

show igmpsnooping ssm {entries | groups I stats}

Parameters

entries	Display source specific multicast forwarding database.
groups	Display IGMP SSM group membership information.
stats	Display statistics of IGMP snooping SSMFDB.

Default

The default is None.

Command Mode

Privileged EXEC

5-480 show mac-address-table igmpsnooping

Displays the IGMP Snooping entries in the MFDB table.

show mac-address-table igmpsnooping

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

VLAN ID	The VLAN identified as the source of the MAC address.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry, static or dynamic.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP Snooping Querier Commands

The IGMP Querier requires the central switch or router that periodically queries all end-devices on the network to announce their multicast memberships. Essentially, the responses, known as IGMP reports, maintains updates with the current multicast group membership on a port-by-port basis.

5-481 set igmp querier

Enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. The function allows you to specify the IP Address that the Snooping Querier switch should use as a source address while generating periodic queries.

Note: Querier IP Addresses assigned as a VLAN take preference over global configuration.

IGMP Snooping Querier supports sending periodic general queries on the VLAN to solicit membership reports.

No command disables IGMP Snooping Querier on the system. Use the optional address parameter to reset the querier address to 0.0.0.0.

set igmp querier [address *ipv4_address***]**

no set igmp querier [address *ipv4_address***]**

Parameters

address *ipv4_address*	(Optional) Indicates the Querier IPv4 address.

Default

The default is Disabled.

Command Mode

- Global Config
- VLAN Mode

5-482 set igmp querier query-interval

Set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

No command sets the IGMP Querier Query Interval time to default.

set igmp querier query-interval *1-1800*

no set igmp querier query-interval

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-483 set igmp querier timer expiry

Set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

No command sets the IGMP Querier timer expiration period to default.

set igmp querier timer expiry *60-300*

no set igmp querier timer expiry

Parameters

None

Default

The default is 60 seconds.

Command Mode

Global Config

5-484 set igmp querier version

Set the IGMP version of the query that the snooping switch is going to send periodically.

No command sets the IGMP Querier version to its default value.

set igmp querier version *1-2*

no set igmp querier version

Parameters

None

Default

The default is 1.

Command Mode

Global Config

5-485 set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Use the **no** command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

set igmp querier election participate

no set igmp querier election participate

Parameters

None

Default

The default is Disabled.

Command Mode

VLAN Config

5-486 show igmpsnooping querier

Display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

show igmpsnooping querier [{detail | vlan *vlanid***}]**

Parameters

detail	(Optional) Display IGMP Snooping Querier detailed information.
vlan *vlanid*	(Optional) Display IGMP Snooping Querier VLAN information.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show igmpsnooping querier

Global IGMP Snooping querier status
-----------------------------------
IGMP Snooping Querier Mode..................... Enable
Querier Address................................ 0.0.0.0
IGMP Version................................... 2
Querier Query Interval......................... 60
Querier Expiry Interval........................ 125
```

Display Parameters

When the optional argument *vlanid* is not used, the command displays the following information

Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following additional information appears.

VLAN Admin Mode	Indicates whether IGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in “Querier” or “Non-Querier" state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier

	state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument detail is used, the command shows the global information and the information for all Querier-enabled VLANs

MLD Snooping Commands

This section describes commands used for MLD Snooping. In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast addresses. In IPv6, MLD Snooping performs a similar function. With MLD Snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

5-487 set mld

This command enables MLD Snooping on the system (Global Config Mode) or an Interface (Interface Config Mode). This command also enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.

If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port channel (LAG) membership from an interface that has MLD Snooping enabled.

No command disables MLD Snooping on the system.

set mld *vlanid*

no set mld *vlanid*

Parameters

vlanid	Display MLD VLAN information.

Default

The default is Disabled.

Command Mode

- Global Config
- Interface Config
- VLAN Mode

5-488 set mld interfacemode

Enable MLD Snooping on all interfaces. When the interface is enabled for MLD Snooping and routing or it is enlisted as a member of a port-channel (LAG), MLD Snooping functionality is disabled.

No command disables MLD Snooping on all interfaces.

set mld interfacemode

no set mld interfacemode

Parameters

None.

Default

The default is Disabled.

Command Mode

Global Config

5-489 set mld fast-leave

Use this command to enable MLD Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving and MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

Note: You should enable fast-leave admin mode only on VLANs where only one host is connected to each Layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group.

Note: Fast-leave processing is supported only with MLD version 1 hosts.

Use the **no** command to disable MLD Snooping fast-leave admin mode on a selected interface.

set mld fast-leave *vlanid*

no set mld fast-leave *vlanid*

Parameters

vlanid	Display MLD VLAN information

Default

The default is Disable.

Command Mode

- Interface Config
- VLAN Mode

5-490 set mld groupmembership-interval

Use this command to set the MLD Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

Use the **no** command to set the MLDv2 Group Membership Interval time to the default value.

set mld groupmembership-interval *vlanid 2-3600*

no set mld groupmembership-interval

Parameters

vlanid	Display MLD group membership VLAN information

Default

The default is 260.

Command Mode

- Global Config
- Interface Config
- VLAN Mode

5-491 set mld maxresponse

Use this command to set the MLD Maximum Response time for the system, on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Query Interval time value. The range is 1 to 65 seconds.

Use the **no** command to set the max response time (on the interface or VLAN) to the default value.

set mld maxresponse *1-65*

no set mld maxresponse

Parameters

None

Default

The default is 10.

Command Mode

- Global Config
- Interface Config
- VLAN Mode

5-492 set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

Use the **no** command to set the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

set mld mcrtexpiretime *0-3600*

no set mld mcrtexpiretime

Parameters

<*expiration time*>	Enter 0 to 3600 seconds.

Default

The default is 0.

Command Mode

- Global Config
- Interface Config

5-493 set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Use the **no** command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

set mld mrouter *vlanid*

no set mld mrouter *vlanid*

Parameters

vlanid	Enter a VLAN ID.
interface	Configure port as a static Multicast Router.

Default

The default is None.

Command Mode

Interface Config

5-494 set mld mrouter interface

Use this command to configure the interface as a multicast router-attached interface. When configured as a multicast router interface, the interface is treated as a multicast router-attached interface in all VLANs.

Use the **no** command to disable the status of the interface as a statically configured multicast router-attached interface.

set mld mrouter interface

no set mld mrouter interface

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-495 show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

show mldsnooping [*slot/port* **|** *vlanid***]**

Parameters

slot/port	(Optional) Enter an interface in slot/port format.
vlanid	(Optional) Display MLD Snooping valid VLAN ID information.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

When the optional arguments *slot/port* or *vlanid* are not used, the command displays the following information.

Admin Mode	Indicates whether or not MLD Snooping is active on the switch.
Interfaces Enabled for MLD Snooping	Interfaces on which MLD Snooping is enabled.
MLD Control Frame Count	Displays the number of MLD Control frames that are processed by the CPU.
VLANs Enabled for MLD Snooping	VLANs on which MLD Snooping is enabled.

When you specify the *slot/port* values, the following information displays.

MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the interface.
Fast Leave Mode	lndicates whether MLD Snooping Fast Leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Max Response Time	Displays the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Present Expiration Time	Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlanid*, the following information appears.

VLAN Admin Mode	Indicates whether MLD Snooping is active on the VLAN.

5-496 show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

show mldsnooping mrouter interface *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Interface	Shows the interface on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	Displays the list of VLANs of which the interface is a member.

5-497 show mldsnooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

show mldsnooping mrouter vlan *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Interface	Shows the interface on which multicast router information is being displayed.

VLAN ID	Displays the list of VLANs of which the interface is a member.

5-498 show mldsnooping ssm entries

Use this command to display the source specific multicast forwarding database built by MLD snooping.

show mldsnooping ssm entries

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

VLAN	The VLAN on which the entry is learned.
Group	The IPv6 multicast group address.
Source	The IPv6 source address.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Interfaces	1. If Source Filter Mode is “include,” specifies the list of interfaces on which an incoming packet is forwarded. If it's source IP address is equal to the current entry’s Source, the destination IP address is equal to the current entry’s Group and the VLAN ID on which it arrived is current entry’s VLAN. 2. If Source Filter Mode is “Exclude,” specifies the list of interfaces on which an incoming packet is forwarded. If it’s source IP address is *not* equal to the current entry’s Source, the destination IP address is equal to current entry's Group and VLAN ID on which it arrived is current entry’s VLAN.

5-499 show mldsnooping ssm stats

Use this command to display the statistics of MLD snooping's SSMFDB. This command takes no options.

show mldsnooping ssm stats

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show mldsnooping ssm stats

Total Entries..................................... 508
Most SSM FDB Entries Ever Used.................... 0
Current Entries................................... 0
```

Display Parameters

Total Entries	The total number of entries that can possibly be in the MLD snooping's SSMFDB.
Most SSMFDB Entries Ever Used	The largest number of entries that have been present in the MLD snooping‘s SSMFDB.
Current Entries	The current number of entries in the MLD snooping's SSMFDB.

5-500 show mldsnooping ssm groups

Use this command to display the MLD SSM group membership information.

show mldsnooping ssm groups

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

VLAN	VLAN on which the MLD v2 report is received.

Group	The IPv6 multicast group address.
Interface	The interface on which the MLD v2 report is received.
Reporter	The IPv6 address of the host that sent the MLDv2 report.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Source Address List	List of source IP addresses for which source filtering is requested.

5-501 show mac-address-table mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

show mac-address-table mldsnooping

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

VLAN ID	The VLAN in which the MAC address is learned
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol.)
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

5-502 clear mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

clear mldsnooping

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

MLD Snooping Querier Commands

In an IPv6 environment, MLD Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the MLD Querier. The MLD query responses, known as MLD reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes the commands you use to configure and display information on MLD Snooping queries on the network and, separately, on VLANs.

Note: This note clarifies the prioritization of Multicast Group Membership Discovery (MGMD) Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

5-503 set mld querier

Use this command to enable MLD Snooping Querier on the system(Global Config Mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as a source address while generating periodic queries.

If a VLAN has MLD Snooping Querier enabled and MLD Snooping is operationally disabled on it, MLD Snooping Querier functionality is disabled on that VLAN. MLD Snooping functionality is re-enabled if MLD Snooping is operational on the VLAN.

The MLD Snooping Querier sends periodic general queries on the VLAN to solicit membership reports.

Use the **no** command to disable MLDSnooping Querier on the system. Use the optional parameter address to reset the querier address.

set mld querier [*vlan-id***] {address** *ipv6_address* **| query-interval** *interval* **| timer [expiry** *interval* **] }**

no set mld querier [*vlan-id***] [address]**

Parameters

vlan-id	(Optional) Display MLD Snooping querier VLAN ID information.
address *ipv6_address*	(Optional) Configure Querier IPv6 address.
query-interval *1-1800*	Configure Querier Query interval.

timer	Configure Querier Expiry interval.
expiry *60-300*	Enter Querier Expiry Interval.

Default

The default is Disabled.

Command Mode

- Global Config
- VLAN Mode

5-504 set mld querier query_interval

Use this command to set the MLD Querier Query lnterval time. It is the amount of time in seconds that the switch waits before sending another general query.

Use the **no** command to set the MLD Querier Query lnterval time to its default value.

set mld querier query_interval *1-1800*

no set mld querier query_interval

Parameters

None

Default

The default is 60 seconds.

Command Mode

Global Config

5-505 set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Use the **no** command to set the MLD Querier timer expiration period to its default value.

set mld querier timer expiry *60-300*

no set mld querier timer expiry

Parameters

None

Default

The default is 60 seconds.

Command Mode

Global Config

5-506 set mld querier election participate

Use this command to enable Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Use the **no** command to set the snooping querier not to participate in querier election but go into a non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

set mld querier election participate

no set mld querier election participate

Parameters

None

Default

The default is Disabled.

Command Mode

VLAN Config

5-507 show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

show mldsnooping querier [{detail | vlan *vlanid***}]**

Parameters

detail	(Optional) Display MLD Snooping Querier detailed information.
vlan *vlanid*	(Optional) Display MLD Snooping Querier VLAN information.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

When the optional argument *vlanid* is not used, the command displays the following information

Admin Mode	Indicates whether or not MLD Snooping Querier is active on the switch.
Admin Version	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to **MLD v1** and it cannot be changed
Querier Address	Shows the IP address which will be used in the IPv6 header while sending out MLD queries. it can be configured using the appropriate command.
Query Interval	Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following information appears

VLAN Admin Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
VLAN Operational State	lndicates whether MLD Snooping Querier is in "Querier" or “Non-Querier” state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participate	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv6 header while sending out MLD queries on this VLAN. It can be configured using the appropriate command.
Operational Version	This version of IPv6 will be used while sending out MLD queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the MLD version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument **detail** is used, the command shows the global information and the information for all Querier-enabled VLANs.

Port Security Commands

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

Note: To enable the SNMP trap specific to port security, see "snmp-server enable traps violation".

5-508 port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Use the **no** command to disable port locking for one (Interface Config) or all (Global Config) ports.

port-security

no port-security

Parameters

None

Default

The default is Disabled.

Command Mode

- Global Config (to enable port locking globally)
- Interface Config (to enable port locking on an interface or range of interfaces)

5-509 port-security max-dynamic

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

Use the **no** command to reset the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

port-security max-dynqmic *maxvalue*

no port-security max-dynqmic

Parameters

maxvalue	Set Dynamic Limit for the interface (0-600).

Default

The default is 600.

Command Mode

Interface Config

5-510 port-security max-static

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

Use the **no** command to set maximum number of statically locked MAC addresses to the default value.

port-security max-static *maxvalue*

no port-security max-static

Parameters

maxvalue	Set Dynamic Limit for the interface (0-20).

Default

The default is 1.

Command Mode

Interface Config

5-511 port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The *vid* is the VLAN ID.

Use the **no** command to remove a MAC address from the list of statically locked MAC addresses.

port-security mac-address *mac-address vid*

no port-security mac-address *mac-address vid*

Parameters

mac-address	Add Static MAC address to the interface.
vid	Enter a VLAN ID (1-4093).

Default

The default is None.

Command Mode

Interface Config

5-512 port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

port-security mac-address move

Parameters

None

Default

The default is None.

Command Mode

Interface Config

5-513 port-security mac-address sticky

This command enables sticky mode Port MAC Locking on a port. If accompanied by a MAC address and a VLAN ID (for Interface Config mode only), it adds a sticky MAC address to the list of statically locked MAC addresses. These sticky addresses are converted back to dynamically locked addresses if sticky mode is disabled on the port. The <vid> is the VLAN ID. The Global command applies the “sticky” mode to all valid interfaces (physical and LAG). There is no global sticky mode as such.

Sticky addresses that are dynamically learned will appear in **show running config** as “port-security mac-address sticky <mac> <vid>” entries. This distinguishes them from static entries.

Use the **no** command to removes the sticky mode. The sticky MAC address can be deleted by using the command “no port-security mac-address <mac-address> <vid>”..

port-security mac-address sticky [<mac-address> <vid>]

no port-security mac-address sticky [<mac-address> <vid>]

Parameters

<mac-address>	Add Static MAC address to the interface.
<vid>	Enter a VLAN ID (1-4093).

Default

The default is None.

Command Mode

- Global Config
- Interface Config

Example

The following is a command example.

```
(Routing)(ConFig)#port-security mac-address sticky
(Routing)(Interface 0/1)#port-security mac-address sticky

  00:00:00:00:00:01 2
```

5-514 mac-address-table limit

This command enables VLAN port security. VLAN MAC locking allows you to secure the network by locking down allowable MAC addresses on a given VLAN. Packets with a matching source MAC address can be forwarded normally. All other packets will be discarded. VLAN MAC locking will lock the dynamic MAC entries.

If VLAN and port MAC locking are enabled, VLAN MAC locking will be given precedence over port MAC locking.

Use the **no** command to disable VLAN port security on the specified VLAN.

mac-address-table limit [action shutdown] [notification trap] [*maximum-num***] [vlan** *vlan-id***]**

no mac-address-table limit [action shutdown] [notification trap] [*maximum-num***] [vlan** *vlan-id***]**

Parameters

action shutdown	(Optional) After the MAC limit has been reached, the action will shut down the ports participating in the VLAN.
notification trap	(Optional) Enables snmp-server enable traps violation on the ports participating in the VLAN. After the MAC limit has been reached, log message will be generated with the violation MAC address details.
maximum-num	(Optional) MAC limit to be configured.
vlan *vlan-id*	(Optional) VLAN on which the MAC limit is to be applied.

Default

The default is Disabled.

Command Mode

Global Config

Example

The following is a command example.

```
(Routing)(Config)#mac-address-table limit 3 vlan 10
```

```
(Routing)(Config)#mac-address-table limit action shutdown 5 vlan 20

(Routing)(Config)#mac-address-table limit notification trap 4 vlan 30

(Routing)(Config)#mac-address-table limit action shutdown notification trap 6 vlan 100
```

5-515 show port-security

This command displays the port-security settings for the port(s). If you do not use a parameter, the command displays the Port Security Administrative mode. Use the optional parameters to display the settings on a specific interface, LAG, or on all interfaces.

show port-security [{*slot/port* **| lag** *lag-id* **| all}]**

Parameters

slot/port	(Optional) Display port security information for a specific interface.
lag *lag-id*	(Optional) Enter into interface lag mode.
all	(Optional) Display port-security information for all interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing) #show port-security 0/1

Intf    Admin Mode    Dynamic Limit   Static Limit    Violation Trap Mode  Sticky Mode
-----   ----------    -------------   ------------    -------------------  ------------
0/1     Disabled      1               1               Disabled             Enabled
```

Display Parameters

Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information appears:

Admin Mode	Port Locking mode for the Interface.

Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.
Sticky Mode	Displays whether or not mode is enabled.

5-516 show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

show port-security dynamic {*slot/port* **| lag** *lag-id***}**

Parameters

slot/port	(Optional) Display port security information for a specific interface.
lag *lag-id*	(Optional) Enter into interface lag mode.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

MAC Address	MAC Address of dynamically locked MAC.

5-517 show port-security static

This command displays the statically locked MAC addresses for port. Instead of *slot/port*, **lag** *lag-id* can be used as an alternate way to specify the LAG interface. **lag** *lag-id* can also be used to specify the LAG interface where *lag-id* is the LAG port number.

show port-security static {*slot/port* **| lag** *lag-id***}**

Parameters

slot/port	(Optional) Display port security information for a specific interface.
lag *lag-id*	(Optional) Enter into interface lag mode.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show port-security static 0/1

Number of static MAC addresses configured: 2

Statically configured MAC Address      VLAN ID      Sticky
-----------------------------------    ----------   ----------
00:00:00:00:00:01                      2            Yes
00:00:00:00:00:02                      2            No
```

Display Parameters

Statically Configured MAC Address	The statically configured MAC address.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky	Indicates whether the static MAC address entry is added in sticky mode.

5-518 show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port. Instead of *slot/port*, **lag** *lag-id* can be used as an alternate way to specify the LAG interface. **lag** *lag-id* can also be used to specify the LAG interface where *lag-id* is the LAG port number.

show port-security violation {*slot/port* **| lag** *lag-id***}**

Parameters

slot/port	Enter an interface in slot/port format.
lag *lag-id*	Enter into interface lag mode.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

MAC Address	The source MAC address of the last frame that was discarded at a locked port.
VLAN ID	The VLAN ID, if applicable, associated with the MAC address of the last frame that was discarded at a locked port.

5-519 show mac-address-table limit

This command displays the VLAN port security configuration

show mac-address-table limit [*vlan-id***]**

Parameters

vlan-id	The VLAN ID on which MAC locking has been configured.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#show mac-address-table limit

Vlan MAC Locking Administration Mode: Enabled

For Vlan 10
Configured mac limit 3
Operational mac limit 3
Violation trap mode Enabled
Violation shutdown mode Disabled

vlan   Interface    Mac-Address
-----  ----------   --------------------
10     0/2          00:00:00:00:44:44
10     0/2          00:00:00:00:44:45
10     0/2          00:00:00:00:44:46

For Vlan 20
Configured mac limit 3
Operational mac limit 3
Violation trap mode Enabled
Violation shutdown mode Disabled
```

```
vlan   Interface    Mac-Address
-----  ----------   -------------------
20     0/28         00:00:00:00:00:11
20     0/28         00:00:00:00:00:12
20     0/28         00:00:00:00:00:13

(Routing)#show mac-address-table limit 10

Vlan MAC Locking Administration Mode: Enabled

For Vlan 10
Configured mac limit 3
Operational mac limit 3

vlan   Interface    Mac-Address
-----  ----------   -------------------
10     0/2          00:00:00:00:44:44
10     0/2          00:00:00:00:44:45
10     0/2          00:00:00:00:44:46
```

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.

5-520 lldp transmit

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Use the **no** command to return the local data transmission capability to the default.

lldp transmit

no lldp transmit

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-521 lldp receive

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Use the **no** command to return the reception of LLDPDUs to the default value.

lldp receive

no lldp receive

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-522 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.

Use the **no** command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

lldp timers [interval *interval-seconds*] **[hold** *hold-value*] **[reinit** *reinit-seconds*]

no lldp timers [interval] [hold] [reinit]

Parameters

interval *interval-seconds*	(Optional) The interval in seconds to transmit local LLDP data.
hold *hold-value*	(Optional) The interval multiplier to set local LLDP data TTL.
reinit *reinit-seconds*	(Optional) The delay before re-initialization.

Default

The default is as follows:

- Interval – 30 seconds
- hold – 4
- reinit – 2 seconds

Command Mode

Global Config

5-523 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”. 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.

Use the **no** command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

lldp transmit-tlv [*sys-desc***] [***sys-name***] [***sys-cap***] [***port-desc***]**

no lldp transmit-tlv [*sys-desc***] [***sys-name***] [***sys-cap***] [***port-desc***]**

Parameters

sys-desc	(Optional) Include/Exclude LLDP system description TLV.
sys-name	(Optional) Include/Exclude LLDP system name TLV.
sys-cap	(Optional) Include/Exclude LLDP system capabilities TLV.
port-desc	(Optional) Include/Exclude LLDP port description TLV.

Default

The default is is as follows: No optional TLVs are included.

Command Mode

Interface Config

5-524 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.

Use the **no** 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.

lldp transmit-mgmt

no lldp transmit-mgmt

Parameters

None

Default

The default is None.

Command Mode

Interface Config

5-525 lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Use the **no** command to disable notifications.

lldp notification

no lldp notification

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-526 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.

Use the **no** command to return the notification interval to the default value.

lldp notification-interval *5-3600*

no lldp notification-interval

Parameters

None

Default

The default is 5 seconds.

Command Mode

Global Config

5-527 clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

clear lldp statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-528 clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

clear lldp remote-data

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-529 show lldp

Use this command to display a summary of the current LLDP configuration.

show lldp

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show lldp

LLDP Global Configuration

Transmit Interval.............................. 30 seconds
Transmit Hold Multiplier....................... 4
Reinit Delay................................... 2 seconds
Notification Interval.......................... 5 seconds
```

Display Parameters

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.

5-530 show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

show lldp interface {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter all for all interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show lldp interface all

LLDP Interface Configuration

Interface    Link    Transmit     Receive      Notify       TLVs    Mgmt
----------   -----   ----------   ----------   ----------   -----   -----
0/1          Up      Disabled     Disabled     Disabled     N
0/2          Up      Disabled     Disabled     Disabled     N
0/3          Down    Disabled     Disabled     Disabled     N
0/4          Down    Disabled     Disabled     Disabled     N
0/5          Down    Disabled     Disabled     Disabled     N
0/6          Down    Disabled     Disabled     Disabled     N
0/7          Down    Disabled     Disabled     Disabled     N
0/8          Down    Disabled     Disabled     Disabled     N
0/9          Down    Disabled     Disabled     Disabled     N
0/10         Down    Disabled     Disabled     Disabled     N
0/11         Down    Disabled     Disabled     Disabled     N
0/12         Down    Disabled     Disabled     Disabled     N
0/13         Down    Disabled     Disabled     Disabled     N
0/14         Down    Disabled     Disabled     Disabled     N
0/15         Down    Disabled     Disabled     Disabled     N
0/16         Down    Disabled     Disabled     Disabled     N
0/17         Down    Disabled     Disabled     Disabled     N
0/18         Down    Disabled     Disabled     Disabled     N
0/19         Down    Disabled     Disabled     Disabled     N
0/20         Down    Disabled     Disabled     Disabled     N
0/21         Down    Disabled     Disabled     Disabled     N
0/22         Down    Disabled     Disabled     Disabled     N
0/23         Down    Disabled     Disabled     Disabled     N
0/24         Down    Disabled     Disabled     Disabled     N
0/25         Down    Disabled     Disabled     Disabled     N
0/26         Down    Disabled     Disabled     Disabled     N
0/27         Down    Disabled     Disabled     Disabled     N
0/28         Down    Disabled     Disabled     Disabled     N
0/29         Down    Disabled     Disabled     Disabled     N
0/30         Down    Disabled     Disabled     Disabled     N
0/31         Down    Disabled     Disabled     Disabled     N
0/32         Down    Disabled     Disabled     Disabled     N
0/33         Down    Disabled     Disabled     Disabled     N
0/34         Down    Disabled     Disabled     Disabled     N
0/35         Down    Disabled     Disabled     Disabled     N
0/36         Down    Disabled     Disabled     Disabled     N
0/37         Down    Disabled     Disabled     Disabled     N
0/38         Down    Disabled     Disabled     Disabled     N
```

```
0/39          Down    Disabled     Disabled     Disabled     N
0/40          Down    Disabled     Disabled     Disabled     N
0/41          Down    Disabled     Disabled     Disabled     N
0/42          Down    Disabled     Disabled     Disabled     N
0/43          Down    Disabled     Disabled     Disabled     N
0/44          Down    Disabled     Disabled     Disabled     N
0/45          Down    Disabled     Disabled     Disabled     N
0/46          Down    Disabled     Disabled     Disabled     N
0/47          Down    Disabled     Disabled     Disabled     N
0/48          Down    Disabled     Disabled     Disabled     N
0/49          Down    Enabled      Enabled      Disabled     N
0/50          Down    Disabled     Disabled     Disabled     N
0/51          Down    Disabled     Disabled     Disabled     N
0/52          Down    Disabled     Disabled     Disabled     N
0/53          Down    Disabled     Disabled     Disabled     N
0/54          Down    Disabled     Disabled     Disabled     N
0/55          Detach  Disabled     Disabled     Disabled     N
0/56          Detach  Disabled     Disabled     Disabled     N
0/57          Detach  Disabled     Disabled     Disabled     N
0/58          Detach  Disabled     Disabled     Disabled     N
0/59          Detach  Disabled     Disabled     Disabled     N
0/60          Detach  Disabled     Disabled     Disabled     N
0/61          Detach  Disabled     Disabled     Disabled     N
0/62          Detach  Disabled     Disabled     Disabled     N
0/63          Detach  Disabled     Disabled     Disabled     N
0/64          Detach  Disabled     Disabled     Disabled     N
0/65          Detach  Disabled     Disabled     Disabled     N
0/66          Detach  Disabled     Disabled     Disabled     N
0/67          Detach  Disabled     Disabled     Disabled     N
0/68          Detach  Disabled     Disabled     Disabled     N
0/69          Detach  Disabled     Disabled     Disabled     N
0/70          Detach  Disabled     Disabled     Disabled     N
0/71          Detach  Disabled     Disabled     Disabled     N
0/72          Detach  Disabled     Disabled     Disabled     N
0/73          Detach  Disabled     Disabled     Disabled     N
0/74          Detach  Disabled     Disabled     Disabled     N
0/75          Detach  Disabled     Disabled     Disabled     N
0/76          Detach  Disabled     Disabled     Disabled     N
0/77          Detach  Disabled     Disabled     Disabled     N
0/78          Detach  Disabled     Disabled     Disabled     N

TLV Codes:   0- Port Description,    1- System Name
             2- System Description,  3- System Capabilities
```

Display Parameters

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.

5-531 show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

show lldp statistics {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter all for all interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show lldp statistics all

LLDP Device Statistics

Last Update.................................... 0 days 00:00:00
Total Inserts.................................. 0
Total Deletes.................................. 0
Total Drops.................................... 0
Total Ageouts.................................. 0

Interface  Tx     Rx     Discards   Errors  Ageout  TLV      TLV      TLV  TLV    TLV
           Total  Total                              Discards Unknowns MED  802.1  802.3
---------  -----  -----  --------   -------  ------  -------- -------- ---- -----  -----
0/49       0      0      0          0       0       0        0        0    0      0
```

Display Parameters

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:

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.
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.

5-532 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.

show lldp remote-device {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.

all	Enter all for all interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example 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
```

Display Parameters

Local Interface	The interface that received the LIRDPDU 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.

5-533 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.

show lldp remote-device detail *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Switching)#show lldp remote-device detail 0/7

LLDP Remo 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
```

Display Parameters

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.

5-534 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.

show lldp local-device {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Enter all for all interfaces.

Default

The default is DHCP.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show lldp local-device all

LLDP Local Device Summary

Interface    Port ID                 Port Description
----------   --------------------    -------------------------
0/49         00:05:64:2F:0F:82
```

Display Parameters

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.

5-535 show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

show lldp local-device detail *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

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.

5-536 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.

Use the **no** command to disable MED.

lldp med

no lldp med

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-537 lldp med confignotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Use the **no** command to disable notifications.

lldp med confignotification

no lldp med confignotification

Parameters

None

Default

The default is Disabled.

Command Mode

lnterface Config

5-538 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.

Use the **no** command to remove a TLV.

lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]

no lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]

Parameters

capabilities	(Optional) Transmit the LLDP capabilities TLV.
ex-pd	(Optional) Transmit the LLDP extended PD TLV.
ex-pse	(Optional) Transmit the LLDP extended PSE TLV.
inventory	(Optional) Transmit the LLDP inventory TLV.
location	(Optional) Transmit the LLDP location TLV.
network-policy	(Optional) Transmit the LLDP network policy TLV.

Default

The default is as follows: capabilities and network policy TLVs included.

Command Mode

Interface Config

5-539 lldp med all

Use this command to configure LLDP-MED on all the ports.

lldp med all

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-540 lldp med confignotification all

Use this command to configure all the ports to send the topology change notification

lldp med confignotification all

Parameters

None

Default

The default is None.

Command Mode

Global Config

5-541 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.

Use the **no** command to return to the factory default value.

lldp med faststartrepeatcount [*count***]**

no lldp med faststartrepeatcount

Parameters

count	(Optional) The number of LLDP PDUs that will be sent when enabled.

Default

The default is 3.

Command Mode

Global Config

5-542 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).

Use the **no** command to remove a TLV.

lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]

no lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]

Parameters

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.

Default

The default is as follows: Capabilities and network policy TLVs included.

Command Mode

Global Config

5-543 show lldp med

Use this command to display a summary of the current LLDP MED configuration

show lldp med

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show lldp med

LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity
```

```
(Routing)#
```

5-544 show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface *sot/port* indicates a specific physical interface. all indicates **all** valid LLDP interfaces.

show lldp med interface {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Display LLDP MED configuration for an interface.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example 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
--More-- or (q)uit

(Routing)#
```

5-545 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.

show lldp med local-device detail *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example 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 : streamin
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
```

5-546 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.

show lldp med remote-device {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Display LLDP MED configuration for an interface.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example 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
```

Display Parameters

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.

5-547 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.

show lldp med remote-device detail *slot/port*

Parameters

slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show lldp med remote-device detail 0/8

LLDP MED Remote Device Detail

Local Interface: 0/42

Remote Identifier: 8


Capabilities
MED Capabilities Supported:
MED Capabilities Enabled:

Network Policies
```

Denial of Service Commands

This section describes the commands you use to configure Denial of Service (DoS) Control. D-LINK OS software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- **SIP = DIP:** Source IP address = Destination IP address.
- **First Fragment:** TCP Header size smaller then configured value.
- **TCP Fragment:** Allows the device to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.
- **SMAC = DMAC:** Source MAC address = Destination MAC address.
- **TCP Port:** Source TCP Port = Destination TCP Port.
- **UDP Port:** Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **TCP Offset:** Allows the device to drop packets that have a TCP header Offset set to 1.
- **TCP SYN:** TCP Flag SYN set.
- **TCP SYN &. FIN:** TCP Flags SYN and FIN set.
- **TCP FIN & URG & PSH:** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6:** Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment:** Checks for fragmented ICMP packets.

5-548 dos-control all

This command enables Denial of Service protection checks globally.

Use the **no** command to disable Denial of Service prevention checks globally.

dos-control all

no dos-control all

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-549 dos-control sipdip

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Use the **no** command to disable Source IP address = Destination IP address SIP = DIP) Denial of Service prevention.

dos-control sipdip

no dos-control sipdip

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-550 dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller than the configured value, the packets will be dropped if the mode is enabled. The default is *disabled*. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to 20.

Use the **no** command to set Minimum TCP Header Size Denial of Service protection to the default value of *disabled*.

dos-control firstfrag [*0-255***]**

no dos-control firstfrag

Parameters

None

Default

The default is Disabled (20).

Command Mode

Global Config

5-551 dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack and packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size are dropped.

Use the **no** command to disable TCP Fragment Denial of Service protection.

dos-control tcpfrag

no dos-control tcpfrag

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-552 dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks and packets will be dropped, as follows:

- Packets ingress have the TCP Flag SYN set and a source port less than 1024.
- The TCP Control Flags are set to 0 and the TCP Sequence Number is set to 0.
- The TCP Flags FIN, URG, and PSH are set and the TCP Sequence Number is set to 0.
- The TCP Flags SYN and FIN are both set.

Use the **no** command to set disables TCP Flag Denial of Service protections.

dos-control tcpflag

no dos-control tcpflag

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-553 dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled. Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Use the **no** command to disable L4 Port Denial of Service protections.

Note: Some applications mirror source and destination L4 ports.

dos-control l4port

no dos-control l4port

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-554 dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Use the **no** command to disable Maximum ICMP Packet Size Denial of Service protections.

dos-control icmp *0-1023*

no dos-control icmp

Parameters

None

Default

The default is Disabled (512).

Command Mode

Global Config

5-555 dos-control smacdmac

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Use the **no** command to disable Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

dos-control smacdmac

no dos-control smacdmac

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-556 dos-control tcpport

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Use the **no** command to disable TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

dos-control tcpport

no dos-control tcpport

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-557 dos-control udpport

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) DoS protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Use the **no** command to disable UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

dos-control udpport

no dos-control udpport

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-558 dos-control tcpflagseq

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack and packets will be dropped if the TCP Control Flags are set to 0 and the TCP Sequence Number is set to 0.

Use the **no** command to set disables TCP Flag and Sequence Denial of Service protection.

dos-control tcpflagseq

no dos-control tcpflagseq

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-559 dos-control tcpoffset

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Use the **no** command to disable TCP Offset Denial of Service protection.

dos-control tcpoffset

no dos-control tcpoffset

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-560 dos-control tcpsyn

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Use the **no** command to set disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

dos-control tcpsyn

no dos-control tcpsyn

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-561 dos-control tcpsynfin

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Use the **no** command to set disables TCP SYN & FIN Denial of Sen/ice protection.

dos-control tcpsynfin

no dos-control tcpsynfin

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-562 dos-control tcpfinurgpsh

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress

having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Use the **no** command to set disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

dos-control tcpfinurgpsh

no dos-control tcpfinurgpsh

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-563 dos-control icmpv6

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Use the **no** command to disable Maximum ICMP Packet Size Denial of Service protections.

dos-control icmpv6 *0-16376*

no dos-control icmpv6

Parameters

None

Default

The default is Disabled (512).

Command Mode

Global Config

5-564 dos-control icmpfrag

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Use the **no** command to disable ICMP Fragment Denial of Service protection.

dos-control icmpfrag

no dos-control icmpfrag

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-565 show dos-control

This command displays Denial of Service configuration information.

show dos-control

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show dos-control

Port D-disable mode.............................. Disable
First Fragment Mode.............................. Disable
Min TCP Hdr Size................................. 20
ICMPv4 Mode...................................... Disable
Max ICMPv4 Payload Size.......................... 512
ICMPv6 Mode...................................... Disable
Max ICMPv6 Payload Size.......................... 512
ICMPv4 Fragment Mode............................. Disable
L4 Port Mode..................................... Disable
TCP Port Mode.................................... Disable
```

```
UDP Port Mode..................................... Disable
SIPDIP Mode....................................... Disable
SMACDMAC Mode..................................... Disable
TCP FIN&URG&PSH Mode.............................. Disable
TCP Flag & Sequence Mode.......................... Disable
TCP SYN Mode...................................... Disable
TCP SYN&FIN Mode.................................. Disable
TCP Fragment Mode................................. Disable
TCP Offset Mode................................... Disable
```

Display Parameters

First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size	The factory default is 20.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Pkt Size	The range is 0-16376. The factory default is 512.
Max ICMPv6 Pkt Size	The range is 0-16376. The factory default is 512.
ICMP Fragment Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
TCP Port Mode	May be enabled or disabled. The factory default is disabled.
UDP Port Mode	May be enabled or disabled. The factory default is disabled.
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
SMACDMAC Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
TCP FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

5-566 bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The range is 10 to 1,000,000 seconds.

Use the **no** command to set the forwarding database address aging timeout to the default value.

bridge aging-time *10-1000000*

no bridge aging-time

Parameters

None

Default

The default is 300.

Command Mode

Global Config

5-567 show forwardingdb agetime

This command displays the timeout for address aging.

show forwardingdb agetime

Parameters

None

Default

The default is All.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show forwardingdb agetime

Address Aging Timeout: 300
```

Display Parameters

Address Aging Timeout	Displays the system's address aging timeout value in seconds.

5-568 show mac-address-table multicast

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

show mac-address-table multicast *macaddr*

Parameters

macaddr	Enter a 6 byte MAC Address.

Default

The default is None.

Command Mode

Privileged EXEC

Example

If one or more entries exist in the multicast forwarding table, the command output looks similar to the following.

```
(Routing)#show mac-address-table multicast

VLAN ID    MAC Address         Source    Type     Description  Interface   Fwd Interface
--------   ------------------  --------  -------  -----------  ----------  -------------
1          01:00:5E:01:02:03   Filter    Static   Mgmt Config  Fwd:        Fwd:
                                                                0/1,        0/1,
                                                                0/2,        0/2,
                                                                0/3,        0/3,
                                                                0/4,        0/4,
                                                                0/5,        0/5,
                                                                0/6,        0/6,
                                                                0/7,        0/7,
                                                                0/8,        0/8,
                                                                0/9,        0/9,
                                                                0/10,       0/10,
--More-- or (q)uit
```

Display Parameters

VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Source	The component that is responsible for this entry in the Multicast Forwarding Database. The source can be IGMP Snooping, GMRP, and Static Filtering.

Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Fwd Interface	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

5-569 show mac-address-table stats

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

show mac-address-table stats

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show mac-address-table stats

Max MFDB Table Entries.......................... 2048
Most MFDB Entries Since Last Reset.............. 0
Current Entries................................. 0
```

Display Parameters

Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

ISDP Commands

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

5-570 isdp run

This command enables ISDP on the switch.

Use the **no** command to disable ISDP on the switch.

isdp run

no isdp run

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

5-571 isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

isdp holdtime *10-255*

Parameters

None

Default

The default is 180.

Command Mode

Global Config

5-572 isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

isdp timer *5-254*

Parameters

None

Default

The default is 30.

Command Mode

Global Config

5-573 isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Use the **no** command to disable the sending of ISDP version 2 packets from the device.

isdp advertise-v2

no isdp advertise-v2

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

5-574 isdp enable

This command enables ISDP on an interface or range of interfaces.

Use the **no** command to disable ISDP on the interface.

Note: ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command “isdp run”.

isdp enable

no isdp enable

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

5-575 clear isdp counters

This command clears ISDP counters.

clear isdp counters

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-576 clear isdp table

This command clears entries in the ISDP table.

clear isdp table

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-577 show isdp

This command displays global ISDP settings.

show isdp

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)#show isdp

Timer..................................... 30
Hold Time................................. 180
Version 2 Advertisements.................. Enabled
Neighbors table time since last change.... 0 days 00:00:00
Device ID................................. 2S41J000253
Device ID format capability............... Serial Number, Host Name
Device ID format.......................... Serial Number
```

Display Parameters

Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
ISDPv2 Advertisements	The setting for sending lSDPv2 packets. If disabled, version 1 packets are transmitted.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	Indicates the Device ID format capability of the device. • **serialNumber** indicates that the device uses a serial number as the format for its Device ID.

	• **macAddress** indicates that the device uses a Layer 2 MAC address as the format for its Device ID. • **other** indicates that the device uses its platform-specific format as the format for its Device ID.
Device ID Format	Indicates the Device ID format of the device. • **serialNumber** indicates that the value is in the form of an ASCII string containing the device serial number. • **macAddress** indicates that the value is in the form of a Layer 2 MAC address. • **other** indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepended with system name.

5-578 show isdp interface

This command displays ISDP settings for the specified interface.

show isdp interface {all | *slot/port***}**

Parameters

all	Display ISDP mode for all available interfaces.
slot/port	Enter an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)#show isdp interface 0/1

Interface    Mode
----------   ----------
0/1          Enabled
```

Display Parameters

Mode	ISDP mode enabled/disabled status for the interface(s).

5-579 show isdp entry

This command displays ISDP entries. If the device ID is specified, then only entries for that device are shown.

show isdp entry {all | deviceid}

Parameters

all	Display ISDP entries for all available devices.
deviceid	Display ISDP entry information for device ID.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.

5-580 show isdp neighbors

This command displays the list of neighboring devices.

show isdp neighbors [{*slot/port* **| detail}]**

Parameters

slot/port	Enter an interface in slot/port format.
detail	Display ISDP neighbors detail table.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Switching)#show isdp neighbors detail

(Routing)#show isdp neighbors detail

Device ID                    0001f52f2bc1
Address(es):
Capability                   Router
Platform                     DXS-5000-54S
Interface                    0/33
Port ID                      0/37
Holdtime                     180
Advertisement Version        2
Time when last changed       2 days 05:47:33
Version:
1.2.0.3
```

Display Parameters

Device ID	The device ID associated with the neighbor which advertised the information.
IP Address(es)	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (*slot/port*) on which the neighbor‘s advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Time when last changed	Displays when the entry was last modified.
Version	The software version that the neighbor is running.

5-581 show isdp traffic

This command displays ISDP statistics.

show isdp traffic

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

ISDP Packets Received	Total number of ISDP packets received.
ISDP Packets Transmitted	Total number of ISDP packets transmitted.
ISDPv1 Packets Received	Total number of ISDPv1 packets received.
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted.
ISDPv2 Packets Received	Total number of ISDPv2 packets received.
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted.
ISDP Bad Header	Number of packets received with a bad header.
ISDP Checksum Error	Number of packets received with a checksum error.
ISDP Transmission Failure	Number of packets which failed to transmit.
ISDP invalid Format	Number of invalid packets received.
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database.
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

Unidirectional Link Detection Commands

The Unidirectional Link Detection (UDLD) feature detects unidirectional links' physical ports. UDLD must be enabled on both sides of the link in order to detect a unidirectional link. The UDLD protocol operates by exchanging packets containing information about neighboring devices.

The purpose of the UDLD feature is to detect and avoid unidirectional links. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bi-directional link stops passing traffic in one direction.

5-582 udld enable (Global Config)

Use the **udld enable** command in Global Config mode to enable UDLD globally on the switch.

Use the **no** command in Global Config mode to disable UDLD globally on the switch.

udld enable

no udld enable

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

5-583 udld message time

Use the **udld message time** command in Global Config mode to configure the interval between UDLD probe messages on ports that are in the advertisement phase.

Use the **no** command to remove.

udld message time *7-90*

Parameters

None

Default

The default is 15 seconds.

Command Mode

Global Config

5-584 udld timeout interval

Use the **udld timeout interval** command in Global Config mode to configure the time interval after which the UDLD link is considered to be unidirectional. The interval range is from 5 to 60 seconds.

Use the **no** command to remove.

udld timeout interval *5-60*

Parameters

None

Default

The default is 5 seconds.

Command Mode

Global Config

5-585 udld enable (Interface Config)

Use the **udld enable** command in Interface Config mode to enable UDLD on the specified interface.

Use the **no** command to in Interface Config mode to disable UDLD on the specified interface.

udld enable

no udld enable

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

5-586 udld port

Use the **udld port** command in Interface Config mode to select the UDLD mode operating on this interface. If the keyword **aggressive** is not entered, the port operates in normal mode.

udld port [aggressive]

Parameters

aggressive	Set aggressive mode on the interface.

Default

The default is Normal.

Command Mode

Interface Config

5-587 udld reset

Use the **udld reset** command in Privileged EXEC mode to reset all interfaces that have been shut down by UDLD.

udld reset

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

5-588 show udld

Use the **show udld** command in Privileged EXEC or User EXEC modes to display the global settings of UDLD.

show udld

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show udld

Admin Mode..................................... Enabled
Message Interval............................... 15 seconds
Timeout Interval............................... 5 seconds
```

Display Parameters

Admin Mode	The global administrative mode of UDLD.
Message Interval	The time period (in seconds) between the transmission of UDLD probe packets.
Timeout Interval	The time period (in seconds) before making the decision that the link is unidirectional.

5-589 show udld slot/port

Use the **show udld** *slot/port* command in Privileged EXEC or User EXEC modes to display the UDLD settings for the specified slot/port.

show udld {*slot/port* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
all	Display UDLD mode for all available interfaces.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show udld 0/2

Port   Admin Mode    UDLD Mode     UDLD Status
-----  ----------    ----------    ---------------
0/2    Enabled       Aggressive    Bidirectional
```

Display Parameters

Port	The identifying port of the interface.
Admin Mode	The administrative mode of UDLD configured on this interface. The mode is either **Enabled** or **Disabled**.
UDLD Mode	The UDLD mode configured on this interface. The mode is either **Normal** or **Aggressive**.
UDLD Status	The status of the link as determined by UniDirectional Link Detection (UDLD) protocol. The options are: • Undetermined – mode has not collected enough information to determine the state of the link. • Not applicable – mode is disabled, either globally or on the port. • Shutdown – mode has detected a unidirectional link and shutdown the port. That is, the port is in an errDisabled state. • Bidirectional – mode has detected a bidirectional link. • Undetermined (Link Down) – mode shuts down a port if it can explicitly determine that the associated link has been faulty for an extended period of time.

Interface Error Disable and Auto Recovery

Interface error disable automatically disables an interface when an error is detected; no traffic is allowed until the interface is either manually re-enabled or, if auto recovery is configured, the configured auto recovery time interval has passed.

For interface error disable and auto recovery, an error condition is detected for an interface, the interface is placed in a diagnostic disabled state by shutting down the interface. The error disabled interface does not allow any traffic until the interface is re-enabled. The error disabled interface can be manually enabled. Alternatively administrator can enable auto recovery feature. D-LINK OS Auto Recovery re-enables the interface after the expiry of configured time interval.

5-590 errdisable recovery cause

Use this command to enable auto recovery for a specified cause or all causes. When auto recovery is enabled, ports in the diag-disable state are recovered (link up) when the recovery interval expires. If the interface continues to experience errors, the interface may be placed back in the diag-disable state and disabled (link down). Interfaces in the diag-disable state can be manually recovered by entering the **no shutdown** command for the interface.

Use the **no** command to disable auto recovery for a specific cause. When disabled. auto recovery will not occur for interfaces in a diag-disable state due to that cause.

errdisable recovery cause {all | udld | storm-control | bpdu | mac-flap | link-flap}

no errdisable recovery cause {all | udld | storm-control | bpdu | mac-flap | link-flap}

Parameters

all	Enable/Disable timer to recover from all error disable state.
bpdu	Enable/Disable timer to recover from spanning-tree error disable state.
mac-flap	Enable/Disable timer to recover from mac flapping error disable state.
storm-control	Enable/Disable timer to recover from storm-control error disable state.
udld	Enable/Disable timer to recover from udld error disable state.
link-flap	Enable/Disable timer to recover from link flapping error disable state.

Default

The default is None.

Command Mode

Global Config

5-591 errdisable recovery interval

Use this command to configure the auto recovery time interval. The auto recovery time interval is common for all causes. The time can be any value from 30 to 86400 seconds. When the recovery interval expires, the system attempts to bring interfaces in the diag-disable state back into service (link up).

Use the **no** command to reset the auto recovery interval to the factory default value of 300.

errdisable recovery interval *30-86400*

no errdisable recovery interval

Parameters

None

Default

The default is 300.

Command Mode

Global Config

5-592 show errdisable recovery

Use this command to display the error-disabled auto-recovery configuration status of all configurable causes.

show errdisable recovery

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Routing)#show errdisable recovery

Errdisable Reason          Auto-recovery Status
--------------------       -------------------------
dhcp-rate-limit            Disabled
arp-inspection             Disabled
udld                       Disabled
bpduguard                  Disabled
bpdustorm                  Disabled
sfp-mismatch               Disabled
keepalive                  Disabled
mac-locking                Disabled
denial-of-service          Disabled
Timeout for Auto-recovery from D-Disable state 300
```

Display Parameters

arp-inspection	Enable/Disable status of arp-inspection auto recovery.
bpduguard	Enable/Disable status of bpduguard auto recovery.
dhcp-rate-limit	Enable/Disable status of dhcp-rate-limit auto recovery.
sfp-mismatch	Enable/Disable status of sfp-mismatch auto recovery.
udld	Enable/Disable status of UDLD auto recovery.
bpdustorm	Enable/Disable status of bpdustorm auto recovery.
keepalive	Enable/Disable status of keepalive auto recovery.
mac-locking	Enable/Disable status of MAC locking auto recovery.
denial-of-service	Enable/Disable status of DoS auto recovery.
time interval	Time interval for auto recovery in seconds.

6. Data Center Commands

This chapter describes the commands to configure the data center features available in the D-LINK OS CLI. The Data Center Commands section includes the following commands:

Data Center Bridging Exchange Protocol Commands

The Data Center Bridging Exchange Protocol (DCBX) is used by DCB devices to exchange configuration information with directly-connected peers. The protocol is also used to detect misconfiguration of the peer DCB devices and, optionally, for configuration of peer DCB devices.

6-1 lldp dcbx version

Use the **lldp dcbx version** command in Global Configuration mode to configure the administrative version for the Data Center Bridging Capability Exchange (DCBX) protocol. This command enables the switch to support a specific version of the DCBX protocol or to detect the peer version and match it. DCBX can be configured to operate in IEEE mode or CEE mode or CIN. In auto mode, version detection is based on the peer device DCBX version. The switch operates in either IEEE or one legacy modes on each interface.

In **auto** mode, the switch will attempt to jump start the exchange by sending an IEEE frame, followed by a CEE frame followed by a CIN frame. The switch will parse the received response and immediately switch to the peer version.

Note: CIN is Cisco Intel Nuova DCBX (version 1.0). CEE is converged enhanced ethernet DCBX (version 1.06).

Use the **no** command to reset the DCBX version to the default value of auto.

lldp dcbx version {auto | cin | cee | ieee}

no lldp dcbx version

Parameters

auto	Automatically select the version based on the peer response.
cin	Force the mode to Cisco-Intel-Nuova. (DCBX 1.0)
cee	Force the mode to CEE. (DCBX 1.06)
ieee	Force the mode to IEEE 802.1Qaz.

Default

The default is Auto.

Command Mode

Global Config

Example

The following example configures the switch to use CEE DCBX.

```
(Routing)(config)#lldp dcbx version cee
```

6-2 lldp tlv-select dcbxp

Use the **lldp tlv-select dcbxp** command in Interface Configuration or Global Configuration mode to send specific DCBX TLVs if LLDP is enabled to transmit on the given interface. If no parameter is given, all DCBX TLVs are enabled for transmission. The default is all DCBX TLVs are enabled for transmission. If executed in Interface mode, the interface configuration overrides the global configuration on the designated interface. Entering the command with no parameters enables transmission of all TLVs.

Use the **no** command to disable LLDP from sending all or individual DCBX TLVs, even if LLDP is enabled for transmission on the given interface.

lldp tlv-select dcbxp [ets-config | ets-recommend | pfc | application-priority]

no lldp tlv-select dcbxp [ets-config | ets-recommend | pfc | application-priority]

Parameters

ets-config	(Optional) Transmit the Enhanced Transmission Selection (ETS) configuration TLV.
ets-recommend	(Optional) Transmit the ETS recommendation TLV.
pfc	(Optional) Transmit the PFC configuration TLV.
application-priority	(Optional) Transmit the application priority TLV.

Default

The default is as follows: Transmission of all TLVs is enabled.

Command Mode

- Global Config
- Interface Config

Example

The following example configures the port to transmit all TLVs.

```
(Routing)(Config)#no lldp tlv-select dcbxp
```

6-3 lldp dcbx port-role

Use the **lldp dcbx port-role** command in Interface Configuration mode to configure the port role to manual, auto-upstream, auto-downstream and configuration source. In order to reduce configuration flapping, ports that obtain configuration information from a configuration source port will maintain that configuration for 2x the LLDP timeout, even if the configuration source port becomes operationally disabled.

Use the **no** command in Interface Configuration mode to configure the port role to manual.

lldp dcbx port-role {auto-up | auto-down | manual |configuration-source}

no lldp dcbx port-role

Parameters

auto-up	Advertises a configuration, but is also willing to accept a configuration from the link-partner and propagate it internally to the auto-downstream ports as well as receive configuration propagated internally by other auto-upstr ports. These ports have the willing bit enabled. These ports should be connected to FCFs.
auto-down	Advertises a configuration but is not willing to accept one from the link partner. However, the port will accept a configuration propagated internally by the configuration source. These ports have the willing bit set to disabled. Selection of a port based upon compatibility of the received configuration is suppressed. These ports should be connected to a trusted FCF.
manual	Ports operating in the **Manual** role do not have their configuration affected by peer devices or by internal propagation of configuration. These ports will advertise their configuration to their peer if DCBX is enabled on that port. The willing bit is set to disabled on manual role ports.
configuration-source	In this role, the port has been manually selected to be the configuration source. Configuration received over this port is propagated to the other auto-configuration ports. Selection of a port based upon compatibility of the received configuration is suppressed. These ports should be connected to a trusted FCF. These ports have the willing bit enabled.

Default

The default is Manual.

Command Mode

Interface Config

Example

The following example configures an FCF facing port.

```
(Routing)(Interface 0/1)#lldp dcbx port-role auto-up
```

The following example configures an FCoE host facing port.

```
(Routing)(Interface 0/1)#lldp dcbx port-role auto-down
```

6-4 show lldp tlv-select

Use the **show lldp tlv-select** command in Privileged EXEC mode to display the per interface TLV configuration

show lldp tlv-select {interface all | *slot/port***}**

Parameters

all	All interfaces.
slot/port	A valid physical interface specifier.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following command shows the TLVs selected for transmission on multiple interfaces.

```
(Routing)#show lldp tlv-select interface all

Interface   ETS Config   ETS Recommend     PFC     App     Priority    QCN
----------  ----------   ---------------   -----   -----   ---------   ----------
0/1         Yes          No                Yes     No      Yes
0/2         No           No                Yes     No      Yes         4.1.3.2
```

Display Parameters

Interfaces	Specifies all the ports on which DCBX TLV can be configured.
ETS Config	Specifies the DCBX ets-configuration TLV status of the interfaces.
ETS Recommend	Specifies the DCBX DCBX ets-recommendation TLV on the interfaces.
PFC	Specifies the DCBX priority flow control TLV on the interfaces.
App	Displays App priority Specifies the DCBX application-priority TLV on the interfaces.
Priority	App priority Specifies the DCBX application-priority TLV on the interfaces.
QCN	Displays the Quantized Congestion Notification (QCN) management point.

6-5 show lldp dcbx interface

Use the **show lldp dcbx interface** command in Privileged EXEC mode to display the local DCBX control status of an interface.

show lldp dcbx {interface all | *slot/port***} [detail | status]**

Parameters

all	All interfaces.

slot/port	A valid physical interface specifier.
detail	Display detailed DCBX information.
status	Displays a status summary.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows DCBX status.

```
(Routing)#show lldp dcbx interface all

Is configuration source selected.....False
Interface   Status     Role    Version  DCBX Tx  DCBX Rx  DCBX Errors  unknown TLV
----------  --------   ------  -------  -------  -------  ----------   -------------
0/1         Disabled   Manual  Auto     0        0        0            0
0/2         Disabled   Manual  Auto     0        0        0            0
0/3         Disabled   Manual  Auto     0        0        0            0
0/4         Disabled   Manual  Auto     0        0        0            0
0/5         Disabled   Manual  Auto     0        0        0            0
0/6         Disabled   Manual  Auto     0        0        0            0
0/7         Disabled   Manual  Auto     0        0        0            0
0/8         Disabled   Manual  Auto     0        0        0            0
```

In the following example, DCBX is not enabled.

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

DCBX operational status:.....................Disabled (Reason: LLDP TX/RX is disabled.)
Configured DCBX version:.....................Auto
Peer DCBX version:...........................
Peer MAC:....................................
Peer Description:............................
Auto-configuration Port Role:................Manual
Peer Is configuration Source:................False

Error counters:
ETS incompatible configuration..............0
PFC incompatible configuration..............0
Disappearing neighbor.......................0
Multiple neighbors detected.................0
```

The following example displays details.

```
(Routing)#show lldp dcbx interface 0/1 detail
```

```
DCBX operational status.....Disabled (Reason: LLDP Tx/Rx is disabled.)
Configured DCBX version:.....Auto
Peer DCBX version:.....
Peer MAC:.....
Peer Description:.....
Auto-configuration Port Role:.....Manual
Peer Is configuration Source:.....False

Error counters:
ETS incompatible configuration.....0
PFC incompatible configuration.....0
Disappearing neighbor.....0
Multiple neighbors detected.....0

Local configuration:

PFC configuration (Tx enabled)
willing: False      MBC: False    Max PFC classes supported: 8
PFC enable vector:  0:0    1:0    2:0    3:0    4:0    5:0    6:0    7:0

ETS configuration (Tx enabled)
```

Quantized Congestion Notification Commands

The Quantized Congestion Notification (QCN) feature is an aspect of the Data Center Package.

6-6 qcn enable

The **qcn enable** command is used in the Global Configuration mode in order to enable QCN on all of the ports of the system, that is, the command is a master enable control. Once QCN has been enabled, the system will recognize the CN-TAG in any received frames, such that the Congestion algorithm will run on the configured Congestion Points (CP) while Congestion Notification Messages (CNMs) will be transmitted in the event that congestion is detected on a CP.

The **no** command is used in the Global Configuration mode in order to disable QCN on all of the ports of the system. Once QCN has been disabled, the received frames with CN-TAGs will be treated as normal data frames and no CNMs will ever be generated.

qcn enable

no qcn enable

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

6-7 qcn cnm-transmit-priority

The **qcn cnm-transmit-priority** command is used in the Global Configuration mode in order to globally configure the dot1p priority value for the congestion notification messages (CNM) that are sent by the system. By default, CNMs are sent with a dot1p priority value of zero.

The **no** command is used in the Global Configuration mode in order to reset the dot1p priority value for the CNMs transmitted by the system back to the default value.

qcn cnm-transmit-priority *dot1p-priority*

no qcn cnm-transmit-priority

Parameters

dot1p-priority	Enter dot1p priority, range 0-7.

Default

The default is 0.

Command Mode

Global Config

6-8 qcn cnpv-priority (datacenter bridging config)

The **qcn cnpv-priority** command is used in the Data Center Bridging Configuration mode in order to globally configure a CP (port-queue) that has been mapped to the specified dot1p priority as a congestion enabled (**interior**), congestion disabled (**disable**), or edge congestion point (**edge**) for all the ports that have the defense mode configured as **component**.

qcn cnpv-priority *cnpv-priority* **{interior | edge | disable}**

Parameters

cnpv-priority	The range is 0-7.
interior	Interior congestion point (ICP). Used when a flow with the specified dot1p priority needs to be congestion aware. This setting enables detection of congestion of the selected priority.
edge	Edge congestion point (ECP). Used when the congestion point(CP) is on the edge of the congestion notification domain (CND).
disable	Disabled for QCN. Used when it is desired that the priority be

	congestion unaware. This setting disables detection of congestion on the priority.

Default

The default is Disabled QCN Priorities.

Command Mode

Data Center Bridging Config

6-9 qcn cnpv-priority alternate-priority

The **qcn cnpv-priority alternate-priority** command is used in the Global Configuration mode in order to globally configure the alternate priority of the selected cnpv-priority, such that when a frame with a dot1p priority equal to the congestion notification priority value is received, the priority value in the frame will be remarked with the alternate priority. The alternate priority is only applied to incoming frames if the dot1p priority of the incoming frame is equal to the Congestion Notification Priority Value (CNPV) priority of the CP and the CP is configured as Edge.

The alternate priority setting is used to steer away any traffic that is sent from CN-unaware sources. When entering the Congestion Notification Domain (CND) domain, traffic from non-congestion aware sources is remarked so that those resources granted to the congestion-enabled queues will not be exhausted with traffic from QCN unaware sources. Since those frames are being sent from non-QCN sources, they will not have a CN-TAG. As such, if the frames are mapped to the congestion-enabled queue, they may contribute to congestion and, as a result, trigger the generation of CNMs. This is not helpful for sources that are QCN-unaware.

This configuration will be applied to all the ports for which the defense-mode-choice is configured as component.

The **no** command is used in the Global Configuration mode to reset the alternate priority back to the default value.

qcn cnpv-priority *cnpv-priority* **alternate-priority** *non-cnpv-priority*

no qcn cnpv-priority *cnpv-priority* **alternate-priority**

Parameters

cnpv-priority	The range is 0-7.
non-cnpv-priority	The range of alternate priority is 0-7.

Default

The default is None.

Command Mode

Global Config

6-10 qcn cnpv-priority cp-creation

The **qcn cnpv-priority cp-creation** command is used in the Global Configuration mode to globally configure the default scope of the per port-priority defense mode choice that is made whenever a CP is newly created. The default scope in question can be **admin** or **component**.

qcn cnpv-priority *cnpv-priority* **cp-creation {enable | disable}**

Parameters

cnpv-priority	The range is 0-7.
enable	If cp-creation is enabled, the per-port defense mode choice is set to component
disable	If cp-creation is disabled, the per-port defense mode choice is set to admin.

Default

The default is Enabled for qcn cp-creation.

Command Mode

Global Config

6-11 qcn cnpv-priority defense-mode-choice

The **qcn cnpv-priority defense-mode-choice** command is used in the Interface Configuration mode to choose **admin** or **component** as the defense mode of an interface, that is, to choose whether the **interior/edge/disable** and alternate priorities will use the per-priority configuration or per-port-priority configuration.

qcn cnpv-priority *cnpv-priority* **defense-mode-choice {admin | component}**

Parameters

cnpv-priority	The range is 0-7.
admin	Per priority.
component	Per priority level configuration.

Default

The default is Enabled.

Command Mode

Interface Config

6-12 qcn cnpv-priority

The **qcn cnpv-priority** command is used in the Interface Config mode in order to configure a CP (port-queue) that has been mapped to the specified dot1p priority as a congestion enabled (interior), congestion disabled (disabled), or edge congestion point (edge) for a given interface that has the defense mode configured as **component** and a defense mode of **Admin**.

This configuration is only applied in the event that the defense mode choice is configured as Admin.

qcn cnpv-priority *cnpv-priority* **{interior | edge | disable}**

Parameters

cnpv-priority	The range is 0-7.
interior	Interior congestion point (ICP). Used when a flow with the specified dot1p priority needs to be congestion aware. This setting enables detection of congestion of the selected priority.
edge	Edge congestion point (ECP). Used when the congestion point (CP) is on the edge of the congestion notification domain (CND).
disable	Disabled for QCN. Used when it is desired that the priority be congestion unaware. This setting disables detection of congestion on the priority.

Default

The default is Disabled for all QCN priority.

Command Mode

Interface Config

6-13 qcn cnpv-priority alternate-priority

The **qcn cnpv-priority alternate-priority** command is used in the Interface Configuration mode in order to configure the alternate priority on an interface for a specified incoming ICP priority. This alternate-priority will override the alternate-priority that has been set in the global mode for this incoming ICP priority on the given port. This configuration is only applied in the event that the defense mode is configured as **Admin**.

The **no** command is used in the Interface Configuration mode to reset the alternate priority value of the given port-priority back to the default value. In the event that a global alternate priority value has been configured, it will be used.

qcn cnpv-priority *cnpv-priority* **alternate-priority** *alternate-priority*

no qcn cnpv-priority *cnpv-priority* **alternate-priority**

Parameters

cnpv-priority	Enter dot1p priority, range 0-7.
alternate-priority	Configure priority to remark the traffic when defense-mode is edge.

Default

The default is Globally configured alternative-priority.

Command Mode

Interface Config

6-14 qcn transmit-tlv enable

The **qcn transmit-tlv enable** command is used in the Interface Configuration mode in order to enable the transmission of QCN TLVs via LLDP.

The **no** command is used in the Interface Configuration mode in order to configure the mode of the QCN TLV transmission to disabled. QCN TLVs transmissions are propagated via LLDP.

qcn transmit-tlv enable

no qcn transmit-tlv enable

Parameters

None

Default

The default is Disabled QCN TLVs transmission.

Command Mode

Interface Config

6-15 clear qcn statistics

The **clear qcn statistics** command is used in the Privileged EXEC mode in order to clear the CNM transmitted counters for the given CP. In the event that a specific interface and CP are not mentioned, then the command will clear all the CNM counters for all of the CPs in the system. If an interface number only is specified, then only all of the CNM transmit counters on that interface will be cleared.

clear qcn statistics [*slot/port***] [cp** *cp-index***]**

Parameters

slot/port	(Optional) If only the interface number is specified, then all the CNM transmit counters on that interface are cleared.
cp-index	(Optional) If only the cp index is specified, then CNM transmit counters for that cp index on all interfaces are cleared.

Default

The default is None.

Command Mode

Privileged EXEC

6-16 show qcn priority

The **show qcn priority** command is used in the Privileged EXEC mode to show the QCN configuration

show qcn priority [*priority***] [interface** *slot/port* **| all]**

Parameters

priority	If only priority is specified, then per-priority configuration is displayed.
slot/port	If the interface number is also specified, then the command displays the configuration per-port-priority for the given priority.
all	If all is specified, then per priority information for all dot1p priorities is displayed.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show qcn priority 1

Global Configuration:
QCN status(Master enable)    : Enabled
CNM transmit priority        : 0

Per-priority configuration:
Defense mode: interior
Alternate priority: 2
cp-creation: disabled
```

```
Errored port list: 0/1,0/8
LLDP mismatch port list: 0/5-8
Configured as CNPV on ports: 0/1,0/7-12
```

The following is an example of the CLI display output for the command.

```
(Routing)#show qcn priority

Global Configuration:
QCN status(Master enable)    : Enabled
CNM transmit priority        : 0

Per-priority configuration:
dot1p-     Defense-   Alternate-  cp-         Errored     LLDP             Configured as
priority   mode       priority    creation    Port List   mismatch list    cnpv on ports
--------   ---------  ----------  ---------   ----------  --------------   -------------
0          disabled   -           -           -           -                -
1          interior   0           enable      0/1,0/8     0/5-7            0/1-10
2          edge       0           disable     0/1         0/5-7            0/1-10
3          disabled   -           -           -           -                -
4          disabled   -           -           -           -                -
5          disabled   -           -           -           -                -
6          disabled   -           -           -           -                -
7          disabled   -           -           -           -                -
```

The following is an example of the CLI display output for the command.

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

Global Configuration:
QCN status(Master enable)    : Enabled
CNM transmit priority        : 0

Per-port-priority configuration:
Defense mode choice: admin
Defense mode: interior
Alternate priority: 2
```

The following shows example CLI display output for the command.

```
(Routing) #show qcn priority 1 interface all

Global Configuration:
QCN status(Master enable)    : Enabled
CNM transmit priority        : 0

Per-port-priority configuration
Interface Number    Defense-mode Choice        Defense Mode  Alternate Priority
-----------------   --------------------       ------------  --------------------
0/1                 admin                      disabled      -
0/2                 admin                      interior      2
```

```
0/3                 admin                     edge          -
0/4                 component                 interior      3
```

6-17 show qcn active priority

The **show qcn active priority** command is used in the Privileged EXEC mode to show the operational QCN configuration for the dot1p priority specified.

show qcn active priority *0-7*

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#

Interface Number     Defense mode      Alternate priority
-----------------    ---------------   --------------------
0/1                  interior          2
0/2                  edge              -
0/3                  interior          0
0/4                  disabled          -
0/5                  interior          -
```

The following is an example of the CLI display output for the command.

```
(Routing)#show qcn active priority 1

Port    Defense mode      Alternate priority
-----   ---------------   --------------------
0/1     disable           0
0/2     disable           0
0/3     disable           0
0/4     disable           0
0/5     disable           0
0/6     disable           0
0/7     disable           0
0/8     disable           0
0/9     disable           0
--More-- or (q)uit
```

6-18 show qcn interface

The **show qcn interface** command is used in the Privileged EXEC mode to show the Congestion Point information for the port specified.

show qcn interface *slot/port* **[cp-index** *cp-index***]**

Parameters

slot/port	Indicates the slot/port interface.
cp-index *cp-index*	(Optional) Enter the congestion point index

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show qcn interface 0/1 cp-index 1

Interface    0/1
cp-index     1
MAC-Address  00:10:18:00:00:FF
CP-Identifier: 00012610071005
CNM-transmit-Priority      0
Congestion queue weight
Sample-base
Cp-Sizesetpoint
Min—HeaderOctets

Note: CPID can be deciphered as mentioned below
000126 : Last 3 bytes of system MAC Address
1    - unit number on which congestion is detected
0    - slot number on which congestion is detected
07   - port number on which congestion is detected
1    - unit number from which CNM is transmitted
0    - slot number from which CNM is transmitted
05   - port number on which CNM is transmitted
```

6-19 show qcn statistics

The **show qcn statistics** command is used in the Privileged EXEC mode to show the statistics of the CNM and the data frames of all the ports or of a specific CP of the given port.

show qcn statistics {*slot/port* **cp-index** *cp-index***}**

Parameters

interface *slot/port*	Display CP information for interface in slot/port format.
cp-index *cp-index*	Display the CP index for the interface.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following data is shown in a tabular format as the output for this command.

```
(Routing)#show qcn statistics interface 0/1 cp-index 1

Interfax     Cp Index     CNMs transmitted
----------   ----------   --------------------
0/1          1            1230
```

FIP Snooping Commands

The Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) is utilized in order to perform the functions of FC_BB_E device discovery, initialization, and maintenance. The FIP uses a separate EtherType from FCoE in order to enable the capacity to distinguish discovery, initialization, and maintenance traffic from other types of FCoE traffic. With only one exception, FIP frames are of the standard Ethernet size (that is, 1518 Byte 802.1q frame), while FCoE frames have a maximum size of 2240 bytes.

This document describes FIP snooping. FIP snooping is a frame inspection method that is used by FIP Snooping Bridges in order to monitor FIP frames and to apply policies based upon the L2 header information included in those frames, following the recommendations in Annex C of FC_BB_5 Rev 2.00. This makes the following actions possible:

1. The auto-configuration of Ethernet ACLs according to information included in the Ethernet headers of FIP frames.
2. The emulation of FC point-to-point links within the DCB Ethernet network.
3. The enhancement of FCoE security/robustness through the prevention of FCoE MAC spoofing.

In D-LINK OS, the FIP Snooping Bridge solution supports configuration-only of the perimeter port role and the FCF-facing port roles and is intended only for use at the edge of the switched network.

The roles of FIP Snooping-enabled ports on the switch are categorized under one of the following types:

1. Perimeter or Edge port (that is, connected directly to ENode).

2. FCF facing port (that is, a port that receives traffic from the FCFs targeted to the ENodes).

6-20 feature fip-snooping

The **feature fip-snooping** command is used in the Global Configuration mode in order to globally enable Fibre Channel over Ethernet Initialization Protocol (FIP) snooping on the switch. Any received FIP frames are forwarded or flooded using the normal multicast rules if FIP snooping is disabled.

When it is enabled, however, FC-BB-5 Annex D ACLs will be installed on the switch and the FIP frames will be snooped. Unless and until a port is operationally enabled for PFC, then FIP snooping will not permit FIP or Fibre Channel over Ethernet (FCoE) frames to be forwarded over that port. And, in order to carry dot1p values through the network, VLAN tagging must be enabled on the interface.

The **no** command is used to reset the settings back to the default values and to globally disable FIP snooping. Any received FIP frames will be forwarded or flooded using the normal multicast rules when FIP snooping is disabled. In addition, no other FIP snooping commands will be available until the FIP snooping feature has been enabled.

feature fip-snooping

no feature fip-snooping

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

Example

The following example of the command enables the FIP snooping feature.

```
s1(config)#feature fip-snooping
```

The following example of the **no** command disables the FIP snooping feature.

```
s1(config)#no feature fip-snooping
```

6-21 fip-snooping enable

The **fip-snooping enable** command is used in the VLAN Configuration mode in order to enable the snooping of FIP packets on the configured VLANs. (By default, FIP snooping is disabled on VLANs.)

Before FIP snooping can operate on an interface, Priority Flow Control (PFC) must be operationally enabled. Meanwhile, VLAN tagging has to be enabled on the interface in order for the dot1p value to be carried through the network.

This command may only be input after FIP snooping has been enabled using the “priority-flow-control mode” command. Otherwise, the command will not appear in the CLI syntax tree.

The **no** command resets the mode to the default setting (off).

fip-snooping enable

no fip-snooping enable

Parameters

None

Default

The default is Disable.

Command Mode

VLAN Config

Example

The following example of the command enables FIP snooping on VLANs 2 through 8.

```
s1(config)#vlan 2-8
s1(Config)(Vlan 2-8)#fip-snooping enable
```

The following example of the command disables FIP snooping on VLANs 2 through 8.

```
s1(config)#vlan 2-8
s1(config)(vlan 2-8)#no fip-snooping enable
s1(config)(vlan 2-8)#exit
```

6-22 fip-snooping fc-map

The **fip-snooping fc-map** command is used in the VLAN Configuration mode in order to configure the FP-MAP value on a VLAN. This value helps to secure the switch against misconfiguration.

If they have been configured using fabric-provided MAC addresses, then FCoE devices will transmit any frames containing the FC map value in the upper 24 bits. However, only those frames that match the configured FC map value will be passed across the VLAN, while any other frames will be discarded.

This command may only be input after FIP snooping has been enabled. Otherwise, the command will not appear in the CLI syntax tree.

The **no** command resets the FC-MAP value for the VLAN back to the default value.

fip-snooping fc-map *map value*

no fip-snooping fc-map

Parameters

map value	Valid FC map values are in the range of 0x0 to 0xffffff.

Default

The default is 0x0efc00.

Command Mode

VLAN Config

Example

The following example of the command configures an FC map value of 0x100 on VLAN 208.

```
(config)#vlan 208
(config)(vlan 208)#fip-snooping enable
(config)(vlan 208)#fip-snooping fc-map 0x100
```

The following example of the command configures an FC map value 0xFFCB for VLANs 2 through 8

```
(config)#vlan 2-8
(config)(vlan 2-8)#fip-snooping fc-map 0xecffcb
(config)(vlan 2-8)#exit
```

6-23 fip-snooping port-mode

The switch must know the interfaces to which the Fibre Channel Fabric (FCF) is connected in order to relay FIP packets received from the hosts toward the FCF. The **fip-snooping port-mode** command is used in the Interface Configuration mode to configure an interface to face towards the FCF. If an interface is not configured to be an FCF-facing interface, then it will, by default, be a host-facing interface.

In order to receive DCBX information and propagate it to the CNAs on the downstream (host-facing) ports, it is recommended that FCF-facing ports be placed into the auto-upstream mode.

Meanwhile, before FCoE traffic can pass over the port, interfaces enabled for PFC should be configured in the trunk mode or the general mode and must be PFC-operationally enabled.

The **fip-snooping port-mode** command can only be input after FIP snooping has been enabled using the "priority-flow-control mode" command. Otherwise, the command will not appear in the CLI syntax tree.

The **no** command is used to set the interface to face towards the host.

fip-snooping port-mode fcf

no fip-snooping port-mode fcf

Parameters

fcf	Fibre Channel Fabric.

Default

The default is as follows: host-facing interface.

Command Mode

Interface Config

Example

The following example of the command configures an interface to be connected with an FCF switch.

```
(Config)#interface 0/1
(Interface 0/1)#fip-snooping port-mode fcf
(Interface 0/1)#exit
```

The following example of the command sets an interface to be connected with the host.

```
(Config)#interface 0/1
(Interface 0/1)#no fip-snooping port-mode fcf
(Interface 0/1)#exit
```

6-24 show fip-snooping

The **show fip-snooping** command is used in the User EXEC or the Privileged EXEC mode to show information regarding the global FIP snooping configuration and status.

show fip-snooping

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch)#show fip-snooping

Global Mode:            Enable
FCoE VLAN List:         2,4,5-8
FCFs:                   2
ENoi:les :              2
Sessions :              10
Max VLANs:              8
Max FCFs in VLAN:       4
Max ENodes:          312
Max Sessions:        1024
```

Display Parameters

Global Mode	FIP snooping configuration status on the switch. It displays **Enable** when FIP snooping is enabled on the switch and **Disable** when FIP snooping is disabled on the switch.
FCoE VLAN List	List of VLAN IDs on which FIP snooping is enabled.
FCFs	Number of FCFs discovered on the switch.
ENodes	Number of ENodes discovered on the switch.
Sessions	Total virtual sessions on the switch.
Max VLANs	Maximum number of VLANs that can be enabled for FIP snooping on the switch.
Max FCFs in VLAN	Maximum number of FCFs supported in a VLAN.
Max ENodes	Maximum number of ENodes supported in the switch.
Max Sessions	Maximum number of Sessions supported in the switch.

Priority-Based Flow Control Commands

Typically, when a physical link is enabled with flow control, the flow control is applied to all of the traffic on the link. In the event of congestion, the hardware then sends pause frames that halt the traffic flow temporarily, which helps to prevent buffer overflow and the dropping of frames.

Priority-based flow control (PFC) provides a means by which to determine, based on the priority of the traffic, which traffic on a physical link will be paused when congestion occurs. It is possible to configure an interface to pause only high priority (that is, loss-sensitive) traffic as necessary to prevent dropped frames, while still allowing traffic with greater loss tolerance to continue flowing over the interface.

The priority field of the IEEE 802.1Q VLAN header differentiates among priorities, with the field identifying the given IEEE 802.1 p priority value. In D-LINK OS, it is required that these priority value be mapped to internal class-of-service (CoS) values.

The following steps should be taken to enable priority-based flow control for a specific CoS value on a given interface:

1. Ensure that VLAN tagging has been enabled on the interface to make sure that the 802.1p priority values are transmittied through the network.
2. Ensure that the 802.1p priority values are then mapped to the relevant D-LINK OS CoS value.

The interface defaults to the IEEE 802.3x flow control setting for the interface when priority-flow-control is disabled. When, in contrast, priority-based flow control has been enabled, the interface will not cause any CoS to be paused unless at least one no-drop priority is present.

6-25 priority-flow-control mode

The **priority-flow-control mode** command is used in the Datacenter-Bridging Config mode in order to enable Priority-Flow-Control (PFC) on a specific interface.

In order to carry the dot1p value through the network, VLAN tagging (whether trunk or general mode) has to be enabled on the interface. Additionally, the setting for dot1mapping to class-of-service must be one-to-one.

The normal PAUSE control mechanism is operationally disabled when PFC is enabled on an interface.

The **no** command is used to reset the PFC mode to the default mode (off).

priority-flow-control mode {on | off}

no priority-flow-control mode

Parameters

on	Enable PFC on the interface
off	Disable PFC on the interface.

Default

The default is Priority-flow-control mode Off (disabled).

Command Mode

Datacenter-Bridging Config

Example

The following example of the command enables PFC on an interface.

```
(Routing)(Config)#interface 0/1
(Routing)(Interface 0/1)#datacenter-bridging
(Routing)(config-if-dcb)#priority-flow-control mode on
```

6-26 priority-flow-control priority

The **priority-flow-control priority** command is used in the Datacenter-Bridging Config mode in order to enable the priority group for lossy (drop) or lossless (no-drop) behavior on the given interface. A maximum of two lossless priorities may be enabled on a single interface. In order to ensure end-to-end lossless behavior, the administrator must configure the no-drop priorities to be the same across the network.

The command does not have any effect on those interfaces not enabled for PFC. In addition, VLAN tagging must be turned on to transmit the dot1p value through the network, while the setting of dot1pmapping to class-of-service must be one-to-one.

The **no** command is used in the Datacenter-Bridging Config mode in order to enable lossy behavior for all priorities on the given interface. Use of the command will have no effect, however, on those interfaces not enabled for PFC or that have no lossless priorities configured.

priority-flow-control priority *priority-list* **(drop | no-drop}**

no priority-flow-control priority

Parameters

priority-list	Indicates the priority list.
drop	Disable lossless behavior on the selected priorities.
no-drop	Enable lossless behavior on the selected priorities.

Default

The default is Drop.

Command Mode

Datacenter-Bridging Config

Example

The following example of the command sets priority 3 to no-drop behavior.

```
(Routing)(ConFig)#interface 0/1
(Routing)(Interface 0/1)#datacenter-bridging
(Routing)(config-if-dcb)#priority-flow-control mode on
(Routing)(config-if-dcb)#priority-flow-control priority 3 no-drop
```

6-27 clear priority-flow-control statistics

The **clear priority-flow-control statistics** command is used to delete all global and interface PFC statistics.

clear priority-flow-control statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command.

```
(Routing)#clear priority-flow-control statistics
```

6-28 show interface priority-flow-control

The **show interface priority-flow-control** command is used in the Privileged EXEC mode in order to display the PFC information for a given interface or all of the interfaces.

show interface [*slot/port***] priority-flow-control**

Parameters

slot/port	Indicates a valid slot/port identifier.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following examples of the command cause the priority flow control status and statistics to be shown.

```
(Routing) #show interface 0/1 priority-flow-control

Interface Detail:                       0/1
PFC Configured State:                   Disabled
PFC Operational State:                  Enabled
Configured Drop Priorities:             2-7
Operational Drop Priorities:            2-7
Configured No-Drop Priorities:          0-1
Operational No-Drop Priorities:         0-1
Delay Allowance:                        32456 bit times
Peer Configuration Compatible:          True
Compatible Configuration Count:         3
Incompatible Configuration Count:       1

Priority     Received PFC Frames     Transmitted PFC Frames
----------   --------------------    --------------------------
0            0                       0
1            0                       0
2            0                       0
3            0                       0
4            0                       0
5            0                       0
6            0                       0
7            0                       0
```

```
(Routing)#show interface priority-flow-control

Port    Drop Priorities      No-Drop Priorities      Oper State
-----   ---------------      --------------------    ----------
0/1     1-4,7                5,6                     Enabled
0/2     1-4,6-7              5                       Enabled
...
0/48    1-4,7                5,6                     Enabled
```

Display Parameters

Interface Detail	The port for which data is displayed.
PFC Operational Status	The operational status of the interface.
PFC Configured State	The administrative mode of PFC on the interface.
Configured Drop Priorities	The 802.1p priority values that are configured with a drop priority on the interface. Drop priorities do not participate in pause.
Configured No-Drop Priorities	The 802.1p priority values that are configured with a no-drop priority on the interface. If an 802.1p priority that is designated as no-drop is congested, the priority is paused.
Operational Drop Priorities	The 802.1p priority values that the switch is using with a drop priority. The operational drop priorities might not be the same as the configured priorities if the interface has accepted different priorities from a peer device.
Operational No-Drop Priorities	The 802.1p priority values that the switch is using with a no-drop priority. The operational drop priorities might not be the same as the configured priorities if the interface has accepted different priorities from a peer device.
Delay Allowance	The operational status of the interface.
Peer Configuration Compatible	Indicates whether the local switch has accepted a compatible configuration from a peer switch.
Compatible Configuration Count	The number of received configurations accepted and processed as valid. This number does not included duplicate configurations.
Incompatible Configuration Count	The number of received configurations that were not accepted from a peer device because they were incompatible.
Priority	The 802.1p priority value.
Received PFC Frames	The number of PFC frames received by the interface with the associated 802.1p priority.
Transmitted PFC Frames	The number of PFC frames transmitted by the interface with the associated 802.1p priority.

OpenFlow Commands

The OpenFlow feature is used to enable management of the switch via a centralized OpenFlow Controller and used of the OpenFlow protocol.

6-29 openflow enable

The **openflow enable** command enables the OpenFlow feature. However, if the OpenFlow feature is not in the disabled state when the command is issued, then issuing it will have no effect on the OpenFlow feature.

The **no** command is used to disable the OpenFlow feature. The OpenFlow feature can be disabled administratively at any time.

openflow enable

no openflow enable

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

6-30 openflow static-ip

The **openflow static-ip** command is used to set the IP address that will be used for the OpenFlow feature. Only when the static lP mode is enabled will the static IP be applied. Also, in order for the static IP address to be used for the OpenFlow feature, the switch must have an operational IP interface with the specified address. Otherwise, the OpenFlow feature is operationally disabled.

ln the event that the OpenFlow feature is enabled upon issuing of this command and the specified static IP address is not the IP address already being used by the OpenFlow feature, then the feature will be automatically disabled and then re-enabled.

The **no** command is used to set the OpenFlow static IP address to 0.0.0.0. The OpenFlow feature will become operationally disabled if this command is issued when OpenFlow is enabled and using a static IP.

openflow static-ip *IPv4 Address*

no openflow static-ip

Parameters

IPv4 Address	Enter a valid IP address.

Default

The default is None.

Command Mode

Global Config

6-31 openflow controller

This command is used to specify up to twenty IP addresses with which the switch should establish an OpenFlow Controllers connection. One IP address and connection mode (TCP or SSL) are specified by each use of the command, while the default IP port number 6633 will be used if the IP Port is omitted. By

default, the connection mode is SSL. The controller table that is configured by this command will be used by the switch in the OpenFlow 1.0/1.3 modes.

The **no** command is used to delete the specified OpenFlow Controller IP address or to delete all of the Controller addresses. All of the entries for the specified IP address will be deleted if the IP Port number is omitted.

openflow controller *ip-address* **[***ip-port***] [***connection mode***]**

no openflow controller {*ip-address* **[***ip-port***] | all}**

Parameters

ip-address	Specify up to twenty IP addresses to which the switch should establish an OpenFlow Management connection.
portid	lP port to use for an OpenFlow Management connection. If the IP Port is omitted, then the default IP port number 6633 is used.
connection mode	TCP or SSL. The default is SSL.
all	Indicates deleting.

Default

The default is as follows: 6633 (adding), all (deleting).

Command Mode

Global Config

6-32 openflow default-table

This command is used to configure the Hardware Table that will be used as the target for any flows transmitted by an OpenFlow 1.0 controller that has not been enhanced to handle multiple hardware tables. The parameter can only be applied when the OpenFlow variant is set to **OpenFlow 1.0**.

openflow default-table *parameter*

Parameters

parameter	Possible values are full-match or layer-2-match.

Default

The default is Full-match.

Command Mode

Global Config

6-33 openflow ip-mode

This command is used to direct the OpenFlow feature to use the configured IP address. If this command is issued when the OpenFlow feature is already enabled, it will cause the feature to become disabled and then re-enabled with the new IP address.

The **no** command is used to direct the OpenFlow feature to assign the IP address to itself automatically.

openflow ip-mode {auto | static | serviceport}

no openflow ip-mode

Parameters

auto	Use network IP address.
static	Use static IP address.
serviceport	Use serviceport IP address.

Default

The default is Disabled.

Command Mode

Global Config

6-34 openflow passive-mode

This command is used to enable the OpenFlow passive-mode.

No command disables the OpenFlow passive-mode.

openflow passive-mode

no openflow passive-mode

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

6-35 openflow variant

This command is used to configure the OpenFlow feature to the variant specified. The user can configure the OpenFlow feature so that it uses one of two variants, **OpenFlow 1.0** or **OpenFlow 1.3**. By default, the OpenFlow feature is configured to use **OpenFlow 1.3**.

openflow variant {openflow10 | openflow13}

Parameters

None

Default

The default is OpenFlow 1.3.

Command Mode

Global Config

6-36 clear openflow ca-cert

This command is used to erase the Certificate Authority certificates that are used to validate the OpenFlow Controllers from the switch. Issuing of the command will automatically disable and then re-enable the OpenFlow feature. The new SSL certificates will then be reloaded from the OpenFlow Controller upon the first connection to the controller, or they can be loaded manually with a copy command.

clear openflow ca-cert

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

6-37 show openflow

This command is used to show the status and configuration information for the OpenFlow feature.

show openflow

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show openflow

Administrative Mode.............................. Enable
Administrative Status............................ Disabled
Disable Reason................................... No-Suitable-IP-Interface
IP Address....................................... None
IP Mode.......................................... Auto
Static IP Address................................ 10.1.1.1
OpenFlow Variant................................. Tenant Networking
Default Table.................................... layer-2-match
Passive Mode..................................... Enable
```

The following is an example of the CLI display output for the command

```
(Routing)#show openflow

Administrative Mode.............................. Enable
Administrative Status............................ Enabled
Disable Reason................................... None
IP Address....................................... 10.27.65.64
IP Mode.......................................... Auto
Static IP Address................................ 10.1.1.1
OpenFlow Variant................................. OpenFlow 1.0
Passive Mode..................................... Enable
```

Display Parameters

Administrative Mode	The OpenFlow feature administrative mode set by the command.
Administrative Status	The operational status of the OpenFlow feature. Although the feature may be administratively enabled, it could be operationally disabled due to various reasons.
Disable Reason	If the OpenFlow feature is operationally disabled, then this status shows the reason for the feature to be disabled.
IP Address	IPv4 Address assigned to the feature. If the IP address is not assigned,

	then the status is **None**.
IP Mode	IP mode assigned by the command. The IP mode can be **Auto**, **Static**, or **ServicePort IP**.
Static IP Address	Static IP address assigned by the command.
OpenFlow Variant	OpenFlow Protocol Variant. The OpenFlow protocol can be **OpenFlow 1.0** or **OpenFlow 1.3**.
Default Table	The Hardware Table used as the target for flows installed by an OpenFlow 1.0 controller which is not enhanced to handle multiple hardware tables.
Passive Mode	The OpenFlow passive mode set by the command.

6-38 show openflow configured controller

This command is used to display a list of the configured OpenFlow Controllers. Only when the OpenFlow variant is 1.0 or 1.3 will the switch communicate with these controllers.

show openflow configured controller

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show openflow configured controller

IP Address         IP Port      Connection Mode    Role
---------------    ----------   ---------------    ----------
172.21.4.217       6633         SSL                Master
```

Display Parameters

IP Address	IPv4 address of the controller.
IP Port	IPv4 port number for the controller connection.
Connection Mode	SSL or TCP Controller Connection mode.
Role	The role of the controller: Master, Equal, Slave.

6-39 show openflow installed flows

This command is used to show the list of configured flows on the switch.

show openflow installed flows [dest_ip *ip-address* **| dest_ip_port** *1-65535* **| dest_mac** *macaddr* **| dscp** *0-63* **| ether_type** *0-0xFFFF* **| ingress_port** *slot/port* **| ip_proto** *0-255* **| priority** *1-65535* **| source_ip** *ip-address* **| source_ip_port** *1-65535* **| source_mac** *macaddr* **| table** *4,24,25* **| vlan** *1-4093* **| vlan_prio** *0-7***]**

Parameters

dest_ip *ip-address*	The IP address of the destination.
dest_ip_port *1-65535*	The port number of the destination.
dest_mac *macaddr*	The MAC address of the destination.
dscp *0-63*	The DSCP value.
ether_type *0-0xFFFF*	The ethertype value.
ingress_port *slot/port*	The slot and port for the ingress.
ip_proto *0-255*	The IP protocol.
priority *1-65535*	The priority of the flow.
source_ip *ip-address*	The IP address of the source.
source_ip_port *1-65535*	The port number of the source.
source_mac *macaddr*	The MAC address of the source.
table *4,24,25*	The table number.
vlan *1-4093*	Indicates an interface in VLAN format (1-4093).
vlan_prio *0-7*	The VLAN priority.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command regarding the flow type 1DOT0.

```
(Routing) #show openflow installed flows

Flow type "1DOT0"

Match criteria:
Flow table            24 : Priority        1
Ingress port         0/0
```

```
Actions:
Action:             Drop
Status:
Duration:              2 : Idle            0 : installed in hardware            1

Flow type "1DOT0"

Match criteria:
Flow table            24 : Priority     102

Ingress port         0/0 : Ether type   88CC
Actions:
Status:
Duration               55 : Idle           45 : installed in hardware            1
```

The following is an example of the CLI display output for the command regarding the flow type 1DOT3.

```
(Routing)#show openflow installed flows

Flow type "1DOT3"

Match criteria:
Flow table     60 : Priority      10
Ingress port  0/1 : Src MAC       00:00:02:37:38:01 : Dst MAC 00:00:18:37:22:01
VLAN            1 : VLAN prio     1 : Ether type      0x0800
IP proto       17 : Src IP        100.0.0.225 : Dst IP       192.0.0.225
Src IP port     1 : Dst IP port   1 : TOS             32(DSCP: 8)

Actions:
New Src IP    3.3.3.3 : New SrcIP Mask 255.255.255.255 : New Dst IP       4.4.4.4
New DstIP Mask 255.255.255.255 : Egress port   0/1
Status:
Duration      5 : Idle            2 : installed in hardware  1

Flow type "1DOT3"

Match criteria:
Flow table     60 : Priority      10
Ingress port  0/1 : Src MAC       00:00:1A:38:38:01 : Dst MAC 00:00:30:38:22:01
VLAN            1 : VLAN prio     1 : Ether type      0x0800
IP proto       17 : Src IP        100.0.1.249 : Dst IP       192.0.1.249
Src IP port     1 : Dst IP port   1 : TOS             32(DSCP: 8)

Actions:
Egress port   0/1
Status:
Duration      2 : Idle            0 : installed in hardware  1
```

Display Parameters

Flow Type	The type of flow. (For example, 1.0 or Layer 2 Match).
Flow Table	The hardware table in which the flow is installed.
Flow Priority	The priority of the flow versus other flows.
Match Criteria	The match criteria specified by the flow.
Ingress Port	The port on which the flow is active.
Action	The action specified by the flow.
Idle	The time since the flow was hit.
Installed in hardware	If the flow could be added to the hardware. 1. 0 is displayed if the flow cannot be added. 2. 1 is displayed if the flow was added.

6-40 show openflow installed groups

This command is used to show a list of the configured groups on the switch

show openflow installed groups

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#show openflow installed groups

Max Indirect Group Entries..................... 1234
Current Indirect Group Entries in database..... 123

Max All Group Entries.......................... 1234
Current A11 Group Entries in database.......... 123

Max Select Group Entries....................... 1234
Current Select Group Entries in database....... 123

Group Id 12345678 type "Indirect"
=======================================
Ref Count                    1 : Duration                    8 : Bucket Count   1
```

```
Bucket Entry List:
--------------------
Bucket Index                25 : Output Port                1
Src MAC       00:00:00:00:00:AB : Dst MAC                   00:00:00:00:00:CD
VLAN                       101 : Reference Group Id         NA

Group Id 23456789 type "All"
=======================================
Ref Count                   NA : Duration                   10 : Bucket Count   2

Bucket Entry List:
--------------------
Bucket Index                26 : Output Port                2
Src MAC                     NA : Dst MAC                    NA
VLAN                       102 : Reference Group Id         NA

Bucket Index                27 : Output Port                3
Src MAC                     NA : Dst MAC                    NA
VLAN                       103 : Reference Group Id         NA

Group Id 34567890 type "Select"
=======================================
Ref Count                   NA : Duration                   10 : Bucket Count   3

Bucket Entry List:
--------------------
Bucket Index                28 : Output Port                NA
Src MAC                     NA : Dst MAC                    NA
VLAN                        NA: Reference Group Id          12345678

Bucket Index                29 : Output Port                NA
Src MAC                     NA : Dst MAC                    NA
VLAN                        NA: Reference Group Id          12345678

Bucket Index                30 : Output Port                NA
Src MAC                     NA : Dst MAC                    NA
VLAN                        NA: Reference Group Id          12345678
```

Display Parameters

Group Type	Type of the Group - Indirect, All, Select etc.
Group Id	Unique ID of the Group
Ref Count	Group Reference Count - is used only for Indirect groups This count indicates how many Select groups are referring to the current Indirect group.
Duration	The time since the group was created.
Bucket Count	Number of Buckets in the group.

Reference Group Id	References the Indirect group ID and used for Select group only.

6-41 show openflow table-status

This command is used to show the supported OpenFlow tables and the reported usage information for the tables.

show openflow table-status {openflow10 | opnflow13)

Parameters

openflow10	Indicates OpenFlow 1.0.
openflow13	Indicates OpenFlow 1.3

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show openflow table-status openflow10

Flow Table..................................... 1
Flow Table Name................................ Forwarding Database
Maximum Size................................... 64
Number of Entries.............................. 8
Hardware Entries............................... 7
Software-Only Entries.......................... 1
Waiting for Space Entries...................... 0
Flow Insertion Count........................... 1
Flow Deletion Count............................ 0
Insertion Failure Count........................ 0
Flow Table Description:
The forwarding database maps non-multicast MAC addresses and the ports on which these
addresses are located.
```

The following is an example of the CLI display output for the command.

```
(Routing)#show openflow table-status openflow13

Flow Table..................................... 60
Flow Table Name................................ Openflow 1.3
Maximum Size................................... 1920
```

```
Number of Entries.............................. 0
Hardware Entries............................... 0
Software-Only Entries.......................... 0
Waiting For Space Entries...................... 0
Flow Insertion Count........................... 0
Flow Deletion Count............................ 0
Insertion Failure Count........................ 0
Flow Table Description:
The Openflow 1.3 table matches on the packet layer-2 header, including DA-MAC, SA-MAC,
VLAN, Vlan priority ether type; layer-3 header, including SRC-IP, DST-IP, IP protocol,
IP-TOS; layer-4 header, including UDP/TCP source and dest port, ICMP type, and code;
SRC-IPv6, DST_IPv6, IPv6 Flow Label, ECN, ICMPv6 type and code, source L4 Port for TCP
/ UDP / SCTP and input port including physical port and LAG port.
```

Display Parameters

Flow Table	OpenFlow table identifier. The range is 0 to 255.
Flow Table Name	The name of this table.
Flow Table Description	A detailed description for this table.
Maximum Size	Platform-defined maximum size for this flow table.
Number of Entries	Total number of entries in this table. The count includes delete-pending entries.
Hardware Entries	Number of entries currently inserted into hardware.
Software-Only Entries	Number of entries that are not installed in the hardware for any reason. This includes entries pending for insertion, entries that cannot be inserted due to missing interfaces and entries that cannot be inserted due to table-full condition.
Waiting for Space Entries	Number of entries that are not currently in the hardware because the attempt to insert the entry failed.
Flow Insertion Count	Total number of flows that were added to this table since the switch powered up.
Flow Deletion Count	Total number of flows that were deleted from this table since the switch powered up.
Insertion Failure Count	Total number of hardware insertion attempts that were rejected due to lack of space since the switch powered up.

NVGRE/VXLAN Commands

In this section, the commands that are used to enable the network virtualization technologies (VXLAN/NVGRE) to communicate with another network are described.

6-42 nvgre enable

This command is used to enable the NVGRE mode on the switch. This mode must be enabled before any NVGRE configuration can be performed on the switch.

The **no** command is used to disable the NVGRE mode on the switch. It also clears the switch of all existing NVGRE configurations, including all NVGRE tunnels, tenants, tenant VLAN associations, and configured forwarding entries.

Note: The NVGRE mode and VXLAN mode are mutually exclusive modes. That is, the NVGRE mode cannot be enabled on the switch if the VXLAN mode is enabled. Rather, the VXLAN mode must be disabled before enabling the NVGRE mode.

nvgre enable

no nvgre enable

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

6-43 nvgre source-interface

This command is used to specify a VXLAN source interface.

nvgre vxlan source-interface loopback *loopback-id*

no nvgre vxlan source-interface loopback *loopback-id*

Parameters

loopback-id	Enter Loopback Interface ID (0-63).

Default

The default is None.

Command Mode

Global Config

6-44 vxlan enable

This command is used to enable the VXLAN mode on the switch. The VXLAN mode, which is disabled by default, must be enabled before any VXLAN configuration can be performed on the switch.

Note: The NVGRE mode and VXLAN mode are mutually exclusive modes. That is, the VXLAN mode cannot be enabled on the switch if the NVGRE mode is enabled. Rather, the NVGRE mode must be disabled before enabling the VXLAN mode.

The **no** command is used to disable the VXLAN mode on the switch. It also clears the switch of all existing VXLAN configurations, including all VXLAN tunnels, tenants, tenant VLAN associations, and configured forwarding entries.

vxlan enable

no vxlan enable

Parameters

None

Default

The default is None.

Command Mode

Global Config

6-45 vxlan source-interface loopback

This command is used to specify the outer source IP address for any encapsulated packets transmitted on a VXLAN with a given virtual network ID (VNID). The source-interface consists of the intended local VTEP for the tenant specified with the VNID. If there is no VXLAN with the given VNID, then the system will create it.

The allowed configurable range for the VSID 1 to 16777214, while the use of 16777215 is reserved for internal purposes.

The **no** command is used to delete the configuration of the local VTEP identified by ip-address from the VXLAN specified by the VNID.

Note: It is recommended that a loopback interface be configured with the intended local VXLAN Gateway IP address for use as the source-ip for all tenants. Tenants can also be configured, if necessary, with a different source-ip if multiple loopback interfaces have been configured and are used as local VXLAN Gateways. Meanwhile, any loopback interfaces that are meant to be used as local VXLAN Gateways should be used solely for that purpose and not for any others.

vxlan source-interface loopback *loopback-id*

no vxlan source-interface loopback *loopback-id*

Parameters

loopback-id	Enter Loopback Interface ID (0-63).

Default

The default is No source IP address.

Command Mode

Global Config

6-46 vxlan tenant-system

This command is used to configure the forwarding entity for the tenant system MAC address mac-addr in the specified VN that can be reached through the access interface. The tenant systems can be configured one by one. Typically, the system learns the MAC address for tenant systems automatically from the traffic received on the access interface. The tenant systems MAC address mac-addr can be configured when accessing the interface to prevent initial flooding. If a tenant system has been configured on an interface, then the configuration overrides the learning for the indicated MAC address in that VN.

Note: This command is only valid for physical and port-channel interfaces, and the configured interface ought to also be a member of VLAN associated with the specified VNID.

The MAC addresses for the tenant system are maintained in a separate table and are not listed in the FDB mac-address table. These addresses internally consume shared resources for system hardware layer 2 address tables. As such, the maximum number of tenant systems configured or learned is dependent upon the number of resources that remain in the hardware layer 2 table, with that number being dynamic in nature.

The allowed configurable range for the VNID is 1 to 16777214, while the use of 16777215 is reserved for internal purposes.

A maximum of 24 tenant systems per physical or port-channel interface can be configured.

The **no** command is used to delete the configured tenant system forwarding entry on an interface when both the VNID and the tenant system mac-address are specified. The command cannot be utilized in order to delete a dynamically-learned tenant system association on the interface in a specified VNID VN.

Note: When the removal of an access port configuration of the VN specified by VNID occurs, then all of the forwarding entries configured by the user and learned by the switch on that access port, if any, are also removed due to the removal of the port participation of the associated VLAN.

vxlan *vnid* **tenant-system** *mac-addr*

no vxlan *vnid* **tenant-system** *mac-addr*

Parameters

vnid	Indicates the VXLAN VNID.
mac-addr	Indicates the MAC Address of the tenant system.

Default

The default is Tenant MAC addresses not associated with the VN.

Command Mode

Interface Config

6-47 vxlan udp-dst-port

This command is used to configure a specific UDP port to be the VXLAN UDP destination port of the switch. All the VXLANs on the switch, when encapsulating, will then utilize this UDP port as the UDP

destination port in the UDP header. The switch will also terminate any incoming VXLAN packets that match the specified UDP destination port.

Moreover, the command also updates all of the existing VXLAN tunnels in the hardware with the newly configured UDP destination port, and no or very little traffic disruption occurs during this operation.

The allowed configurable range for the VNID is 1 to 16777214, while the use of 16777215 is reserved for internal purposes.

The allowed configurable range for the UDP port is 1024 to 65535.

The **no** command is used to reset the switch's VXLAN UDP destination port configuration back to the default value. The command updates all of the existing VXLAN tunnels in the hardware with to use the default VXLAN UDP destination port, and no or very little traffic disruption occurs during this operation.

vxlan udp-dst-port *port-number*

no vxlan udp-dst-port

Parameters

port-number	Indicates a UDP port number.

Default

The default is 4789 (IANA-assigned UDP port to VXLAN).

Command Mode

Global Config

6-48 vxlan vlan

This command is used to associate an access VLAN to a specific by VXLAN tenant. In the event that the VXLAN specified has not been created already, then it will be created upon issuing of this command. A maximum of 1024 DCVPNs can be created on the switch.

Those packets that have the specified VLAN vlan-id tag will be associated to the VXLAN VNID upon arrival. This command causes only the traffic from the specified VLAN to be associated with the given VN identified by VSID. For the command to have any effect, the VLAN vlan-id must have already been created. Also, access ports for the VN specified by the VNID must be configured by configuring the VLAN vlan-id membership on the eligible interfaces before or after this command is issued.

Note: For all member ports of the VLAN vlan-id, it is recommended that ingress filtering be configured.

The allowed configurable range for the VNID is 1 to 16777214, while the use of 16777215 is reserved for internal purposes..

The **no** command is used to remove an associated VLAN from the specified VXLAN. All of the configured access ports of the VN specified by the VNID will be removed.

vxlan *vnid* **vlan** *vlan-id*

no vxlan *vnid* **vlan**

Parameters

vnid	Indicates VXLAN VNID (1-16777214).
vlan-id	Indicates a VLAN ID (1-4093).

Default

The default is None.

Command Mode

Global Config

6-49 vxlan vtep

This command is used to configure a specific IP address to be the remote virtual tunnel endpoint (VTEP) within the VXLAN. In the event that the VXLAN specified has not been created already, then it will be created upon issuing of this command. A maximum of 1024 DCVPNs can be created on the switch, and multiple remote VTEPs can be configured one by one, as necessary, for the same VNID.

Note: The switch supports the configuration of a Multicast IP address to automatically discover remote VTEPs in order to define a flood group for DCVPN. The command should be utilized in order to manually configure all remote VTEPS behind which the Tenant (VNID) hosts are present for each DCVPN.

One or more tenant systems reachable through the VTEP can be optionally specified by the user. For a particular VXLAN, the tenant systems can be added or deleted one by one. Typically, the system learns tenant systems automatically from received messages, but if a tenant system has been configured, then the configuration overrides such learning for the given MAC address.

The MAC addresses for the tenant system are maintained in a separate table and are not listed in the FDB mac-address table. These addresses internally consume shared resources for system hardware layer 2 address tables. As such, the maximum number of tenant systems is dependent upon the number of resources that remain in the hardware layer 2 table, with that number being dynamic in nature.

A maximum of 600 remote tenant system entries may be configured per VN, while an overall total of 4096 entries may be configured on the switch.

The allowed configurable range for the VNID is 1 to 16777214, while the use of 16777215 is reserved for internal purposes.

The **no** command is used to remove a remote VTEP from a VXLAN. The command also causes all tenant system MAC address associations with the specified VTEP and DCVPN to be cleared from the system. Moreover, the command will delete the manual association of a tenant system to a remote VTEP if the optional [tenant-system mac-addr] parameter is used. The command cannot be utilized in order to delete a dynamically-learned tenant system association.

vxlan *vnid* **vtep** *ipadd* **[tenant-system** *mac-addr***]**

no vxlan *vnid* **vtep** *ipadd* **tenant-system** *mac-addr*

Parameters

vnid	Indicates VXLAN VNID (1-16777214).
ipadd	Indicates an IP Address.

tenant-system *mac-addr*	Indicates the MAC address for the tenant system configuration.

Default

The default is None.

Command Mode

Global Config

6-50 clear counters nvgre

This command is used to clear the packet and byte counters for all of the configured NVGRE virtual networks.

clear counters nvgre

The command causes the following counter information to be cleared for all configured NVGRE NVEs:

Packets TX	Number of unicast packets sent to the NVE.
Packets RX	Number of unicast packets received from the NVE.
Bytes TX	Number of unicast bytes sent to the NVE.
Bytes RX	Number of unicast bytes received from the NVE.

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

6-51 clear counters vxlan

This command is used to clear the packet and byte counters for all of the configured VXLAN virtual networks.

clear counters vxlan

The command causes the following counter information to be cleared for all configured VXLAN VTEPs:

Packets TX	Number of unicast packets sent to the VTEP.

Packets RX	Number of unicast packets received from the VTEP.
Bytes TX	Number of unicast bytes sent to the VTEP.
Bytes RX	Number of unicast bytes received from the VTEP.

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

6-52 show nvgre

This command is used to show the configuration and status of one or more NVGRE VNs. It also shows information regarding allowed limits and statistics

show nvgge [*vsid*]

Parameters

vsid	(Optional) Indicates a NVGRE VSID (1-16777214).

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)(ConFig)#show nvgre

NVGRE Admin Mode.............................. Enable

Maximum Allowed Limits or Table Sizes
-----------------------------------------------------
Tenant Table Size.............................. 1024
Access Ports Table Size........................ 2048
Tunnel/Network Reference Ports Table Size..... 8192

Current Entries Count or Table Usage
-----------------------------------------------------
Tenant Table Entries........................... 1
```

```
Access Port Entries.............................. 1
Tunnel/Network Reference Port entries............ 2

NVGRE ID     Source Address     VLAN       Access Port(s)     Remote TEP(s)
----------   ---------------    -----      ---------------    ---------------
1            192.168.10.1       10         0/2                10.10.10.1
                                                               100.100.100.1
```

```
(Routing)#shcw nvgre 1

Source Address................................... 192.168.10.1
Tenant VLAN...................................... 10
Access Port(s)................................... 0/2
Remote TEP(s).................................... 10.10.10.1
                                                  100.100.100.1
```

Display Parameters

NVGRE Admin Mode	Admin mode of NVGRE Enable/Disable.
NVGRE ID	Virtual Subnet ID (VSID).
Source Address	Source IP address of the local TEP.
VLAN	Associated VLAN ID to classify access ports.
Access Ports	List of access ports associated with this VN.
Remote TEP(s)	List of remote NVEs participating in this VN.

6-53 show nvgre nve

This command is used to display the status for a specified remote NVE within a specified NVGRE virtual network.

show nvgre *vsid* **nve [***ip-address***]**

Parameters

vsid	Indicates a NVGRE VSID (1-16777214).
ip-address	(Optional) Indicates the IP address for remote NVE.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)(ConFig)#show nvgre 1 nve

Remote NVE        Uptime (sec)    Reachable    Reachable Transitions
----------------------------------------------------------------------
10.10.10.1        0               NO           0
100.100.100.1     0               N0           0
```

```
(Routing)(Config)#show nvgre 1 nve 10.10.10.1

NVGRE ID..................................... 1
Remote NVE................................... 10.10.10.1
Reachable.................................... NO
Uptime (sec) ................................ 0
Reachable Transitions........................ 0

Unicast Counters
----------------------------------------------------------------------
Packets Tx................................... 0
Packets Rx................................... 0
Bytes Tx..................................... 0
Bytes Rx..................................... 0
```

Display Parameters

NVGRE ID	Virtual subnet ID (VSID).
Remote NVE	Remote NVE IP address.
Uptime	How long the NVE has been reachable.
Reachable	Whether the NVE is currently reachable.
Reachable Transitions	Number of times the NVE has transitioned to reachable state.
Packets TX	Number of unicast packets sent to the NVE.
Packets RX	Number of unicast packets received from the NVE.
Bytes TX	Number of unicast bytes sent to the NVE.
Bytes RX	Number of unicast bytes received from the NVE.

6-54 show nvgre tenant-systems

This command is used to list all of the tenant systems that are currently configured or dynamically learned within a given VN. If the optional mac-addr for a VN is specified, then the command can also be used to find a specific host or tenant system.

show nvgre *vsid* **tenant-systems [***mac-addr***]**

Parameters

vsid	Indicates a NVGRE VSID (1-16777214).
mac-addr	(Optional) Indicates a MAC Address for the tenant systems.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)(Config)#show nvgre 1 tenant-systems

Tenant MAC             NVE          Interface    Type         Age (sec)
---------------------  -----------  -----------  -----------  -----------
00:00:00:00:00:02                   0/2          Learned      278
00:00:DC:2C:00:32      10.10.10.1                Learned      13423
```

Display Parameters

Tenant MAC	MAC address of a host or tenant system.
NVE	IP address of NVE if the tenant system is behind the remote NVE. This is valid for remote tenant system, otherwise it is blank.
Interface	Access interface on which MAC entry is learned or configured. This is valid for tenant system on local access interface, otherwise, it is blank.
Type	Configured or learned.
Age	How long since the entry was learned. Not applicable for configured entries.

6-55 show nvgre tenant-systems

This command is used to list all of the tenant systems that are currently configured or dynamically learned within all of the configured VNs. In addition, the command shows information regarding the allowed limits on tenant system configuration and forwarding table statistics.

Entries can also be optionally filtered according to tenant system location, that is, local or remote. Local entries can be reached through the configured local access ports, while remote entries are located behind the remote NVEs and can be reached through the NVGREs configured to the remote NVEs.

show nvgre tenant-systems [local | remote]

Parameters

local	(Optional) Display local tenant systems details.
remote	(Optional) Display remote tenant systems details.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#show nvgre tenant-systems

Maximum Allowed Limits or Table Sizes
-----------------------------------------------------
Static Local Host Entries per Interface.......... 24
Static Remote Host Entries per Tenant............ 600
Static Remote Host Entries per Switch............ 4096
Forwarding Table Size............................ 32768

Current Entries Count or Table Usage
-----------------------------------------------------
Static Host Entries.............................. 4
Learned Host Entries............................. 2
Forwarding Table Entries......................... 6

Tenant ID    Tenant MAC            NVE         Interface   AppIfIndex    Entry Type
----------   -------------------   ----------  ----------  ----------    ----------
1            00:00:00:11:22:33                 0/13        8537          Static
1            00:00:00:11:22:44                 0/13        8537          Static
1            00:72:44:3A:D2:43                 0/13        8537          Learned
1            00:00:AA:BB:CC:DD     1.1.1.1                 345           Static
1            00:00:AA:BB:CC:EE     1.1.1.1                 345           Static
1            00:EA:08:CA:16:45     1.1.1.1                 345           Learned
```

```
(Routing)#show nvgre tenant-systems local

Tenant ID    Tenant MAC            NVE         AppIfIndex  Entry Type
----------   -------------------   ----------  ----------  ----------
1            00:00:00:11:22:33     0/13        8537        Static
1            00:00:00:11:22:44     0/13        8537        Static
1            00:72:44:3A:D2:43     0/13        8537        Learned
```

```
(Routing)#show nvgre tenant-systems remote

Tenant ID    Tenant MAC            NVE         AppIfIndex  Entry Type
----------   -------------------   ----------  ----------  ----------
```

```
1            00:00:AA:BB:CC:DD     1.1.1.1     345         Static
1            00:09:AA:BB:CC:EE     1.1.1.1     345         Static
1            00:EA:08:CA:16:45     1.1.1.1     345         Learned
```

Display Parameters

Tenant ID	Virtual Subnet ID (VSID).
Tenant MAC	MAC address of a host or tenant system.
NVE	IP address of NVE if the tenant system is behind the remote NVE. This is valid for the remote tenant system, otherwise it is blank..
Interface	Access interface on which the MAC entry is learned or configured. This valid for the tenant system on the local access interface, otherwise it is blank.
ApplfIndex	Internal access or tunnel port handle.
Entry Type	Configured or learned.

6-56 show vxlan

This command is used to display the configuration and status of one or more VXLAN VNs. The command also shows information regarding allowed limits and statistics.

show vxlan [*vnid***]**

Parameters

vnid	(Optional) Indicates VXLAN VNID.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)(Config)#show vxlan

VXLAN Admin Mode.............................. Enable
Destination UDP Port.......................... 4789

Maximum Allowed Limits or Table Sizes
-------------------------------------------------------------
Tenant Table Size............................. 1024
Access Ports Table Size....................... 2048
```

```
Tunnel/Network Reference Ports Table Size..... 8192

Current Entries Count or Table Usage
-------------------------------------------------------------
Tenant Table Entries.......................... 1
Access Port Entries........................... 1
Tunnel/Network Reference Port entries......... 2


VXLAN ID     Source Address    VLAN      Access Port(s)    Remote TEP(s)
----------   ---------------   -----     ---------------   ---------------
1            192.168.10.1      10        0/2               20.20.20.1
                                                           200.200.200.1
```

```
(Routing)#show vxlan 1

Source Address................................ 192.168.10.1
Tenant VLAN................................... 10
Access Port(s)................................ 0/2
Remote TEP(s)................................. 20.20.20.1
.............................................. 200.200.200.1
```

Display Parameters

VXLAN Admin Mode	Admin mode of VXLAN Enable/Disable.
Destination UDP Port	UDP destination port used in VXLAN header.
VXLAN ID	Virtual network ID (VNID)
Source Address	Source IP address of the local TEP.
Access Ports	List of access ports associated with this VXLAN.
VLAN	Associated VLAN ID to classify access ports.
Remote TEP(s)	List of remote VTEPs participating in this VXLAN.

6-57 show vxlan tenant-systems

This command is used to display a list of all the tenant systems currently configured or dynamically learned within a given DCVPN (which is identified by VNID). The tenant systems which are located behind the VTEP and that can also be reached through local access interfaces will be listed.

show vxlan *vnid* **tenant-systems [***mac-addr***]**

Parameters

vnid	Indicates VXLAN VNID.

mac-addr	(Optional) Indicates a MAC address identifier of tenant system.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Routing)(Config)#show vxlan 1 tenant-systems

Tenant MAC             VTEP              Interface       Entry Type    Age (sec)
--------------------   ---------------   ----------      ----------    ----------
00:00:00:00:00:02                        0/2             Learned       278323
00:00:00:1A:00:11      20.20.20.1                        Learned       12423
```

Display Parameters

Tenant MAC	MAC address of tenant system.
VTEP	Remote VTEP IP address.
Interface	Access interface on which MAC entry is learned or configured.
Entry Type	Configured or learned.
Age	How long since the entry was learned. Not applicable for configured entries.

6-58 show vxlan tenant-systems

This command is used to display a list of all the tenant systems that are currently configured or dynamically learned within in all the configured VNs. It also shows information regarding the allowed limits on tenant system configuration and forwarding table statistics.

Entries can also be optionally filtered according to tenant system location, that is, local or remote. Local entries can be reached through the configured local VN access ports, while remote entries are located behind the remote VTEPs and can be reached through the VXLANs configured to the remote VTEPs.

show vxlan tenant-systems [local | remote]

Parameters

local	(Optional) Display local tenant systems details.
remote	(Optional) Display remote tenant systems details.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is a command example.

```
(Routing)#show vxlan tenant-systems

Maximum AllowedLimits or Table Sizes
-----------------------------------------------------
Static Local Host Entries per Interface.......... 24
Static Remote Host Entries per Tenant............ 600
Static Remote Host Entries per Switch............ 4096
Forwarding Table Size............................ 32768

Current Entries Count or Table Usage
-----------------------------------------------------
Static Host Entries.............................. 4
Learned Host Entries............................. 2
Forwarding Table Entries......................... 6

Tenant ID    Tenant MAC            VTEP        Interface   AppIfIndex     Entry Type
----------   -------------------   ----------  ----------  ----------     ----------
1            00:00:00:23:27:a2     0/11        8545        Static
1            00:00:AC:BD:12:78     0/11        8548        Static
1            00:12:88:37:BD:C5     0/14        8547        Learned
1            00:00:42:B2:22:A3     12.12.12.1  346         Static
1            00:23:72:5B:62:1E     12.12.12.1  346         Static
1            00:1A:09:A3:11:21     12.12.12.1  346         Learned
```

```
(Routing)#show vxlan tenant-systems local

Tenant ID    Tenant MAC            Interface   AppIfIndex  Entry Type
----------   -------------------   ----------  ----------  ----------
1            00:00:00:23:27:a2     0/11        8545        Static
1            00:00:AC:BD:12:78     0/11        8548        Static
1            00:12:88:37:BD:C5     0/14        8547        Learned
```

```
(Routing) #show vxlan tenant-systems remote

Tenant ID    Tenant MAC            VTEP        AppIfIndex  Entry Type
----------   -------------------   ----------  ----------  ----------
1            00:00:42:B2:22:A3     12.12.12.1  346         Static
1            00:23:72:5B:62:1E     12.12.12.1  346         Static
1            00:1A:09:A3:11:21     12.12.12.1  346         Learned
```

Display Parameters

Tenant ID	Virtual Subnet ID (VSID).
Tenant MAC	MAC address of a host or tenant system.
VTEP	IP address of the VTEP if the tenant system is behind the remote VTEP. This is valid for the remote tenant system, otherwise it is blank.
Interface	Access interface on which the MAC entry is learned or configured. This valid for the tenant system on the local access interface, otherwise it is blank.
ApplfIndex	Internal access or tunnel port handle.
Entry Type	Configured or learned.

6-59 show vxlan vtep

This command is used to show the status of the remote VTEPs included in a given VXLAN virtual network.

show vxlan *vnid* **vtep [***ip-address***]**

Parameters

vnid	Indicates VXLAN VNID.
ip-address	(Optional) Indicates an IP address identifier of tenant system.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)(Config)#show vxlan 1 vtep

Remote VTEP      Dest UDP Port    Uptime (sec)    Reachable    Reachable Transitions
---------------  ---------------  ------------    ---------    ----------------------
20.20.20.1       4789             0               NO           0
200.200.200.1    4789             0               NO           0
```

```
(Routing)(ConFig)#show vxlan 1 vtep 20.20.20.1

VXLAN ID..................................... 1
Remote VTEP.................................. 20.20.20.1
Destination UDP Port......................... 4789
Reachable.................................... NO
```

```
Uptime (sec)..................................... 0
Reachable Transitions............................ 0

Unicast Counters
------------------------------------------------------
Packets Tx....................................... 0
Packets Rx....................................... 0
Bytes Tx......................................... 0
Bytes Rx......................................... 0
```

Display Parameters

VXLAN ID	Virtual Network ID (VNID).
Remote VTEP	Remote VTEP IP address.
Destination UDP Port	UDP destination port used in UDP header.
Uptime	How long the VTEP has been reachable.
Reachable	Whether the VTEP is currently reachable.
Reachable Transitions	Number of times the VTEP has transitioned to reachable state.
Packets TX	Number of unicast packets sent to the VTEP.
Packets RX	Number of unicast packets received from the VTEP.
Bytes TX	Number of unicast bytes sent to the VTEP.
Bytes RX	Number of unicast bytes received from the VTEP.

7. IPv4 Routing Commands

This section describes the following routing commands available in the D-LINK OS CLI:

Address Resolution Protocol Commands

This section describes the commands to configure Address Resolution Protocol (ARP) and view ARP information. ARP associates IP and MAC addresses then stores the information as ARP entries in the ARP cache.

7-1 arp

Create an ARP entity for the specified virtual router instance (**vrf** *vrf-name*). A static ARP entity is created in the default router when a virtual router is not specified. The *ipaddress* value is the IP address of a device on a subnet attached to an existing routing interface. The *parametermacaddr* is the unicast MAC address for that device. The next hop interface is determined by the interface parameter.

No command deletes an ARP entry in the specified virtual router. The value for arp entry is the IP address of the interface. The *ipaddress* value is the IP address of a device on a subnet attached to an existing routing interface. The *parametermacaddr* is the unicast MAC address for that device. The next hop interface is determined by the interface parameter.

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

arp [vrf *vrf-name***]** *ipaddress macaddr* **interface {***slot/port* **| vlan** *id***}**

no arp [vrf *vrf-name***]** *ipaddress* **interface {***slot/port* **| vlan** *id***}**

Parameters

vrf *vrf-name*	(Optional) Indicates a VPN Routing/Forwarding instance name.
Ipaddress	Configure IP address for a static ARP entry.
Macaddr	Configure MAC address for a static ARP entry.
slot/port	Enter an interface in slot/port format.
vlan *id*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Global Config

7-2 arp cachesize

Configure the ARP cache size; the value is a platform specific integer value. The default size varies across platforms.

No command configures the default ARP cache size.

arp cachesize *platform specific integer value*

no arp cachesize

Parameters

platform specific integer value	Indicates the cache size value as an integer.

Default

The default is None.

Command Mode

Global Config

7-3 arp dynamicrenew

Enable the ARP component to automatically renew dynamic ARP entries when timed out. The system determines whether to retain or delete timed out ARP entries. If the entry was used to forward data packets, the system renews the entry by sending a neighbor an ARP request. If a response is received, the age of the 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 used to forward data packets, the entry is deleted from the cache, unless the dynamic renew option is enabled. When dynamic renew is enabled, the system sends an ARP request to renew the entry. If the 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 only applies to host entries.

No command prevents dynamic ARP entries from renewing when they time out.

arp dynamicrenew

no arp dynamicrenew

Parameters

None

Default

The default is Disabled.

Command Mode

Privileged EXEC

7-4 arp purge

Remove the specified IP address from the ARP cache in the specified virtual router. If a router is not specified, the ARP entry is deleted in the default. Only dynamic or gateway entry types are affected by this command.

arp purge [vrf *vrf-name***]** *ipaddress* **interface {***slot/port* **| vlan** *id***}**

Parameters

vrf *vrf-name*	(Optional) The virtual router from which IP addresses will be removed.
ipaddress	IP address to remove from the ARP cache.
slot/port	Interface from which IP addresses will be removed.
vlan *id*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

7-5 arp resptime

Configure the ARP request response timeout.

The value is a positive integer, which represents the IP ARP entry response timeout time in seconds.

No command configures the default ARP request response timeout.

arp resptime *1-10*

no arp resptime

Parameters

None

Default

The default is 1.

Command Mode

Global Config

7-6 arp retries

Configure the ARP count of maximum retry requests, represented by an integer.

No command configures the default ARP count of maximum retry requests.

arp retries *0-10*

no arp retries

Parameters

None

Default

The default is 4.

Command Mode

Global Config

7-7 arp timeout

Configure the ARP entry age out time.

The value is a positive integer, which represents the IP ARP entry age out time in seconds.

No command configures the default ARP entry age out time.

arp timeout *15-21600*

no arp timeout

Parameters

None

Default

The default is 1200.

Command Mode

Global Config

7-8 clear arp-cache

Cause all ARP entries of type dynamic to be removed from the ARP cache for the virtual router. lf no router is specified, the cache for the default router is cleared. If the **gateway** keyword is specified, the dynamic gateway type entries are purged as well.

clear arp-cache [vrf *vrf-name***] [gateway]**

Parameters

vrf *vrf-name*	(Optional) Clears the dynamic entries from the ARP cache of a virtual router.
gateway	(Optional) Clears the dynamic and gateway entries from the ARP cache.

Default

The default is None.

Command Mode

Privileged EXEC

7-9 clear arp-switch

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** the DUT from the remote system. 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.

clear arp-switch

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

7-10 show arp

Display the Address Resolution Protocol (ARP) cache for a specified virtual router instance. If a virtual router is not specified, the default router ARP cache is displayed. To view the total ARP entries, the operator should view the **show arp** results in conjunction with the **show arp switch** results.

show arp [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display ARP entries for a Virtual Router instance.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Age Time (seconds)	Time it takes for an ARP entry to age out. This is configurable.
Response Time (seconds)	Time it takes for an ARP request timeout. This value is configurable.
Retries	Maximum number of times an ARP request is retried. This value is configurable.
Cache Size	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	Total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	Static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

IP Address	IP address of a device on a subnet attached to an existing routing interface.
MAC Address	Hardware MAC address of the device.
Interface	Routing slot/port associated with the device ARP entry.
Type	Configurable type. The possible values are Local, Gateway, Dynamic and Static.
Age	Age of the ARP entry since last refresh (in hh:mm:ss format).

7-11 show arp brief

Display brief Address Resolution Protocol (ARP) table information.

show arp brief

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show arp brief

Age Time (seconds)..............................1200
Response Time (seconds).........................1
Retries.........................................4
Cache Size......................................20480
Dynamic Renew Mode..............................Disable
Total Entry Count Current / Peak................0 / 2
Static Entry Count Configured / Active / Max.....0 / 0 / 128
```

Display Parameters

Age Time (seconds)	Time it takes for an ARP entry to age out. This value is configurable.
Response Time (seconds)	Time it takes for an ARP request timeout. This value is configurable.
Retries	Maximum number of times an ARP request is retried. This value is configurable.
Cache Size	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	Total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	Static entry count in the ARP table and maximum static entry count in the ARP table.

7-12 show arp switch

Display the contents of the switch's Address Resolution Protocol (ARP) table.

show arp switch

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing) #show arp switch

MAC Address             IP Address          Interface
--------------------    ---------------     ---------------
00:14:A8:E1:C2:4A       172.20.192.29       Management
00:A0:C9:00:01:AA       172.20.192.107      Management
00:05:64:2F:0D:88       172.20.192.101      Management
F4:4E:05:9F:27:75       172.20.192.72       Management
08:00:27:A6:BB:CD       172.20.192.19       Management
00:14:C2:65:61:61       172.20.192.123      Management
8C:3B:AD:65:6D:35       172.20.192.121      Management
00:05:64:30:73:BC       172.20.192.117      Management
00:05:64:30:73:BC       172.20.192.119      Management
48:6E:73:01:00:A2       172.20.192.115      Management
00:A0:C9:00:01:AA       192.168.0.1         Management
08:00:27:70:20:0E       172.20.192.237      Management
6C:EC:5A:07:E1:06       172.20.192.104      Management
6C:EC:5A:07:E1:06       172.20.192.106      Management
00:05:64:30:73:BC       172.20.192.102      Management
00:A0:C9:00:00:00       172.20.192.122      Management
6C:EC:5A:07:E1:06       172.20.192.118      Management
6C:EC:5A:07:E1:06       172.20.192.116      Management
6C:EC:5A:07:D3:A5       172.20.192.112      Management
6C:EC:5A:07:E1:06       172.20.192.114      Management
00:99:88:77:66:6C       192.168.2.2         Management
8C:3B:AD:65:6D:35       192.168.0.239       Management
08:00:27:F2:4E:09       172.20.192.56       Management
6C:EC:5A:07:D3:24       172.20.192.109      Management
6C:EC:5A:07:D3:24       172.20.192.111      Management
```

Display Parameters

IP Address	IP address of a device on a subnet attached to the switch.
MAC Address	Hardware MAC address of the device.
Interface	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.

7-13 routing

Enable IPv4 routing for an interface or range of interfaces.

No command disables routing for an interface.

You can view the current value for this function with the "show ip brief". The value is labeled as "Routing Mode."

routing

no routing

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

7-14 ip routing

Enable the IP Router Admin Mode for the master switch.

No command disables the IP Router Admin Mode for the master switch.

ip routing

no ip routing

Parameters

None

Default

The default is None.

Command Mode

- Global Config
- Virtual Router Config

7-15 ip address

Configure an IP address on an interface or range of interfaces. Use this command to configure one or more secondary IP addresses on the interface. The command supports RFC 3021 and accepts 31-bit prefixes on IPv4 point-to-point links, and adds the label IP address in the command.

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 D-LINK OS acts as a host, not a router, on these management interfaces.

No 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**.

ip address *ipaddr* **{***subnetmask* **|** *masklen***} [secondary]**

no ip address [{*ipaddr subnetmask* **[secondary]}]**

Parameters

ipaddr	IP address of the interface.
subnetmask	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.
secondary	(Optional) Indicates a secondary IP address interface.

Default

The default is None.

Command 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 the interface VLAN 100.

```
(Routing)(Interface vlan 100)#ip address 192.168.10.1 255.255.255.254
```

The next example of the command shows the configuration of the subnet mask with an IP address in the / notation on interface VLAN 30.

```
(Routing)(Config)#interface vlan 30
(Routing)(Interface vlan 30)#ip address 192.168.10.1 /31
```

7-16 ip address dhcp

Enable 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.

No command releases a leased address and disable 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.

ip address dhcp [*client-id***]**

no ip address dhcp [*client-id***]**

Parameters

client-id	Enable the DHCP client to specify the unique client identifier (option 61).

Default

The default is Disabled.

Command Mode

Interface Config

Example

In the following example, DHCPv4 is enabled on interface 0/1.

```
(routerl)#config
(routerl)(Config)#interface 0/1
(routerl)(Interface 0/1)#ip address dhcp
```

7-17 ip default-gateway

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.

No command removes the default gateway address from the configuration.

ip default-gateway *ipaddr*

no ip default-gateway *ipaddr*

Parameters

ipaddr	Indicates the IPv4 address of an attached router.

Default

The default is None.

Command Mode

- Global Config
- Virtual Router Config

7-18 ip load-sharing

Configure IP ECMP load balancing mode.

No command removes it.

ip load-sharing *mode* **{inner | outer}**

no ip load-sharing

Parameters

mode	Configure 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.

Default

The default is 6.

Command Mode

Global Config

7-19 release dhcp

Force the DHCPv4 client to release the leased address from the specified interface.

release dhcp {*slot/port* **| vlan** *id***}**

Parameters

slot/port	Enter an interface in slot/port format.
vlan *id*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

7-20 renew dhcp

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.

renew dhcp {*slot/port* **| vlan** *id* | *service-port* **|** *network-port***}**

Parameters

slot/port	Enter an interface in slot/port format.
network-port	Renew IP Address on Network port
service-port	Renew IP Address on Service port
vlan *id*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

7-21 renew dhcp network-port

Renew an IP address on a network port.

renew dhcp network-port

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

7-22 renew dhcp service-port

Renew an IP address on a service port

renew dhcp service-port

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

7-23 ip route

Configure a static route. Use the optional **vrf** parameter to configure the static route in a specified virtual router instance. 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 (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 entered into the forwarding database. By specifying the preference of a static route, you control whether it 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.

Use the **No** command to delete 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.

ip route [vrf *vrf-name***]** *ipaddr subnetmask* **{***nexthopip* **| Null0 | interface {***slot/port* **|** *vlan-id***}} [***preference***] [description** *description***]**

no ip route *ipaddr subnetmask* **[{***nexthopip* **[***preference***] | Null0}]**

Parameters

vrf *vrf-name*	Enter the VRF name which includes maximum 64 ASCII characters.
ipaddr	Enter the destination prefix.
subnetmask	Enter the destination network mask.
nexthopip	Enter the IP address of the next router.
Null0	Indicates the null Interface.
slot/port	Enter an interface in slot/port format.
vlan-id	Enter an interface in VLAN format.
preference	Indicates the route preference (1 – 255).
description *description*	Indicates the description for the route.

Default

The default is None.

Command 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 a connected route in the global routing 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
```

7-24 ip route default

Configure the default route. Use the **vrf** parameter to configure the default route in a specified virtual router instance. The *nexthopip* value 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.

No 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.

ip route default [vrf *vrf-name***]** *nexthopip* **[***preference***]**

no ip route default [{*nexthopip* **|** ***preference*****}]**

Parameters

vrf *vrf-name*	Indicates the destination VRF address.
nexthopip	Enter the IP address of the next router.
preference	Set the route preference (1 – 255).

Default

The default is None.

Command Mode

Global Config

7-25 ip route distance

Set the default distance (preference) for static routes. Lower values are preferred when determining the best route. The **ip route** and **ip route default** commands allow you to optionally set the distance of an individual static route. The default distance is used when nothing 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.

No command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

ip route distance *1-255*

no ip route distance

Parameters

None

Default

The default is 1.

Command Mode

Global Config

7-26 ip route net-prototype

Add net prototype IPv4 routes to the hardware.

No command deletes all the net prototype IPv4 routes added to the hardware.

ip route net-prototype *prefix/prefix-length nexthopip num-routes*

no ip route net-prototype *prefix/prefix-length nexthopip num-routes*

Parameters

prefix/prefix-length	Destination network and mask for route.
nexthopip	Next-hop ip address. It must belong to an active routing interface, but does not need to be resolved.
num-routes	Number of routes needed to add into hardware starting from the given prefix argument and within the given prefix-length.

Default

The default is None.

Command Mode

Global Config

7-27 ip netdirbcast

Enable the forwarding of network-directed broadcasts on an interface or range of interfaces.

No command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

ip netdirbcast

no ip netdirbcast

Parameters

None

Default

The default is Disable.

Command Mode

Interface Config

7-28 ip mtu

Set the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. lP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped when IP MTU exceeds 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).

No command resets the ip mtu to the default value.

ip mtu *68-9198*

no ip mtu

Parameters

None

Default

The default is 1500 bytes.

Command Mode

Interface Config

7-29 ip unnumbered gratuitous-arp accept

Enable the configuration of static interface routes to the unnumbered peer dynamically on receiving gratuitous ARP.

No command disables interface route configuration on receiving gratuitous ARP.

ip unnumbered gratuitous-arp accept

no ip unnumbered gratuitous-arp accept

Parameters

None

Default

The default is as follows: Enable interface route installation for receiving gratuitous.

Command Mode

Interface Config

7-30 ip unnumbered loopback

Identify unnumbered interfaces and specify the numbered interface providing the borrowed address. *interface* should be a loopback interface number.

No command removes the unnumbered configuration.

ip unnumbered loopback *interface*

no ip unnumbered loopback

Parameters

interface	Numbered interface providing the borrowed address. The loopback interface is identified by its loopback interface number.

Default

The default is as follows: Interfaces are numbered.

Command Mode

Interface Config

7-31 encapsulation

Configure the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be **ethernet** or **snap**.

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

encapsulation {ethernet | snap}

Parameters

ethernet	Enter an Ethernet encapsulation type.
snap	Enter an Subnetwork Access Protocol type.

Default

The default is Ethernet.

Command Mode

Interface Config

7-32 show dhcp lease

Display a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. Does not apply to service or network ports.

show dhcp lease [interface {*slot/port* **| vlan** *id***}]**

Parameters

slot/port	Enter an interface in slot/port format.
vlan *id*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show dhcp lease
IP address: 10.10.1.1 for peer on Interface: FastEthernet0/0
Subnet mask: 255.255.255.0
DHCP Lease server: 10.10.1.2, state: 3 Bound
DHCP transaction id: 93
Lease: 86400 secs, Renewal: 43200 secs, Rebind: 75600 secs
```

```
Retry count: 0
```

Display Parameters

IP address, Subnet mask	IP address and network mask leased from the DHCP server.
DHCP Lease server	IPv4 address of the DHCP server that leased the address.
State	State of the DHCPv4 Client on this interface.
DHCP transaction ID	Transaction ID of the DHCPv4 Client.
Lease	Time (in seconds) that the IP address was leased by the server.
Renewal	Time (in seconds) that the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address.
Rebind	Time (in seconds) that the DHCP Rebind process starts.
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds.

7-33 show ip brief

Display the summary information of the IP global configurations for the specified virtual router, including the ICMP rate limit and global ICMP Redirect configuration. If no router is specified, default router information is displayed.

show ip brief [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	Display the IP summary of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example 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
```

Display Parameters

Default Time to Live	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	Maximum number of next hops the packet can travel.
Maximum Routes	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.

7-34 show ip interface

Display all pertinent information about the IP interface.

show ip interface {*slot/port* **| brief | loopback | vlan** *vlan-id* **| vrf}**

Parameters

slot/port	Enter an interface in slot/port format.
brief	Display summary information about IP configuration settings for all ports.
loopback	Display the configured Loopback interface information.
vlan *vlan-id*	Enter an interface in VLAN format.
vrf	Display IP interface entries for a Virtual Router Instance.

Default

The default is None.

Command Mode

- Privileged EXEC

- User EXEC

Example

The following shows example 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
```

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..... 0D-LINKOS-0010.1882.160E-vl10
Interface Name..... rt_v10
```

Display Parameters

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	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.
Helper IP Address	Helper IP addresses configured by the command.
Routing Mode	Administrative mode of router interface participation. The possible values are enabled or disabled. This value is configurable.
Administrative Mode	Administrative mode of the specified interface. The possible values of this field are enabled or disabled. This value is configurable.
Forward Net Directed Broadcasts	Indicates whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Active State	Indicates 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	Burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	Encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	Maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Indicates whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Indicates whether ICMP Redirects may be sent (enabled or disabled).
Interface Suppress Status	Indicates whether the event dampening suppresses a constantly unsatable interface until it remains stable for a period of time.
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.
Interface Name	Indicates the given string name given to identify the interface.

7-35 show ip interface brief

Display summary information about IP configuration settings for all ports in the router, and indicate 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.

show ip interface [vrf *vrf-name***] brief**

Parameters

vrf *vrf-name*	Indicates an IP interface entries for a Virtual Router instance.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Switch)#show ip brief

Default Time to Live.............................. 64
Routing Mode...................................... Disabled
Maximum Next Hops................................. 48
Maximum Routes.................................... 8160
Maximum Static Routes............................. 64
ICMP Rate Limit Interval.......................... 1000 msec
ICMP Rate Limit Burst Size........................ 100 messages
ICMP Echo Replies................................. Enabled
ICMP Redirects.................................... Enabled
Import VXLAN Fabric Mode.......................... Disabled
```

```
(Switch)#show ip interface brief

Interface    State   IP Address    IP Mask         TYPE         Method
----------   -----   ----------    ----------      ----------   ----------
Vlan1        Up      1.1.1.1       255.255.255.0   Primary      Manual
Vlan2        Up      2.2.2.2       255.255.255.0   Primary      Manual
```

Display Parameters

Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	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	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.

7-36 show ip load-sharing

Display the currently configured IP ECMP load balancing mode.

show ip load-sharing

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip load-sharing

ip load-sharing 6 inner
```

7-37 show ip protocols

List a summary of the configuration and status for each unicast routing protocol running in the specified virtual router. If a protocol is selected on the command line, the display is limited to that protocol. If no virtual router is specified, the configuration and status for the default router are displayed.

show ip protocols [vrf *vrf-name***] [bgp | ospf]**

Parameters

vrf *vrf-name*	Display the IP protocols information of a virtual router. Indicates a VRF name which includes maximum 64 ASCII characters.
bgp	Indicates BGP only.
ospf	Indicates OSPF only.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Router)#show ip protocols

Routing Protocol................................ BGP
Router ID....................................... 6.6.6.6
Local AS Number................................. 65001
BGPAdmin 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 extl 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
```

Display Parameters

BGP Section:	
Routing Protocol	BGP
Router ID	Router ID configured for BGP.
Local AS Number	AS number that the local router is in.
BGP Admin Mode	Indicates whether BGP is globally enabled or disabled.
Maximum Paths	Maximum number of next hops in an internal or external BGP route.
Always Compare MED	Indicates whether BGP is configured to compare the Multi-Exit Discriminators (MEDs) for routes received from peers in different ASs.
Maximum AS Path Length	Limit on the length of AS-PATH that BGP accepts from its neighbors.
Fast Internal Failover	Indicates whether BGP immediately brings down an iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast External Failover	Indicates whether BGP immediately brings down an eBGP adjacency if the link to the neighbor goes down.
Distance	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	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.

Prefix List In	Global prefix list used to filter inbound routes from all neighbors.
Prefix List Out	Global prefix list used to filter outbound routes to all neighbors.
Neighbors	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	Indicates whether OSPF is enabled or disabled globally.
Maximum Paths	Maximum number of next hops in an OSPF route.
Routing for Networks	Address ranges configured with an OSPF network command.
Distance	Administrative distance (or “route preference”) for intra-area, inter-area, and external routes.
Default Route Advertise	Indicates whether OSPF is configured to originate a default route.
Always	Indicates 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 advertise for redistributed routes of this type.
Subnets	Indicates 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	Indicates 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	Indicates 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.

7-38 show ip route

Display the routing table for the specified virtual router (**vrf** *vrf-name*). If no router is specified, the default router routing table 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.

show ip route [vrf *vrf-name***] [{***ip-address* **[***protocol***] | {***ip-address mask* **[longer-prefixes] [***protocol***] |** *protocol***} [all] | all}]**

Parameters

vrf *vrf-name*	Indicates the virtual router identification.
ip-address	Indicates the IP-Address of the destination network corresponding to this route.
protocol	Indicates the routes whose prefix length is equal to or longer than pfx-len. This option may not be given if the shorter-prefixes option is given.
mask	Indicates the mask of the destination network corresponding to this route.
longer-prefixes	Indicates the option of a longer prefix setting.
all	Not available.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip route

Route Codes: R - RIP Derived, C - Connected, S - Static
       B - BGP Derived
       O - OSPF 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
```

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 56.6.6.0 255.255.255.0 9.0.0.2 0/26
(Router)(Config)#ip route vrf 66.6.6.9 255.255.255.0 8.0.0.2
(Router)(config)#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
```

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
```

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 2S5.255.255.0
(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
```

Display Parameters

Route Codes	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:

Code	Codes for the routing protocols that created the routes.
Default Gateway	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	IP-Address and mask of the destination network corresponding to this route.
Preference	Administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	Cost associated with this route.
via Next-Hop	Outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	Last updated time for dynamic routes. The format of Route-Timestamp is: • Days:Hours:Minutes if days > = 1 • Hours:Minutes:Seconds if days < 1
Interface	Outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.
Truncated	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.

7-39 show ip route ecmp-groups

Report 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 the next hop in each group.

show ip route ecmp-groups

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example 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
```

7-40 show ip route hw-failure

Display the routes that failed to be added to the hardware due to hash errors or a table full condition.

show ip route hw-failure

Parameters

None

Default

The default is None.

Command 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
```

7-41 show ip route net-prototype

Display the net-prototype routes. The net-prototype routes are displayed with a P.

show ip route net-prototype

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(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
```

7-42 show ip route summary

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 one that is not the most preferred 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.

show ip route summary [all]

Parameters

all	(Optional) Display all (best and non-best) routes.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example 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
```

Display Parameters

Connected Routes	Total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
6To4 Routes	Total number of 6to4 routes in the routing table.
BGP Routes	Total number of routes installed by the BGP protocol.
External	Number of external BGP routes.
Internal	Number of internal BGP routes.
Local	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.
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	Number of net-prototype routes.
Total Routes	Total number of routes in the routing table.
Best Routes (High)	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	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	Number of routes that have been added to the routing table.
Route Deletes	Number of routes that have been deleted from the routing table.
Unresolved Route Adds	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. The counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	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	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	Number of routes failed to be inserted into the hardware due to hash error or a table full condition.
Reserved Locals	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.
RIP Routes	Total number of routes installed by RIP protocol.
Unique Next Hops (High)	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.
NextHop Groups (High)	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.
ECMP Groups (High)	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	Number of next hop groups with multiple next hops.
ECMP Routes	Number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	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	Number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	Current number of routes with each number of next hops.

7-43 clear ip route counters

Reset to zero the IPv4 routing table counters reported in the show IP route summary. 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.

clear ip route counters

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

7-44 show ip route preferences

Display 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.

show ip route preferences

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example 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
```

Display Parameters

Local	Local route preference value.
Static	Static route preference value.
BGP External	The BGP external route preference value.
OSPF Intra	OSPF Intra route preference value.
OSPF Inter	OSPF Inter route preference value.
OSPF External	OSPF External route preference value.
RIP	RIP route preference value.
BGP Internal	BGP internal route preference value.
BGP Local	BGP local route preference value.
Configured Default Gateway	Route preference value of the statically-configured default gateway.
DHCP Default Gateway	Route preference value of the default gateway learned from the DHCP server.

7-45 show ip stats

Display 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.

show ip stats [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display the IP statistics of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Switch)#show ip stats

IpInReceives..................................... 49975
```

```
IpInHdrErrors..................................... 0
IpInAddrErrors.................................... 0
IpForwDatagrams................................... 0
IpInUnknownProtos................................. 0
IpInDiscards...................................... 0
IpInDelivers...................................... 49798
IpOutRequests..................................... 2258
IpOutDiscards..................................... 244
IpOutNoRoutes..................................... 6
IpReasmTimeout.................................... 0
IpReasmReqds...................................... 0
IpReasmOKs........................................ 0
IpReasmFails...................................... 0
IpFragOKs......................................... 0
IpFragFails....................................... 0
IpFragCreates..................................... 0
IpRoutingDiscards................................. 0
IcmpInMsgs........................................ 496
IcmpInErrors...................................... 0
IcmpInDestUnreachs................................ 490

IcmpInTimeExcds................................... 0
IcmpInParmProbs................................... 0
IcmpInSrcQuenchs.................................. 0
IcmpInRedirects................................... 0
IcmpInEchos....................................... 6
IcmpInEchoReps.................................... 0
IcmpInTimestamps.................................. 0
IcmpInTimestampReps............................... 0
IcmpInAddrMasks................................... 0
IcmpInAddrMaskReps................................ 0
IcmpOutMsgs....................................... 490
IcmpOutErrors..................................... 0
IcmpOutDestUnreachs............................... 490
IcmpOutTimeExcds.................................. 0
IcmpOutParmProbs.................................. 0
IcmpOutSrcQuenchs................................. 0
IcmpOutRedirects.................................. 0
IcmpOutEchos...................................... 0
IcmpOutEchoReps................................... 0
IcmpOutTimestamps................................. 0
IcmpOutTimestampReps.............................. 0
IcmpOutAddrMasks.................................. 0
```

7-46 show routing heap summary

Display 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 routing applications.

show routing heap summary

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example 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........................ 57945
```

Display Parameters

Heap Size	Amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	Number of bytes currently allocated.
Memory on Free List	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	Number of bytes in the original heap that have never been allocated.
In Use High Water Mark	Maximum memory in use since the system last rebooted.

IP Event Dampening Commands

7-47 dampening

Enable IP event dampening on a routing interface.

No command disables IP event dampening on a routing interface.

dampening [half-life *period***] [***reuse-threshold suppress-threshold max-suppress-time* **[restart** *restart-penalty***]]**

no dampening

Parameters

half-life *period*	(Optional) 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	(Optional) Value of the penalty at which the dampened interface is restored. The configurable range is 1-20,000. Default value is 1000.
suppress-threshold	(Optional) Value of the penalty at which the interface is dampened. The configurable range is 1-20,000. Default value is 2000.
max-suppress-time	(Optional) 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 the half-life period. If half-period value is allowed to default, the maximum suppress time defaults to 20 seconds.
restart *restart-penalt*	(Optional) Penalty applied to the interface after the device reloads. The configurable range is 1-20,000. Default value is 2000.

Default

The default is None.

Command Mode

Interface Config

7-48 show dampening interface

Summarize the number of interfaces configured with dampening and the number of interfaces being suppressed.

show dampening interface

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Router)#show dampening interface

2 interfaces are configured with dampening.
1 interface is being suppressed.
```

7-49 show interface dampening

Display the status and configured parameters of the interfaces configured with dampening.

show interface dampening

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example 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
```

Display Parameters

Flaps	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" resets the flap count to zero
2. The interface CLI command "no shutdown" 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

Routing Policy Commands

7-50 ip policy

Identify a route map to use for policy-based routing on an interface specified by route-map-name. Policy-based routing is configured on the interface that receives the packets, not on the interface from which the packets are sent.

When new statements are added to a route-map or match/set terms are added/removed from the route-map statement, and also if the route-map that is applied on an interface is removed, the route-map needs to be removed from interface and added back again in order to have the changed route-map configuration be effective.

Note: Route-map and Diffserv cannot work on the same interface.

ip policy route-map *route-map-name*

Parameters

route-map *route-map-name*	Apply route-map to this interface.

Default

The default is None.

Command Mode

Interface Config

Example

The following is an example of this command.

```
(Routing)(Config)#interface 0/1
(Routing)(Interface 0/1)#
(Routing)(Interface 0/1)#ip policy route-map equal-access

In order to disable policy based routing from an interface, use no form of this
command no ip policy <route-map-name>
```

7-51 ip prefix-list

To create a prefix list or add a prefix list entry, use the ip prefix-list command in Global Configuration mode. Route prefixes are matched with those specified in the prefix list. Each prefix list includes a sequence of entries ordered by sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route's prefix using the command.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in a prefix list is 64.

No command deletes a prefix list or a statement in a prefix list. The command **no ip prefix-list list-name** deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

ip prefix-list *list-name* **{[seq** *number***] {permit | deny}** *network/length* **[ge** *length***] [le** *length***] | renumber** *renumber-interval first-statement-number***}**

no ip prefix-list *list-name* **[seq** *number***] {permit | deny}** *network/length* **[ge** *length***] [le** *length***]**

Parameters

list-name	Text name of the prefix list. Up to 32 characters.
seq *number*	(Optional) Sequence number for the prefix list statement. Prefix list statements are ordered from lowest to highest sequence number and applied in that order. If you do not specify a sequence number, the system automatically selects a sequence number five units larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.
permit	Permit routes whose destination prefix matches the statement.
deny	Deny routes whose destination prefix matches the statement.
network/length	Specifies the match criteria for routes being compared to the prefix list statement. The network can be any valid IP prefix. The length is any IPv4 prefix length from 0 to 32.
ge *length*	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.

le *length*	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the ge length and less than or equal to 32.
renumber *renumber-interval first-statement-number*	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for renumber-interval is 1-100, and the valid range for first-statement-number is 1-1000.

Default

Prefix lists are not configured by default. When neither the **ge** nor the **le** option is configured, the destination prefix must match the network/length exactly. If the **ge** option is configured without the **le** option, any prefix with a network mask greater than or equal to the **ge** value is considered a match. Similarly, if the **le** option is configured without the ge option, a prefix with a network mask less than or equal to the le value is considered a match.

Command Mode

Global Config

Example

The following example configures a prefix list that allows routes with one of two specific destination prefixes, 172.20.0.0/16 and 192.168.1.0/24.

```
(Routing)(Config)#ip prefix-list apple seq 16 permit 172.20.0.0/16
(Routing)(Config)#ip prefix-list apple seq 20 permit 192.168.10/24
```

The following example disallows only the default route.

```
(Routing)(Config)#ip prefix-list orange deny 0.0.0.0/0
(Routing)(Config)#ip prefix-list orange permi 0.0.0.0/0 ge 1
```

7-52 ip prefix-list description

To apply a text description to a prefix list, use the **ip prefix-list description** command in Global Configuration mode.

No command removes the text description.

ip prefix-list *list-name* **description** *text*

no ip prefix-list *list-name* **description**

Parameters

list-name	The text name of the prefix list.
text	Text description of the prefix list. Up to 80 characters.

Default

No description is configured.

Command Mode

Global Config

7-53 ipv6 prefix-list

Create IPv6 prefix lists. An IPv6 prefix list can contain only ipv6 addresses. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. For IPv6 routes, only IPv6 prefix lists are matched. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not continue through the rest of the list. An IPv6 prefix list may be used within a route map to match a route's prefix using the match ipv6 address command. A route map may contain both IPv4 and IPv4 prefix lists. If a route being matched is an IPv6 route, only the IPv6 prefix lists are matched.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64. These numbers indicate only IPv6 prefix lists. IPv4 prefix lists may be configured in appropriate numbers independently.

No command deletes either the entire prefix list or an individual statement from a prefix list.

Note: The description must be removed using the no ip prefix-list description before using this command to delete an IPv6 Prefix List.

ipv6 prefix-list *list-name* **[seq** *seq-number***] {{permit | deny}** *ipv6-prefix/prefix-length* **[ge** *ge-value***] [le** *le-value***] | description** *text* **| renumber** *renumber-interval first-statement-number***}**

no ipv6 prefix-list *list-name*

Parameters

list-name	Text name of the prefix list. Up to 32 characters.
seq *seq-number*	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five units larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.
permit	Permit routes whose destination prefix matches the statement.
deny	Deny routes whose destination prefix matches the statement.
ipv6-prefix/prefix-length	Specifies the match criteria for routes being compared to the prefix list statement. The ipv6-prefix can be any valid IPv6 prefix where the address is specified in hexadecimal using 16-bit values between colons. The prefix-length is the length of the IPv6 prefix, given as a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
ge *ge-value*	(Optional) lf this option is configured, specifies a prefix length greater than or equal to the ipv6-prefix/prefix-length. It is the highest value of a range of the length.

le *le-value*	(Optional) If this option is configured, specifies a prefix length less than or equal to the ipv6-prefix/prefix-length. It is the highest value of a range of the length.
description *text*	Description of the prefix list. It can be up to 80 characters in length.
renumber *renumber-interval first-statement-number*	Provides the option to renumber the sequence numbers of the IPv6 prefix list statements with a given interval starting from a particular sequence number.

Default

No prefix lists are configured. When neither the **ge** nor the **le** option is configured, the destination prefix must match the network/length exactly. If the **ge** option is configured without the **le** option, any prefix with a network mask greater than or equal to the **ge** value is considered a match. Similarly, if the **le** option is configured without the **ge** option, a prefix with a network mask less than or equal to the **le** value is considered a match.

Command Mode

Global Config

Example

The following example configures a prefix list that allows routes with one of two specific destination prefixes, 2001::/64 and 5F00::/48.

```
(R1)(Config)#ipv6 prefix-list apple seq 10 permit 2001: :/64
(R1)(Config)#ipv6 prefix-list apple seq 20 permit 5F00: :/48
```

7-54 route-map

To create a route map and enter Route Map Configuration mode, use the route-map command in Global Configuration mode. One use of a route map is to limit the redistribution of routes to a specified range of route prefixes. The redistribution command specifies a route map which refers to a prefix list. The prefix list identifies the prefixes that may be redistributed. D-LINK OS accepts up to 64 route maps.

No command deletes a route map or one of its statements.

route-map *map-tag* **[permit | deny] [***sequence-number***]**

no route-map *map-tag* **[permit | deny] [***sequence-number***]**

Parameters

map-tag	Text name of the route map. Route maps with the same name are grouped together in order of their sequence numbers. A route map name may be up to 32 characters long.
permit	(Optional) Permit routes that match all of the match conditions in the route map.
deny	(Optional) Deny routes that match all of the match conditions in the route map.

sequence-number	(Optional) Integer used to order the set of route maps with the same name. Route maps are ordered from lowest to greatest sequence number, with lower sequence numbers being considered first If no sequence number is specified the system assigns a value ten greater than the last statement in the route map. The range is 0 to 65,535.

Default

The default is as follows: No route maps are configured.

Command Mode

Global Config

Example

In the following example, BGP is configured to redistribute the all prefixes within 172.20.0.0 and reject all others.

```
(Routing)(Config)#ip prefix-list redist-pl permit 172.20.0.0/16 le 32
(Routing)(Config)#route-map redist-rm permit
(Routing)(Config-route-map)#match ip address prefix-list redist-pl
(Routing)(Config-route-map)#exit
(Routing)(Config)#router bgp 1
(Routing)(Config-router)#redistribute ospf route-map redist-rm
```

7-55 match as-path

This route map match term matches BGP autonomous system paths against an AS-PATH access list. If you enter a new **match as-path** term in a route map statement that already has a **match as-path** term, the AS-PATH list numbers in the new term are added to the existing match term, up to the maximum number of lists in a term. A route is considered a match if it matches any one or more of the AS-PATH access lists the match term refers to.

No command deletes the match as-path term that matches BGP autonomous system paths against an AS-PATH access list.

match as-path *as-path-list-number*

no *as-path-list-number*

Parameters

as-path-list-number	Integer from 1 to 500 identifying the AS-PATH access list to use as match criteria.

Default

The default is None.

Command Mode

Route Map Config

7-56 match community

To configure a route map to match based on a BGP community list, use the **match community** command in Route Map Configuration mode. If the community list returns a **permit** action, the route is considered a match. If the match statement refers to a community list that is not configured, no routes are considered to match the statement.

No command deletes a match term from a route map. The command **no match community list exact-match** removes the match statement from the route map. (It does not simply remove the exact-match option.) The command **no match community** removes the match term and all its community lists.

match community *community-list* **[***community-list…***] [exact-match]**

no match community *community-list* **[***community-list…***] [exact-match]**

Parameters

community-list	Name of a standard community list. Up to eight names may be included in a single match term.
exact-match	(Optional) When this option is given, a route is only considered a match if the set of communities on the route is an exact match for the set of communities in one of the statements in the community list.

Default

The default is None.

Command Mode

Route Map Config

7-57 match ip address

To configure a route map to match based on a destination prefix, use the match ip address command in Route Map Configuration mode. If you specify multiple prefix lists in one statement, then a match occurs if a prefix matches any one of the prefix lists. If you configure a match ip address statement within a route map section that already has a match ip address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

No command deletes a match statement from a route map.

match ip address prefix-list *prefix-list-name* **[***prefix-list-name...***]**

no match ip address [prefix-list *prefix-list-name* **[***prefix-list-name...***]]**

Parameters

prefix-list *prefix-list-name*	(Optional) The name of a prefix list used to identify the set of matching

	routes. Up to eight prefix lists may be specified.

Default

The default is None.

Command Mode

Route Map Config

7-58 match ip address <access-list-number | access-list-name>

Configure a route map in order to match based on the match criteria configured in an IP access-list. Note that an IPACL must be configured before it is linked to a route-map. Actions present in an IP ACL configuration are applied with other actions involved in route-map. If an IPACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

If there are a list of IP access-lists specified in this command and the packet matches at least one of these access-list match criteria, the corresponding set of actions in route-map are applied to packet. If there are duplicate IP access-list numbers/names in this command, the duplicate configuration is ignored.

No command deletes a match statement from a route map.

match ip address *access-list-number* **|** *access-list-name* **[***access-list-number* **|** *access-list-name…***]**

no match ip address [*access-list-number* **|** *access-list-name***]**

Parameters

access-list-number	Identifies an access-list configured through access-list CLI configuration commands. This number is 1 to 99 for standard access list number. This number is 100 to 199 for extended access list number.
access-list-name	Identifies named IP ACLs. Access-list name can be up to 31 characters in length. A maximum of 16 ACLs can be specified in this ‘match’ clause.

Default

No match criteria are defined.

Command Mode

Route Map Config

Example

The following sequence is creating a route-map with “match” clause on ACL number and applying that route-map on an interface.

```
(Routing)(Config)#access-list 1 permit ip 10.1.0.0.0.0.255.255
(Routing)(Config)#access-list 2 permit ip 10.2.0.0.0.0.255.255
(Routing)(Config)#route-map equal-access permit 10
(Routing)(Config-route-map)#match ip address 1
```

```
(Routing)(Config-route-map)#set ip default next-hop 192.168.6.6
(Routing)(Config-route-map)#route-map equal-access permit 20
(Routing)(Config-route-map)#match ip address 2
(Routing)(Config-route-map)#set ip default next-hop 172.16.7.7
(Routing)(Config)#interface 0/1
(Routing)(Interface 0/1)#ip address 10.1.1.1 255.255.255.0
(Routing)(Interface 0/1)#ip policy route-map equal-access
(Routing)(Config)#interface 0/2
(Routing)(Interface 0/2)#ip address 192.168.6.5 255.255.255.0
(Routing)(Config)#interface 0/3
(Routing)(Interface 0/3)#ip address 172.16.7.6 255.255.255.0
```

The ip policy route-map equal-access command is applied to interface 0/1. All packets coming inside 0/1 are policy-routed.

Sequence number 10 in route map equal-access is used to match all packets sourced from any host in subnet 10.1.0.0. If there is a match, and if the router has no explicit route for the packet's destination, it is sent to next-hop address 192.168.6.6.

Sequence number 20 in route map equal-access is used to match all packets sourced from any host in subnet 10.2.0.0. If there is a match, and if the router has no explicit route for the packet's destination, it is sent to next-hop address 172.16.7.7.

Rest all packets are forwarded as per normal L3 destination-based routing.

This example illustrates the scenario where IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, this is how configuration is rejected.

```
(Routing)#show ip access-lists

Current number of ACLs: 9  Maximum number of ACLs: 100

ACL ID/Name          Rules  Direction    Interface(s)        VLAN(s)
----------           -----  ----------   ---------------     ----------
1                    1
2                    1
3                    1
4                    1
5                    1
madan                1

(Routing)#show mac access-lists

Current number of all ACLs: 9    Maximum number of all ACLs: 100

MAC ACL Name         Rules  Direction    Interface(s)        VLAN(s)
----------           -----  ----------   ---------------     ----------
mohan                1
mohan                1
goud                 1

(Routing)#
(Routing)#configure
```

```
(Routing)(Config)#route-map madan
(Routing)(Route-map)#match ip address 1 2 3 4 5 madan
(Routing)(Route-map)#match mac-list madan mohan goud
(Routing)(Route-map)#exit
(Routing)(Config)#exit
(Routing)#show route-map

route-map madan permit 10
       Match clauses:
              ip address (access-lists) : 1 2 3 4 5 madan
              mac-list (access-lists) : madan mohan goud
       Set clauses:

(Routing)(Config)#access-list 2 permit every

Request denied. Another application using this ACL restricts the number of rules
allowed.
```

7-59 match ipv6 address (route-map)

Configure a route map to match based on a destination prefix. The prefix-list prefix-list-name identifies the name of an IPv6 prefix list used to identify the set of matching routes. Up to eight prefix lists can be specified. If multiple prefix lists are specified, a match occurs if a prefix matches any one of the prefix lists. If you configure a match ipv6 address statement within a route map section that already has a match ipv6 address statement, the new prefix lists are added to the existing set of prefix lists. and a match occurs if any prefix list in the combined set matches the prefix.

No command deletes a match statement from a route map.

match ipv6 address prefix-list *prefix-list-name* **[***prefix-list-name…***]**

no match ipv6 address prefix-list *prefix-list-name* **[***prefix-list-name…***]**

Parameters

prefix-list *prefix-list-name*	Match an ipv6 prefix-list.

Default

The default is as follows: no matching criteria is defined.

Command Mode

Route Map Config

Example

In the example below, lPv6 addresses specified by the prefix list apple are matched through the route map abc.

```
(Router)(config)#route-map abc
(Router)(config-route-map)#match ipv6 address prefix-list apple
```

7-60 match length

Configure a route map to match based on the Layer 3 packet length between specified minimum and maximum values. *min* specifies the packet's minimum Layer 3 length, inclusive, allowed for a match. *max* specifies the packets maximum Layer 3 length, inclusive, allowed for a match. Each route-map statement can contain one 'match' statement on packet length range.

No command deletes a match statement from a route map.

match length *min max*

no match length

Parameters

min	Enter minimum length of the packet greater than or equal to 68.
max	Enter maximum length of the packet less than or equal to 9198

Default

The default is None.

Command Mode

Route Map Config

Example

The following shows an example of the command.

```
(Routing)(config-route-map)#match length 64 1500
```

7-61 match mac-list

Configure a route map in order to match based on the match criteria configured in a MAC access-list.

A MAC ACL is configured before it is linked to a route-map. Actions present in MAC ACL configuration are applied with other actions involved in route-map. When a MAC ACL referenced by a route-map is removed, the route-map rule is also removed and the corresponding rule is not effective. When a MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

No command deletes a match statement from a route map.

match mac-list *mac-list-name* **[***mac-list-name…***]**

no match mac-list *mac-list-name* **[***mac-list-name…***]**

Parameters

mac-list-name	The mac-list name that identifies MAC ACLs. MAC Access-list name can be up to 31 characters in length.

Default

The default is as follows: no matching criteria is defined.

Command Mode

Route Map Config

Example

The following is an example of the command.

```
(Routing)(config-route-map)# match mac-list MacList1
```

This example illustrates the scenario where MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL, this is how configuration is rejected.

```
(Routing)#show mac access-lists

Current number of all ACLs: 9    Maximum number of all ACLs: 100

MAC ACL Name      Rules   Direction    Interface(s)      VLAN(s)
---------------   -----   ----------   ---------------   ----------
madan                     1
mohan                     1
goud                      1

(Routing)#
(Routing)#configure
(Routing)(Config)#route-map madan
(Routing)(Route-map)#match mac-list madan mohan goud
(Routing)(Route-map)#exit
(Routing)(Config)#exit
(Routing)#show route-map

route-map madan permit 10
       Match clauses:
              mac-list (access-lists) : madan mohan goud
       Set clauses:

(Routing)(Config)#mac access-list extended madan
(Routing)(Config-mac-access-list)#permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:ff any
Request denied. Another application using this ACL restricts the number of rules
allowed.
```

7-62 set as-path

To prepend one or more AS numbers to the AS-PATH in a BGP route, use the set as-path command in Route Map Configuration mode. This command is normally used to insert one or more instances of the local AS number at the beginning of the AS_PATH attribute of a BGP route. Doing so increases the AS-PATH length of the route. The AS-PATH length has a strong influence on BGP route selection. Changing the AS-PATH length can influence route selection on the local router or on routers to which the route is advertised.

When prepending an inbound route, if the first segment in the AS_PATH of the received route is an AS_SEQUENCE, *as-path-string* is inserted at the beginning of the sequence. If the first segment is an AS_SET, *as-path-string* is added as a new segment with type AS_SEQUENCE at the beginning of the AS-PATH. When prepending an outbound route to an external peer, *as-path-string* follows the local AS number, which is always the first ASN.

No command removes a **set** command from a route map.

set as-path prepend *as-path-string*

no set as-path prepend *as-path-string*

Parameters

as-path-string	List of AS-PATH numbers to insert at the beginning of the AS_PATH attribute of matching BGP routes. To prepend more than one AS number, separate the ASNs with a space and enclose the string in quotes. Up to ten AS numbers may be prepended.

Default

The default is None.

Command Mode

Route Map Config

Example

The following example prepends three instances an external peer's AS number to paths received from that peer, making routes learned from this peer less likely to be chosen as the best path.

```
(Routing)#config
(Routing)#route-map ppAsPath
(Routing)#set as-path prepend "2 2 2"
(Routing)#exit
(Routing)#router bgp 1
(Routing)#neighbor 172.20.1.2 remote-as 2
(Routing)#neighbor 172.20.1.2 route-map ppAsPath in
```

7-63 set comm-list delete

To remove BGP communities from an inbound or outbound UPDATE message, use the **set comm-list delete** command in Route Map Configuration mode. A route map with this **set** command can be used to remove selected communities from inbound and outbound routes. When a community list is applied to a route for this purpose, each of the route's communities is submitted to the community list one at a time. Communities permitted by the list are removed from the route. Because communities are processed

individually, a community list used to remove communities should not include the exact-match option on statements with multiple communities. Such statements can never match an individual community.

When a route map statement includes both **set** community and **set comm-list delete** terms, the **set comm-list delete** term is processed first, and then the **set** community term (meaning that, communities are first removed, and then communities are added).

No command deletes the **set** command from a route map.

set comm-list *community-list-name* **delete**

no set comm-list

Parameters

community-list-name	A standard community list name.

Default

The default is None.

Command Mode

Route Map Config

7-64 set community

To modify the communities attribute of matching routes, use the **set community** command in Route Map Configuration mode. The **set community** command can be used to assign communities to routes originated through BGP's network and redistribute commands, and to set communities on routes received from a specific neighbor or advertised to a specific neighbor. It can also be used to remove all communities from a route.

To remove a subset of the communities on a route, use the command "**set comm-list delete**".

No command removes a **set** term from a route map.

set community {*community-number* **[additive] | none}**

no set community

Parameters

community-number	One to sixteen community numbers, either as a 32-bit integers or in AA:NN format. Communities are separated by spaces. The well-known communities **no advertise** and **no-export** are also accepted.
additive	(Optional) Communities are added to those already attached to the route.
none	Removes all communities from matching routes.

Default

The default is None.

Command Mode

Route Map Config

7-65 set interface

If the network administrator does not want to revert to normal forwarding but instead wants to drop a packet that does not match the specified criteria, a set statement needs to be configured to route the packets to interface null 0 as the last entry in the route-map. **set interface null0** needs to be configured in a separate statement. It should not be added along with any other statement having other match/set terms.

A route-map statement that is used for PBR is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet meeting the match criteria. If the statement is marked as permit, and if the packet meets all the match criteria, then set commands in the route-map statement are applied. If no match is found in the route-map, the packet is not dropped, instead the packet is forwarded using the routing decision taken by performing destination-based routing.

set interface null0

Parameters

None

Default

The default is None.

Command Mode

Route Map Config

7-66 set ip next-hop

Specify the adjacent next-hop router in the path toward the destination to which the packets should be forwarded. If more than one IP address is specified, the first IP address associated with a currently up-connected interface is used to route the packets.

This command affects all incoming packet types and is always used if configured. If configured next-hop is not present in the routing table, an ARP request is sent from the router.

In a route-map statement, ‘set ip next-hop’ and ‘set ip default next-hop’ terms are mutually exclusive. However, a ‘set ip default next-hop’ can be configured in a separate route-map statement.

No command removes a **set** command from a route map.

set ip next-hop *ip-address* **[***ip-address…***]**

no set ip next-hop *ip-address* **[***ip-address…***]**

Parameters

ip-address	IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this 'set' clause.

Default

The default is None.

Command Mode

Route Map Config

7-67 set ip default next-hop

Set a list of default next-hop IP addresses. When more than one IP address is specified, the following hop specified is used. The optional specified IP addresses are tried in turn.

A packet is routed to the next hop specified by this command only if there is no explicit route for the packet's destination address in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.

ln a route-map statement, 'set ip next-hop' and 'set ip default next-hop' terms are mutually exclusive. However, a 'set ip next-hop' can be configured in a separate route-map statement.

No command removes a **set** command from a route map.

set ip default next-hop *ip-address* **[***ip-address…***]**

no set ip default next-hop *ip-address* **[***ip-address…***]**

Parameters

ip-address	IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this 'set' clause.

Default

The default is None.

Command Mode

Route Map Config

7-68 set ip precedence

Set the three IP precedence bits in the IP packet header. With three bits, you have eight possible values for the lP precedence; values 0 through 7 are defined. This command is used when implementing QoS

and can be used by other QoS services, such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

No command resets the three IP precedence bits in the IP packet header to the default.

set ip precedence *0-7*

no set ip precedence

Parameters

0	Sets the routine precedence.
1	Sets the priority precedence.
2	Sets the immediate precedence.
3	Sets the Flash precedence.
4	Sets the Flash override precedence.
5	Sets the critical precedence.
6	Sets the internetwork control precedence.
7	Sets the network control precedence.

Default

The default is None.

Command Mode

Route Map Config

7-69 set ipv6 next-hop (BGP)

To set the IPv6 next hop of a route, use the **set ipv6 next-hop** command in Route Map Configuration mode. When used in a route map applied to UPDATE messages received from a neighbor, the command sets the next hop address for matching IPv6 routes received from the neighbor.

When used in a route map applied to UPDATE messages sent to a neighbor, the command sets the next hop address for matching IPv6 routes sent to the neighbor. If the address is a link local address, the address is assumed to be on the interface where the UPDATE is sent or received. If the command specifies a global IPv6 address, the address is not required to be on a local subnet.

No command removes a **set** command from a route map.

set ipv6 next-hop *ipv6-address*

no set ipv6 next-hop

Parameters

ipv6-address	lPv6 address set as the Network Address of Next Hop field in the

MP_NLRI attribute of an UPDATE message.

Default

The default is None.

Command Mode

Route Map Config

7-70 set local-preference

To set the local preference of specific BGP routes, use the set local-preference command in Route Map Configuration mode. The local preference is the first attribute used to compare BGP routes. Setting the local preference can influence which route BGP selects as the best route.

No command removes a **set** command from a route map.

set local-preference *value*

no set local-preference *value*

Parameters

value	Local preference value, from 0 to 4,294,967,295 (any 32-bit integer).

Default

The default is None.

Command Mode

Route Map Config

7-71 set metric (BGP)

To set the metric of a route, use the **set metric** command In Route Map Configuration mode. In BGP context, sets the Multi Exit Discriminator (MED). When there are multiple peering points between two autonomous systems (AS), setting the MED on routes advertised by one router can influence the other AS to send traffic through a specific peer.

No command removes a **set** command from a route map.

set metric *value*

no set metric *value*

Parameters

value	A metric value, from 0 to 4,294,967,295 (any 32-bit integer).

Default

The default is None.

Command Mode

Route Map Config

7-72 show ip policy

List the route map associated with each interface.

show ip policy

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ip policy

Interface            Route-Map
------------  ----------------------------------------
FastEthernet0/0      equal-access
```

Display Parameters

Interface	Indicates the interface.
Route-map	Indicates the route map.

7-73 show ip prefix-list

Display configuration and status for a prefix list.

show ip prefix-list [detail | summary] *prefix-list-name* **[***network/length***] [seq** *sequence-number***] [longer] [first-match]**

Parameters

detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
prefix-list-name	(Optional) Name of a specific prefix list.
network/length	(Optional) Network number and length (in bits) of the network mask
seq *sequence-number*	(Optional) Applies the sequence number to the prefix list entry. The sequence number of the prefix list entry.
longer	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
first-match	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

- show ip prefix-list prefix-list-name network/length first-match
- show ip prefix-list prefix-list-name network/length longer
- show ip prefix-list prefix-list-name network/length
- show ip prefix-list prefix-list-name seq sequence-number
- show ip prefix-list prefix-list-name
- show ip prefix-list summary
- show ip prefix-list summary prefix-list-name
- show ip prefix-list detail
- show ip prefix-list detail prefix-list-name

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip prefix-list fred

ip prefix-list fred:
       count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
       seq 5 permit 10.10.1.1/20 ge 22
       seq 10 permit 10.10.1.2/20 le 36
       seq 15 permit 10.10.1.2/20 ge 29 le 30
```

The following shows example CLI display output for the command

```
(Routing)#show ip prefix-list summary fred

ip prefix-list fred:
       count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
```

The following shows example CLI display output for the command

```
(Routing)#show ip prefix-list detail fred

ip prefix-list Fred:
       count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
       seq 5 permit 10.10.1.1/20 ge 22 (hitcount: 0)
       seq 10 permit 10.10.1.2/20 le 30 (hitcount: 0)
       seq 15 permit 10.10.1.2/20 ge 29 le 30 (hitcount: 0)
```

7-74 show ipv6 prefix-list

Display configuration and status for a selected prefix list.

show ipv6 prefix-list [detail | summary] *listname* **[***ipv6-prefix/prefix-length***] [seq** *sequence-number***] [longer] [first-match]**

Parameters

detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
listname	(Optional) Name of a specific prefix list.
ipv6-prefix/prefix-length	(Optional) Network number and length (in bits) of the network mask.
seq *sequence-number*	(Optional) Applies the sequence number to the prefix list entry. The sequence number of the prefix list entry.
longer	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
first-match	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

- show ipv6 prefix-list listname ipv6 prefix/prefix length first-match
- show ipv6 prefix-list listname ipv6-prefix/prefix-length longer
- show ipv6 prefix-list listname ipv6-prefix/prefix-length
- show ipv6 prefix-list listname seq sequence-number
- show ipv6 prefix-list listname
- show ipv6 prefix-list summary
- show ipv6 prefix-list summary prefix-list-name
- show ipv6 prefix-list detail
- show ipv6 prefix-list detail prefix-list-name

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Switch)#show ipv6 prefix-list apple

ipv6 prefix-list apple:
       count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
       seq 5 deny 5F00::/8 le 128
       seq 10 deny ::/0
       seq 15 deny ::/1
       seq 20 deny ::/2
       seq 25 deny ::/3 ge 4
              seq 30 permit ::/0 le 128
```

```
(Switch)#show ipv6 prefix-list summary apple

ipv6 prefix-list apple:
       count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

```
(Switch)#show ipv6 prefix-list detail apple

ipv6 prefix-list apple:
       count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
       seq 5 deny 5F00 ::/8 le 128 (hit count: 0, refcount: 1)
       seq 10 deny ::/0 (hit count: 0, refcount: 1)
       seq 15 deny ::/1 (hit count: 0, refcount: 1)
       seq 20 deny ::/2 (hit count: 0, refcount: 1)
       seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
              seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

Display Parameters

count	Number of entries in the prefix list.
range entries	Number of entries that match the input range.
ref count	Number of entries referencing the given prefix list.
seq	Sequence number of the entry in the list.
permit/deny	Action to take.
sequences	Range of sequence numbers for the entries in the list.
hit count	Number of matches for the prefix entry.

7-75 show route-map

To display a route map, use the **show route-map** command in Privileged EXEC mode.

show route-map [*map-name***]**

Parameters

map-name	(Optional) Name of a specific route map.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show route-map test

route-map test, permit, sequence 10
       Match clauses:
              ip address prefix-lists: orange
                     Set clauses:
                            set metric 50
```

7-76 clear ip prefix-list

To reset IP prefix-list counters, use the **clear ip prefix-list** command in Privileged EXEC mode. This command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

clear ip prefix-list [[*prefix-list-name***] [***network/length***]]**

Parameters

prefix-list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
network/length	(Optional) Network number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#clear ip prefix-list orange 20.0.0.0/8
```

7-77 clear ipv6 prefix-list

Reset and clear IPv6 prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

clear ipv6 prefix-list [*prefix-list-name***] [***ipv6-prefix/prefix-length***]**

Parameters

prefix-list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
ipv6-prefix/prefix-length	(Optional) IPv6 prefix number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

Default

The default is None.

Command Mode

Privileged EXEC

Router Discovery Protocol Commands

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

7-78 ip irdp

Enable Internet Router Discovery Protocol (IRDP) on an interface or range of interfaces.

No command disables Router Discovery on an interface.

ip irdp

no ip irdp

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

7-79 ip irdp address

Configure the address that the interface uses to send the router discovery advertisements. The valid value for *ipaddr* is 255.255.255.255, which is the limited broadcast address.

No command configures the default address used to advertise the router for the interface.

ip irdp address *ipaddr*

no ip irdp address

Parameters

ipaddr	Enter an IP address. The valid options are 224.0.0.1 and 255.255.255.255.

Default

The default is 224.0.0.1.

Command Mode

Interface Config

7-80 ip irdp holdtime

Configure the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of 4 to 9000 seconds.

No command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

ip irdp holdtime *maxadvertinterval*

no ip irdp holdtime

Parameters

maxadvertinterval	Enter the holdtime in seconds.

Default

The default is 3 x *maxadvertinterval*.

Command Mode

Interface Config

7-81 ip irdp maxadvertinterval

Configure the maximum time, in seconds, allowed between sending router advertisements from the interface.

No command configures the default maximum time, in seconds.

ip irdp maxadvertinterval *4-1800*

no ip irdp maxadvertinterval

Parameters

None

Default

The default is 600.

Command Mode

Interface Config

7-82 ip irdp minadvertinterval

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

No command sets the default minimum time to the default.

ip irdp minadvertinterval *maxadvertinterval*

no ip irdp minadvertinterval

Parameters

maxadvertinterval	Enter the minadvertinterval in seconds.

Default

The default is 0.75 * maxadvertinterval.

Command Mode

Interface Config

7-83 ip irdp preference

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

No command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

ip irdp preference *-2147483648-2147483647*

no ip irdp preference

Parameters

None

Default

The default is 0.

Command Mode

Interface Config

7-84 show ip irdp

Display the router discovery information for all interfaces, or a specified interface.

show ip irdp {*slot/port* **| vlan** *vlan-id* **| all}**

Parameters

slot/port	Enter an interface in slot/port format.
vlan *vlan-id*	Enter an interface in VLAN format.
all	Enter 'all' for all interfaces.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ip irdp all

Interface     Ad Mode  Dest Address       Max Int  Min Int  Hold Time  Preference
------------  -------  -----------------  -------  -------  ---------  ----------
0/1           Disable  224.0.0.1          600      450      1800       0
0/2           Disable  224.0.0.1          600      450      1800       0
0/3           Disable  224.0.0.1          600      450      1800       0
0/4           Disable  224.0.0.1          600      450      1800       0
0/5           Disable  224.0.0.1          600      450      1800       0
0/6           Disable  224.0.0.1          600      450      1800       0
0/7           Disable  224.0.0.1          600      450      1800       0
0/8           Disable  224.0.0.1          600      450      1800       0
0/9           Disable  224.0.0.1          600      450      1800       0
0/10          Disable  224.0.0.1          600      450      1800       0
0/11          Disable  224.0.0.1          600      450      1800       0
0/12          Disable  224.0.0.1          600      450      1800       0
0/13          Disable  224.0.0.1          600      450      1800       0
0/14          Disable  224.0.0.1          600      450      1800       0
0/15          Disable  224.0.0.1          600      450      1800       0
0/16          Disable  224.0.0.1          600      450      1800       0
0/17          Disable  224.0.0.1          600      450      1800       0
0/18          Disable  224.0.0.1          600      450      1800       0
0/19          Disable  224.0.0.1          600      450      1800       0
0/20          Disable  224.0.0.1          600      450      1800       0
0/21          Disable  224.0.0.1          600      450      1800       0
0/22          Disable  224.0.0.1          600      450      1800       0

                                  <Output truncated>
```

Display Parameters

Interface	Interface (slot/port or VLAN) that matches the rest of the information in the row.
Ad Mode	Advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Dest Address	Destination IP address for router advertisements.

Max Int	Maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	Minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	Amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	Preference of the address as a default router address, relative to other router addresses on the same subnet.

Virtual Router Commands

7-85 ip vrf

Create a virtual router with a specified name and enters VRF configuration mode.

No command deletes the virtual router with the specified name.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Parameters

vrf-name	Name of the virtual router. The name is a string of up to 64 characters from an ASCII set.

Default

The default is as follows: no VRs are defined.

Command Mode

Global Config

Example

The following example creates two virtual router instances. The routing in the virtual router instance is enabled only when **ip routing** command is issued at the virtual router level.

```
(Router)(C0nfig)#ip vrf Red
(Router)(Config-vrf-Red)#ip routing
(Router)(Config-vrf-Red)#exit
(Router)(Config)#ip vrf Blue
(Router)(Config-vrf-Blue)#ip routing
(Router)(Config-vrf-Blue)#exit
```

7-86 maximum routes

Reserve the number of routes allowed and set the maximum limit on the number of routes for a virtual router instance in the total routing table space for the router, provided there is enough free space in the router's total routing table.

No command removes any reservation for the number of routes allowed in the virtual router instance and clears the warning threshold value.

maximum routes {*limit* **| warn** *threshold***}**

no maximum routes

Parameters

limit	The number of routes for a virtual router instance in the total routing table space for the router. The limit ranges from 1 to 4294967295. If the limit value is greater than the total router table size, it is limited to the total size.
warn *threshold*	The threshold value ranges from 1 to 100 and indicates the percent of the limit value at which a warning message is to be generated. If no limit value is given the platform maximum is taken as the limit value.

Default

The default is as follows: limited by the number of free routes available.

Command Mode

Virtual Router Config

Example

The following shows an example of the command.

```
(Router)(Config)#ip vrf Red
(Router)(Config-vrf-Red)#ip routing
(Router)(Config-vrf-Red)#maximum routes 2048
(Router)(Config-vrf-Red)#maximum routes warn 80
(Router)(Config-vrf-Red)#exit
(Router)(Config)#ip vrf Blue
(Router)(Config-vrf-Blue)#ip routing
(Router)(Config-vrf-Blue)#maximum routes 4096
(Router)(Config-vrf-Blue)#exit
```

7-87 description

Allow the user to configure a descriptive text for a virtual router.

No command removes the descriptive text configuration for a virtual router.

description *text*

no description

Parameters

text	The descriptive text for the virtual router. A set of ASCII characters up to 512 characters in length.

Default

The default is None.

Command Mode

Virtual Router Config

7-88 ip vrf forwarding

Associate an IP interface with a virtual router.

No command disassociates an IP interface from the configured virtual router and associates it back to the default router.

ip vrf forwarding *vrf-name*

no ip vrf forwarding

Parameters

vrf-name	The name of the virtual router.

Default

The default is Default router.

Command Mode

Interface Config

Example

This example creates two virtual router instances and assigns interfaces to those virtual routers.

```
(Router)(Config)#ip vrf Red
(Router)(Config)#ip vrf Blue
(Router)(Config)#interface 0/1
(Router)(Interface 0/1)#ip vrf forwarding Red
(Router)(Interface 0/1)#exit
(Router)(Config)#interface 0/2
(Router)(Interface 0/2)#ip vrf forwarding Blue
(Router)(Interface 0/2)#exit
```

7-89 show ip vrf

Display information about virtual router instances.

show ip vrf [{*vrf-name* **| detail** *vrf-name* **| interfaces | memory [***vrf-name***]}]**

Parameters

vrf-name	(Optional) Name of virtual router instance.
detail *vrf-name*	(Optional) Displays the configuration and status of a virtual router.
interfaces	(Optional) Displays the list of interfaces and virtual routers to which they belong.
memory [*vrf-name***]**	(Optional) Displays the runtime memory utilization of the processes running in a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Router)#show ip vrf

Number of VRs.....................3

Name    Identifier   Route Distinguisher
-----   ----------   -------------------
Red     2            2:200
Blue    4            4:400
Green   3            3:300
```

```
(Router)#show ip vrf Red

VRF Identifier.....................2
Description.....................India office bangalore”
Route Distinguisher.....................2:200
Maximum Routes.....................512
Threshold.....................80%
warning-only.....................TRUE
```

```
(Routing)#show ip vrf detail red

VRF Identifier.....................1
```

```
Description.............................
Route Distinguisher....................300:6
Maximum Routes.........................Not Set
warning-only...........................FALSE
Route table size.......................0
Number of interfaces...................1

Interfaces:
----------
0/10

Export VPN route-target communities
       RT:152:1
Import VPN route-target communities
       RT:152:1
```

Virtual LAN Routing Commands

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

7-90 vlan routing

Enable routing on a VLAN. The vlanid value has a range from 1 to 4093. The [interface ID] value has a range from 1 to 128. Typically, the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the slot/port for the VLAN routing interface. If you select an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface. For products that use text-based configuration, including the interface ID in the VLAN routing command for the text configuration ensures that the slot/port for the VLAN interface stays the same across a restart. Keeping the slot/port the same ensures that the correct interface configuration is applied to each interface when the system restarts.

No command deletes routing on a VLAN.

vlan routing *vlanid* **[***interface ID***]**

no vlan routing *vlanid*

Parameters

vlanid	Indicates VLANs to be configured.
interface ID	(Optional) Indicates the identifier of the interface that sends VLAN routing.

Default

The default is None.

Command Mode

VLAN Config

Example

Shows the command specifying a vlanid value. The interface ID argument is not used.

```
(Routing)(Vlan)#vlan routing 14 ?

<cr> Press enter to execute the command.
<1-128> Enter interface ID
```

Typically, you press <Enter> without supplying the Interface ID value; the system automatically selects the interface ID.

The command specifies interface ID 51 for VLAN 14 interface. The interface ID becomes the port number in the *slot/port* for the VLAN routing interface. In this example, *slot/port* is 4/51 for VLAN 14 interface.

```
(Routing)(Vlan)#vlan 14 51
(Routing)(Vlan)#
(Routing)#show ip vlan

MAC Address uswd by Routing VLANs:      00:11:88:59:47:36

VLAN ID  Logical Interface  IP Address     Subnet Mask
-------  -----------------  ------------   ---------------
10       4/1                172.16.10.1    255.255.255.0
11       4/50               172.16.11.1    255.255.255.0
12       4/3                172.16.12.1    255.255.255.0
13       4/4                172.16.13.1    255.255.255.0
14       4/51               0.0.0.0        0.0.0.0
```

Select an interface ID that is already in use In this case, the CLI displays an error message and does not create the VLAN interface.

```
(Routing)#show ip vlan

MAC Address used by Routing VLANs:        00:11:88:59:47:36

VLAN ID  Logical Interface  IP Address     Subnet Mask
-------  -----------------  ------------   ---------------
10       4/1                172.16.10.1    255.255.255.0
11       4/50               172.16.11.1    255.255.255.0
12       4/3                172.16.12.1    255.255.255.0
13       4/4                172.16.13.1    255.255.255.0
14       4/51               0.0.0.0        0.0.0.0

(Routing)#config
(Routing)(Config)#exit
(Routing)#vlan database
(Routing)(Vlan)#vlan 15
(Routing)(Vlan)#vlan routing 15 1
```

```
Interface ID 1 is already assigned to another interface
```

The show running configuration command always lists the interface ID for each routing VLAN as shown in below.

```
(Routing)#show running-config
!Current Configuration:
!
!System Description "DQS-5000-54SQ28 - 48 25GE + 6 100GE, 2.1.5, Linux 3.16.0-29-
generic"
!System Software Version   "1.00.006"
!System Up Time            "4 days 19 hrs 5 mins 38 secs"
!Cut-through mode is configured as disabled
!Additional Packages BGP-4,QOS,IPv6,IPv6 Management,Rout1ng,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
Set prompt "02.08"
Network protocol dhcp
Vlan database
Vlan 10-14
Vlan routing 10 1
Vlan routing 12 3
Vlan routing 13 4
Vlan routing 11 50
Vlan routing 14 51
```

7-91 interface vlan

Enter Interface configuration mode for the specified VLAN routing interface.

interface vlan *1-4093*

Parameters

None

Default

The default is None.

Command Mode

Global Config

7-92 show ip vlan

Display the VLAN routing information for all VLANs with routing enabled.

show ip vlan

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

MAC Address used by Routing VLANs	MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	Identifier of the VLAN.
Logical Interface	Logical slot/port associated with the VLAN routing interface.
IP Address	IP address associated with this VLAN.
Subnet Mask	Subnet mask that is associated with this VLAN.

Virtual Router Redundancy Protocol Commands

This section describes commands you use to view and configure Virtual Router Redundancy Protocol (VRRP) and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

7-93 ip vrrp (Global Config)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router.

No command in Global Config mode disables the default administrative mode of VRRP on the router.

ip vrrp

no ip vrrp

Parameters

None

Default

The default is None.

Command Mode

Global Config

7-94 ip vrrp (Interface Config)

Use this command in Interface Config mode to create a virtual router associated with the interface or range of interfaces. The parameter *vrid* is the virtual router ID which has an integer value range from 1 to 255.

No command in Interface Config mode to delete the virtual router associated with the interface. The virtual Router ID, *vrid*, is an integer value that ranges from 1 to 255.

ip vrrp *vrid*

no ip vrrp *vrid*

Parameters

vrid	Enter virtual router ID (1-255).

Default

The default is None.

Command Mode

Interface Config

7-95 ip vrrp mode

Enable the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter *vrid* is the virtual router ID which has an integer value ranging from 1 to 255.

No command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

ip vrrp *vrid* **mode**

no ip vrrp *vrid* **mode**

Parameters

vrid	Indicates the virtual router ID.

Default

The default is Disable.

Command Mode

Interface Config

7-96 ip vrrp ip

Set the virtual router IP address value for an interface or range of interfaces. The value for *ipaddr* is the IP address which is to be configured on that interface for VRRP. The parameter *vrid* is the virtual router ID which has an integer value range from 1 to 255. You can use the optional [*secondary*] parameter to designate the IP address as a secondary IP address.

No command in Interface Config mode deletes a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

ip vrrp *vrid* **ip** *ipaddr* **[secondary]**

no ip vrrp *vrid* **ip** *ipaddr* **secondary**

Parameters

vrid	Indicates the virtual router ID.
ipaddr	Indicates the IP address associated with the Virtual Router.
secondary	(Optional) Designates whether an IP address is a secondary address on this interface.

Default

The default is None.

Command Mode

Interface Config

7-97 ip vrrp accept-mode

Allow the VRRP Master to accept ping packets sent to one of the virtual router's IP addresses.

No command prevents the VRRP Master from accepting ping packets sent to one of the virtual router's IP addresses.

Note: VRRP accept-mode allows only ICMP Echo Request packets. No other type of packet is allowed to be delivered to a VRRP address.

ip vrrp *vrid* **accept-mode**

no ip vrrp *vrid* **accept-mode**

Parameters

vrid	Indicates the virtual router ID.

Default

The default is Disable.

Command Mode

Interface Config

7-98 ip vrrp authentication

Set the authorization details value for the virtual router configured on a specified interface or range of interfaces. The parameter **{none | simple}** specifies the authorization type for virtual router configured on the specified interface. The parameter [*key*] is optional, it is only required when authorization type is simple text password. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

No command sets the default authorization details value for the virtual router configured on a specified interface or range of interfaces.

ip vrrp *vrid* **authentication {none | simple** *key***}**

no ip vrrp *vrid* **authentication**

Parameters

vrid	Indicates the virtual router ID.
none	Configure authentication type as none.
simple *key*	Configure authentication type as simple.

Default

The default is no authentication.

Command Mode

Interface Config

7-99 ip vrrp preempt

Set the preemption mode value for the virtual route configured on a specified interface or range of interfaces. The parameter *vrid* is the virtual router ID, which is an integer from 1 to 255.

No command sets the default preemption mode value for the virtual router configured on a specified interface or range of interfaces.

ip vrrp *vrid* **preempt**

no ip vrrp *vrid* **preempt**

Parameters

vrid	Indicates the virtual router ID.

Default

The default is Enabled.

Command Mode

Interface Config

7-100 ip vrrp priority

Set the priority of a router within a VRRP group. It can be used to configure an interface or a range of interfaces. Higher values equal higher priority. The range is from 1 to 254. The parameter *vrid* is the virtual router ID, whose range is from 1 to 255.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the “address owner.” The priority of the address owner is always 255 so that the address owner is always master. If the master has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the master’s priority, the router will take over as master only if preempt mode is enabled.

No command sets the default priority value for the virtual router configured on a specified interface or range of interfaces.

ip vrrp *vrid* **priority** *1-254*

no ip vrrp *vrid* **priority**

Parameters

vrid	Indicates the virtual router ID.

Default

The default is 100. If the router is the address owner, the priority is automatically set to 255.

Command Mode

Interface Config

7-101 ip vrrp timers advertise

Set the frequency, in seconds, that an interface or range of interfaces on the specified virtual router sends a virtual router advertisement.

No command sets the default virtual router advertisement value for an interface or range of interfaces.

ip vrrp *vrid* **timers advertise** *1-255*

no ip vrrp *vrid* **timers advertise**

Parameters

vrid	Indicates the virtual router ID.

Default

The default is 1.

Command Mode

Interface Config

7-102 ip vrrp track interface

Alter the priority of the VRRP router based on the availability of its interfaces. This command is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up when the IP on that interface is up. Otherwise, the tracked interface is down. You can use this command to configure a single interface or a range of interfaces.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the priority argument. When the interface is up for IP protocol, the priority will be incremented by the *priority* value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed interface. The default priority decrement is changed using the *priority* argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. lf you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set.

No command removes the interface or range of interfaces from the tracked list or to restore the priority decrement to its default.

ip vrrp *vrid* **track interface {***slot/port* **| vlan** *vlan-id***} [decrement** *priority***]**

no ip vrrp *vrid* **track interface** *slot/port* **[decrement]**

Parameters

vrid	Indicates the virtual router ID.
slot/port	Indicates an interface in slot/port format.
vlan *vlan-id*	Enter an interface in VLAN format.
decrement *priority*	(Optional) Indicates the reduced priority of a VRRP router in increments of 10 (default) when a tracked interface goes down.

Default

The default is 10.

Command Mode

Interface Config

7-103 ip vrrp track ip route

Track the route reachability on an interface or range of interfaces. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the *priority* argument. When the tracked route is added, the priority will be incremented by the same.

A VRRP configured interface can track more than one route. When a tracked route goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed route. By default no routes are tracked. If you specify just the route to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10. The default priority decrement is changed using the *priority* argument.

No command removes the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, the priority should be incremented by the decrement value if the route is not reachable.

ip vrrp *vrid* **track ip route** *ip-address/prefix-length* **[decrement** *priority***]**

no ip vrrp *vrid* **track ip route** *ip-address/prefix-length* **[decrement]**

Parameters

vrid	Indicates the virtual router ID.
ip-address/prefix-length	Prefix and prefix length of the route to be tracked.
decrement *priority*	(Optional) Enter amount to decrement router priority (1-254).

Default

The default is 10.

Command Mode

Interface Config

7-104 show ip vrrp interface stats

Display the statistical information about each virtual router configured on the switch.

show ip vrrp interface stats {*slot/port* **| vlan** *vlan-id***}** *vrid*

Parameters

slot/port	Enter an interface in slot/port format.
vlan *vlan-id*	Enter an interface in VLAN format.
vrid	Indicates the virtual router ID.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Router)#show ip vrrp interface stats vlan 10 10

UpTime..................................... 9 days 22 hrs 19 mins 12 secs
Protocol................................... IP
State Transitioned to Master............... 3
Advertisement Received..................... 145
Advertisement Interval Errors.............. 0
Authentication Failure..................... 0
IP TTL Errors.............................. 0
Zero Priority Packets Received............. 0
Zero Priority Packets Sent................. 0
Invalid Type Packets Received.............. 0
Address List Errors........................ 0
Invalid Authentication Type................ 0
Authentication Type Mismatch............... 0
Packet Length Errors....................... 0
```

Display Parameters

Uptime	Time that the virtual router has been up in days, hours, minutes and seconds.
Protocol	Protocol configured on the interface.
State Transitioned to Master	Total number of times virtual router state has changed to MASTER.
Advertisement Received	Total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	Total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
Authentication Failure	Total number of VRRP packets received that don't pass the authentication check.
IP TTL Errors	Total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.

Zero Priority Packets Received	Total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	Total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	Total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	Total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	Total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	Total number of VRRP advertisements received for which ‘auth type’ not equal to locally configured one for this virtual router.
Packet Length Errors	Total number of VRRP packets received with packet length less than length of VRRP header.

7-105 show ip vrrp

Display whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring.

show ip vrrp

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Router)#show ip vrrp

Admin Mode..................................... Enable
Router Checksum Errors.......................... 0
Router Version Errors........................... 0
Router VRID Errors.............................. 0
```

Display Parameters

VRRP Admin Mode	Administrative mode for VRRP functionality on the switch.
Router Checksum Errors	Total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	Total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	Total number of VRRP packets received with invalid VRID for this virtual router.

7-106 show ip vrrp interface

Display all configuration information and VRRP router statistics of a virtual router configured on a specific interface. Use the output of the command to verify the track interface and track IP route configurations.

show ip vrrp interface {*slot/port* **| vlan** *vlan-id***}** *vrid*

Parameters

slot/port	Enter an interface in slot/port format.
vlan *vlan-id*	Enter an interface in VLAN format.
vrid	Indicates the virtual router ID.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip vrrp interface 0/1 vrid

Primary IP Address.............................. 1.1.1.5
VMAC Address.................................... 00:00:5e:00:01:01
Authentication Type............................. None
Priority........................................ 80
Configured priority............................. 100
Advertisement Interval (secs.................... 1
Pre-empt Mode................................... Enable
Administrative Mode............................. Enable
Accept Mode..................................... Enable
State........................................... Initialized
```

```
Track Interface    State         DecrementPriority
---------------    ----------    --------------------
<0/1>              down          10

TrackRoute (pfx/len)          State         DecrementPriority
--------------------------    ----------    --------------------
10.10.10.1/255.255.255.0      down          10
```

Display Parameters

IP Address	Configured IP address for the Virtual router.
VMAC Address	VMAC address of the specified router.
Authentication Type	Authentication type for the specific virtual router.
Priority	Priority value for the specific virtual router, taking into account any priority decrements for tracked interfaces or routes.
Configured Priority	Priority configured through the ip vrrp vrid priority 1-254 command.
Advertisement Interval	Advertisement interval in seconds for the specific virtual router.
Pre-Empt Mode	Preemption mode configured on the specified virtual router.
Administrative Mode	Status X of the specific router (Enable or Disable).
Accept Mode	When enabled, the VRRP Master can accept ping packets sent to one of the virtual router's IP addresses.
State	State (Master/backup) of the virtual router.

7-107 show ip vrrp interface brief

Display information about each virtual router configured on the switch.

show ip vrrp interface brief

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Router)#show ip vrrp interface brief

Interface    VRID    IP Address         Mode         State
----------   -----   ---------------    ----------   ----------
Vlan6        6       192.168.16.1       Enable       Master
Vlan10       10      192.168.20.1       Enable       Master
Vlan60       60      192.168.2.1        Enable       Master
Vlan808      8       100.65.251.150     Enable       Master
Vlan200      200     192.168.40.1       Enable       Master
Vlan201      201     192.168.41.1       Enable       Master
```

Display Parameters

Interface	*slot/port*
VRID	Router lD of the virtual router.
IP Address	Virtual router IP address.
Mode	Indicates whether the virtual router is enabled or disabled.
State	State (Master/Backup) of the virtual router.

DHCP and BOOTP Relay Commands

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

7-108 bootpdhcprelay cidoptmode

Enable the circuit ID option mode for BootP/DHCP Relay on the system.

No command disables the circuit ID option mode for BootP/DHCP Relay on the system.

bootpdhcprelay cidoptmode

no bootpdhcprelay cidoptmode

Parameters

None

Default

The default is Disabled.

Command Mode

- Global Config
- Virtual Router Config

7-109 bootpdhcprelay maxhopcount

Configure the maximum allowable relay agent hops for BootP/DHCP Relay on the system.

No command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

bootpdhcprelay maxhopcount *1-16*

no bootpdhcprelay maxhopcount

Parameters

None

Default

The default is 4.

Command Mode

- Global Config
- Virtual Router Config

7-110 bootpdhcprelay minwaittime

Configure 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.

No command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

bootpdhcprelay minwaittime *0-100*

no bootpdhcprelay minwaittime

Parameters

None

Default

The default is 0.

Command Mode

- Global Config
- Virtual Router Config

7-111 show bootpdhcprelay

Display the BootP/DHCP Relay information for the virtual router. If no router is specified, information for the default router is displayed.

show bootpdhcprelay [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	Display the value of BOOTP/DHCP relay parameters of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- Global Config

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show bootpdhcprelay

Maximum Hop Count.............................. 5
Minimum Wait Time(Seconds)..................... 0
Admin Mode..................................... Disable
Circuit Id option mode......................... Enable
```

Display Parameters

Maximum Hop Count	Maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	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.

IP Helper Commands

This section describes the commands used to configure and monitor the IP Helper agent. IP Helper relays DHCP and other broadcast UDP packets from a local client to one or more servers which are not on the same network as the client.

The IP Helper feature provides a mechanism that allows a router to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications to reach servers on non-local subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

Table 9: Default Ports – UDP Port Numbers Implied by Wildcard

Protocol	UDP Port Number
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS+ Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

The system limits the number of relay entries to four times the maximum number of routing interfaces. The network administrator can allocate the relay entries as desired. There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for a given {interface, UDP port} pair.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays to the client packets that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent checks if the interface is configured to relay the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent checks if there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed. Note that if the packet matches a discard relay entry on the ingress interface, then the packet is not forwarded, regardless of the global configuration.

The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF)
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

7-112 clear ip helper statistics

Reset to zero the statistics displayed in **show ip helper statistics** command for the specified virtual router. If no router is specified, the command is executed for the default router.

clear ip helper statistics [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Clear IP helper statistics of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#clear ip helper statistics
```

7-113 ip helper-address (Global Config)

Configure the relay of certain UDP broadcast packets received on any interface. This command can be invoked multiple times, either to specify multiple server addresses for a given UDP port number or to specify multiple UDP port numbers handled by a specific server.

No command deletes an IP helper entry. The command no ip helper-address with no arguments clears all global IP helper addresses.

ip helper-address *server-address* **[***dest-udp-port* **| dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]**

no ip helper-address [*server-address* **[***dest-udp-port* **| dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]**

Parameters

server-address	IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
dest-udp-port	(Optional) Destination UDP port number from 1 to 65535.
port-name	(Optional) The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • DHCP (port 67) • domain (port 53)

- isakmp (port 500)
- mobile-ip (port 434)
- nameserver (port 42)
- netbios-dgm (port 138)
- netbios-ns (port 137)
- ntp (port 123)
- pim-auto-rp (port 496)
- tacacs (port 49)
- tftp (port 69)
- time (port 37)

Other ports must be specified by number.

Default

The default is as follows: helper addresses are not configured.

Command Mode

Global Config

Example

To relay DHCP packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands.

```
(Routing)#config
(Routing)(Config)#ip helper-address 10.1.1.1 dhcp
(Routing)(Config)#ip helper-address 10.1.2.1 dhcp
```

To relay UDP packets received on any interface for all default ports to the server at 20.1 .1.1, use the following commands.

```
(Routing)#config
(Routing)(Config)#ip helper-address 20.1.1.1
```

7-114 ip helper-address (Interface Config)

Configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

No command deletes a relay entry on an interface. The no command with no arguments clears all helper addresses on the interface.

ip helper-address {*server-address* **| discard} [***dest-udp-port* **| dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]**

no ip helper-address [*server-address* **| discard] [***dest-udp-port* **| dhcp | domain | isakmp | mobile ip | nameser-ver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]**

Parameters

server-address	IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be in a subnet on the interface where the relay entry is configured, and cannot be an IP address configured on any interface of the local router.
discard	Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.
dest-udp-port	(Optional) Destination UDP port number from 0 to 65535.
port-name	(Optional) The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • DHCP (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • NTP (port 123) • pim-auto-rp (port 496) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Default

The default is as follows: helper addresses are not configured.

Command Mode

Interface Config

Example

To relay DHCP packets received on interface 0/2 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands.

```
(Routing)#config
(Routing)(Config)#interface 0/2
(Routing)(Interface 0/2)#ip helper-address 192.168.10.1 dhcp
(Routing)(Interface 0/2)#ip helper-address 192.168.20.1 dhcp
```

To relay both DHCP and DNS packets to 192.168.30.1, use the following commands.

```
(Routing)#config
(Routing)(Config)#interface 0/2
(Routing)(Interface 0/2)#ip helper-address 192.168.30.1 dhcp
(Routing)(Interface 0/2)#ip helper-address 192.168.30.1 dns
```

This command takes precedence over an ip helper-address command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than 0/2 and 0/17 to 192.168.40.1, relays DHCP and DNS packets received on 0/2 to 192.168.40.2, relays SNMP traps (port 162) received on interface 0/17 to 192.168.23.1, and drops DHCP packets received on 0/17.

```
(Routing)#config
(Routing)(Config)#ip helper-address 192.168.40.1 dhcp
(Routing)(Config)#interface 0/2
(Routing)(Interface 0/2)#ip helper-address 192.168.40.2 dhcp
(Routing)(Interface 0/2)#ip helper-address 192.168.40.2 domain
(Routing)(Interface 0/2)#exit

(Routing)(Config)#interface 0/17
(Routing)(Interface 0/17)#ip helper-address 192.168.23.1 162
(Routing)(Interface 0/17)#ip helper-address discard dhcp
```

7-115 ip helper enable

Enable relay of UDP packets. This command can be used to temporarily disable IP helper without deleting all IP helper addresses. This command replaces the **bootpdhcprelay enable** command, and affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

No command disables relay of all UDP packets.

ip helper enable

no ip helper enable

Parameters

None

Default

The default is Disabled.

Command Mode

- Global Config
- Virtual Router Config

Example

The following shows an example of the command.

```
(Routing)(Config)#ip helper enable
```

7-116 show ip helper-address

Display the IP helper address configuration on the specified virtual router. If no virtual router is specified, the configuration of the default router is displayed. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **VLAN** is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format.

show ip helper-address [vrf *vrf-name***] [{***slot/port* **| vlan 1-4093}]**

Parameters

vrf *vrf-name*	(Optional) Display the Helper IP's list information of a virtual router.
slot/port	(Optional) Enter an interface in slot/port format.
vlan	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

- Privileged EXEC
- Virtual Router Config

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip helper-address

IP helper is enabled

Interface    UDP Port     Discard      Hit Count    Server Address
----------   ----------   ----------   ----------   ---------------
0/1          dhcp         No           10           10.100.1.254
                                                    10.100.2.254
0/17         any          Yes          2
any          dhcp         No           0            10.200.1.254
```

Display Parameters

Interface	Relay configuration is applied to packets that arrive on this interface. This field is set to any for global IP helper entries.
UDP Port	Relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as any are applied to packets with the destination UDP ports listed in Table 4.
Discard	If Yes, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	Number of times the IP helper function has been used to relay or

	discard a packet.
Server Address	IPv4 address of the server to which packets are relayed.

7-117 show ip helper statistics

Display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent on the specified virtual router. lf no virtual router is specified, the configuration of the default router is displayed.

show ip helper statistics [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display the IP helper statistics of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip helper statistics

DHCP client messages received..................... 8
DHCP client messages relayed...................... 2
DHCP server messages received..................... 2
DHCP server messages relayed...................... 2
UDP client messages received...................... 8
UDP client messages relayed....................... 2
DHCP message hop count exceeded max............... 0
DHCP message with secs field below min............ 0
DHCP message with giaddr set to local address.... 0
Packets with expired TTL.......................... 0
Packets that matched a discard entry.............. 0
```

Display Parameters

DHCP client messages received	Number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL>1 and having valid source and destination IP

	addresses.
DHCP client messages relayed	Number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP server messages received	Number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP server messages relayed	Number of DHCP server messages relayed to a client.
UDP clients messages received	Number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP clients messages relayed	Number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.
DHCP message hop count exceeded max	Number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with secs field below min	Number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with giaddr set to local address	Number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.
Packets with expired TTL	Number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	Number of packets ignored by the relay agent because they match a discard relay entry.

Open Shortest Path First Commands

This section describes the commands you use to view and configure Open Shortest Path First (OSPF), which is a link-state routing protocol used to route traffic within a network.

This section contains the following subsections:

General OSPF Commands

7-118 router ospf

Enable OSPF routing in a specified virtual router and to enter Router OSPF mode. If no virtual router is specified, OSPF routing is enabled in the default router.

router ospf [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Virtual router on which to enable OSPF routing.

Default

The default is None.

Command Mode

Global Config

7-119 enable (OSPF)

Reset the default administrative mode of OSPF in the router (active).

No command sets the administrative mode of OSPF in the router to inactive.

enable

no enable

Parameters

None

Default

The default is Enabled.

Command Mode

Router OSPF Config

7-120 network area (OSPF)

Enable OSPFv2 on an interface and set its area ID if the IP address of an interface is covered by this network command.

No command disables the OSPFv2 on an interface if the IP address of an interface was earlier covered by this network command.

network *ip-address wildcard-mask* **area** *area-id*

no network *ip-address wildcard-mask* **area** *area-id*

Parameters

ip-address	Enter an IP Address.
wildcard-mask	IP-address-type mask that includes “don't-care bits”.
area-id	Identifies the OSPF Router Area identification.

Default

The default is Disabled.

Command Mode

Router OSPF Config

7-121 1583compatibility

Enable OSPF 1583 compatibility.

No command disables OSPF 1583 compatibility.

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

1583compatibility

no 1583compatibility

Parameters

None

Default

The default is Enabled.

Command Mode

Router OSPF Config

7-122 area default-cost (OSPF)

Configure the default cost for the stub area. You must specify the area ID and an integer value from 1 to 16777215.

area *areaid* **default-cost** *1-16777215*

Parameters

areaid	Indicates an area ID.

Default

The default is None.

Command Mode

Router OSPF Config

7-123 area nssa (OSPF)

Configure the specified areaid to function as an NSSA.

No command disables nssa from the specified area ID.

area *areaid* **nssa**

no area *areaid* **nssa**

Parameters

areaid	Indicates an area ID.

Default

The default is None.

Command Mode

Router OSPF Config

7-124 area nssa default-info-originate (OSPF)

Configure the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is ****. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

No command disables the default route advertised into the NSSA.

area *areaid* **nssa default-info-originate [***metric***] [{comparable | non-comparable}]**

no area *areaid* **nssa default-info-originate [***metric***] [{comparable | non-comparable}]**

Parameters

areaid	Indicates an area ID.
metric	Indicates the metric value: (1-16777214).
comparable	Configure the Metric Type as comparable.

non-comparable	Configure the Metric Type as non-comparable.

Default

The default is None.

Command Mode

Router OSPF Config

7-125 area nssa no-redistribute (OSPF)

Configure the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

No command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

area *areaid* **nssa no-redistribute**

no area *areaid* **nssa no-redistribute**

Parameters

areaid	Indicates an area ID.

Default

The default is None.

Command Mode

Router OSPF Config

7-126 area nssa no-summary(OSPF)

Configure the NSSA so that summary LSAs are not advertised into the NSSA.

No command disables nssa from the summary LSAs.

area *areaid* **nssa no-summary**

no area *areaid* **nssa no-summary**

Parameters

areaid	Indicates an area ID.

Default

The default is None.

Command Mode

Router OSPF Config

7-127 area nssa translator-role (OSPF)

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

No command disables the nssa translator role from the specified area id.

area *areaid* **nssa translator-role {always | candidate}**

no area *areaid* **nssa translator-role {always | candidate}**

Parameters

areaid	Indicates an area ID.
always	Enter always for the translator role.
candidate	Enter candidate for the translator role.

Default

The default is None.

Command Mode

Router OSPF Config

7-128 area nssa translator-stab-intv (OSPF)

Configure the translator stability interval of the NSSA. The stability interval is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

No command disables the nssa translator's stability interval from the specified area id.

area *areaid* **nssa translator-stab-intv** *stabilityinterval*

no area *areaid* **nssa translator-stab-intv** *stabilityinterval*

Parameters

areaid	Indicates an area ID.
stabilityinterval	Enter an integer for the Translator Stability interval (0-3600).

Default

The default is None.

Command Mode

Router OSPF Config

7-129 area range (OSPF)

Use the area range command in Router Configuration mode to configure a summary prefix that an area border router advertises for a specific area.

No command deletes a specified area range or reverts an option to its default.

area *areaid* **range** *prefix netmask* **{summarylink | nssaexternallink} [advertise | not-advertise] [cost** *cost***]**

no area *areaid* **range** *prefix netmask* **{summarylink | nssaexternallink} [advertise | not-advertise] [cost]**

Parameters

areaid	Area identifier for the area whose networks are to be summarized.
prefix netmask	Summary prefix to be advertised when the ABR computes a route to one or more networks within this prefix in this area.
summarylink	When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	(Optional) When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.
not-advertise	(Optional) When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. When the not-advertise option is given, any static cost previously configured is removed from the system configuration.
cost	(Optional) If an optional cost is given, OSPF sets the metric field in the summary LSA to the configured value rather than setting the metric to the largest cost among the networks covered by the area range. A static cost may only be configured if the area range is configured to advertise the summary. The range is 0 to 16,777,215. If the cost is set to 16,777,215 for type 3 summarization, a type 3 summary LSA is not advertised, but contained networks are suppressed. This behavior is equivalent to specifying the not-advertise option. If the range is

	configured for type 7 to type 5 translation, a type 5 LSA is sent if the metric is set to 16,777,215; however other routers will not compute a route from a type 5 LSA with this metric.

Default

The default is as follows: Area ranges and cost are not configured.

Command Mode

OSPFv2 Router Config

Example

The following shows an example of the command.

```
!!Create area range
(Routing) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink

!!Delete area range
(Routing) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink
```

The no form may be used to revert the [advertise | not-advertise] option to its default without deleting the area range. Deleting and recreating the area range would cause OSPF to temporarily advertise the prefixes contained within the range. Note that using either the advertise or not-advertise keyword reverts the configuration to the default. For example:

```
!!Create area range. Suppress summary.
(Routing) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink not-advertise

!!Advertise summary.
(Routing) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink not-advertise
```

The no form may be use to remove a static area range cost, so that OSPF sets the cost to the largest cost among the contained routes.

```
!!Create area range with static cost.
(Routing)(Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink cost 1000

!!Remove static cost.
(Routing)(Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink cost
```

7-130 area stub (OSPF)

Create a stub area for the specified area ID. A stub area is characterized by AS External LSAs not being propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

No command deletes a stub area for the specified area ID.

area *areaid* **stub**

no area *areaid* **stub**

Parameters

areaid	Indicates an area ID.

Default

The default is None.

Command Mode

Router OSPF Config

7-131 area stub no-summary (OSPF)

Configure the Summary LSA mode for the stub area identified by *areaid*. Use this command to prevent LSA Summaries from being sent.

No command configures the default Summary LSA mode for the stub area identified by *areaid*.

area *areaid* **stub no-summary**

no area *areaid* **stub no-summary**

Parameters

areaid	Indicates an area ID.

Default

The default is Disabled.

Command Mode

Router OSPF Config

7-132 area virtual-link (OSPF)

Create the OSPF virtual interface for the specified *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

No command deletes the OSPF virtual interface from the given interface, identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

area *areaid* **virtual-link** *neighbor*

no area *areaid* **virtual-link** *neighbor*

Parameters

areaid	Indicates an area ID.
neighbor	Enter the router ID of the virtual neighbor.

Default

The default is None.

Command Mode

Router OSPF Config

7-133 area virtual-link authentication

Configure the authentication type and key for the OSPF virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The value for type is either none, simple, or encrypt. The *key* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypted, a key ID in the range of 0 and 255 must be specified. The default value for authentication type is none. Neither the default password key nor the default key ID are configured.

No command configures the default authentication type for the OSPF virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

area *areaid* **virtual-link** *neighbor* **authentication {none | {simple** *key***} | {encrypt** *key keyid***)}**

no area *areaid* **virtual-link** *neighbor* **authentication**

Parameters

areaid	Indicates an area ID.
neighbor	Enter the router ID of the virtual neighbor.
none	Configure authentication type none for an OSPF virtual link.
simple *key*	Configure authentication type simple for an OSPF virtual link.
encrypt *key keyid*	Configure MD5 encryption for an OSPF virtual link.

Default

The default is None.

Command Mode

Router OSPF Config

7-134 area virtual-link dead-interval (OSPF)

Configure the dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

No command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

area *areaid* **virtual-link** *neighbor* **dead-interval** *1-65535*

no area *areaid* **virtual-link** *neighbor* **dead-interval**

Parameters

areaid	Indicates an area ID.
neighbor	Enter the router ID of the virtual neighbor.

Default

The default is 40.

Command Mode

Router OSPF Config

7-135 area virtual-link hello-interval (OSPF)

Configure the hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

No command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

area *areaid* **virtual-link** *neighbor* **hello-interval** *1-65535*

no area *areaid* **virtual-link** *neighbor* **hello-interval**

Parameters

areaid	Indicates an area ID.
neighbor	Enter the router ID of the virtual neighbor.

Default

The default is 10.

Command Mode

Router OSPF Config

7-136 area virtual-link retransmit-interval (OSPF)

Configure the retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

No command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

area *areaid* **virtual-link** *neighbor* **retransmit-interval** *0-3600*

no area areaid virtual-link neighbor retransmit-interval seconds

Parameters

areaid	Indicates an area ID.
neighbor	Enter the router ID of the virtual neighbor.

Default

The default is 5 seconds.

Command Mode

Router OSPF Config

7-137 area virtual-link transmit-delay (OSPF)

Configure the transmit delay for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

No command resets the default transmit delay for the OSPF virtual interface to the default value.

area *areaid* **virtual-link** *neighbor* **transmit-delay** *0-3600*

no area *areaid* **virtual-link** *neighbor* **transmit-delay**

Parameters

areaid	Indicates an area ID.
neighbor	Enter the router ID of the virtual neighbor.

Default

The default is 1 second.

Command Mode

Router OSPF Config

7-138 auto-cost (OSPF)

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the **auto-cost reference bandwidth** and **bandwidth** commands give you control over the default link cost. You can configure an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where interface bandwidth is defined by the bandwidth command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the **auto-cost** command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps).

No command sets the reference bandwidth to the default value.

auto-cost reference-bandwidth *1-4294967*

no auto-cost reference-bandwidth

Parameters

None

Default

The default is 100 Mbps.

Command Mode

Router OSPF Config

7-139 capability opaque

Enable Opaque Capability on the Router. The information contained in Opaque LSAs may be used directly by OSPF or indirectly by an application wishing to distribute information throughout the OSPF domain. D-LINK OS supports the storing and flooding of Opaque LSAs of different scopes. The default value of enabled means that OSPF will forward opaque LSAs by default. If you want to upgrade from a previous release, where the default was disabled, opaque LSA forwarding will be enabled. If you want to disable opaque LSA forwarding, then you should enter the command no capability opaque in OSPF router configuration mode after the software upgrade.

No command disables opaque capability on the router.

capability opaque

no capability opaque

Parameters

None

Default

The default is Enabled.

Command Mode

Router Config

7-140 clear ip ospf

Disable and reenable OSPF for the specified virtual router. If no virtual router is specified, the default router is disabled and re-enabled.

clear ip ospf [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Indicates the OSPF protocol of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

7-141 clear ip ospf configuration

Reset the OSPF configuration to factory defaults for the specified virtual router. If no virtual router is specified, the default router is cleared.

clear ip ospf configuration [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Indicates the OSPF protocol of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

7-142 clear ip ospf counters

Reset global and interface statistics for the specified virtual router. lf no virtual router is specified, the global and interface statistics are reset for the default router.

clear ip ospf counters [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Indicates the OSPF protocol of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

7-143 clear ip ospf neighbor

Drop the adjacency with all OSPF neighbors for the specified virtual router. On each neighbors interface, send a one-way hello. Adjacencies may then be re-established. If no router is specified, adjacency with all OSPF neighbors is dropped for the default router. To drop all adjacencies with a specific router ID, specify the neighbors Router ID using the optional parameter [***neighbor-id***].

clear ip ospf neighbor [*neighbor-id***] [vrf** *vrf-name***]**

Parameters

neighbor-id	(Optional) Enter the neighbor's Router ID.
vrf *vrf-name*	(Optional) Bounce all OSPF neighbors of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

7-144 clear ip ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter [*slot/port*]. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [*neighbor-id*].

clear ip ospf neighbor interface [*slot/port***] [***neighbor-id***]**

Parameters

slot/port	Enter an interface in slot/port format.
vlan *vlan*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

7-145 clear ip ospf redistribution

Flush all self-originated external LSAs for the specified virtual router. If no router is specified, the command is executed for the default router. Reapply the redistribution configuration and reoriginate prefixes as necessary.

clear ip ospf redistribution [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Flush and reoriginate external LSAs of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

7-146 default-information originate (OSPF)

Control the advertisement of default routes.

No command controls the advertisement of default routes.

default-information originate [always] [metric *0-16777214***] [metric-type {1 | 2}]**

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

Parameters

always	(Optional) Origination does not depend on whether routing table has a default route.

metric *0-16777214*	(Optional) The range of the metric is 0-16777214.
metric-type {1 | 2}	(Optional) Specify the Open Shortest Path First (OSPF) external type 1, equivalent to the link-state metric, or external type 2, cost assigned by the AS boundary router, metric.

Default

- metric – unspecified
- type – 2

Command Mode

Router OSPF Config

7-147 default-metric (OSPF)

Set a default for the metric of distributed routes.

No command sets a default for the metric of distributed routes.

default-metric *1-16777214*

no default-metric

Parameters

None

Default

The default is None.

Command Mode

Router OSPF Config

7-148 distance ospf (OSPF)

Set the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be **intra**, **inter**, or **external**. All the external type routes are given the same preference value. The range of preference value is 1 to 255.

No command sets the default route preference value of OSPF routes in the router. The type of OSPF can be intra, inter, or external. All the external type routes are given the same preference value.

distance ospf {intra-area *1-255* **| inter-area** *1-255* **| external** *1-255***}**

no distance ospf {intro-area | inter-area | external}

Parameters

intra-area *1-255*	Indicates the intra-area route (1 to 255).
inter-area *1-255*	Indicates the inter-area route (1 to 255).
external *1-255*	Indicates the number of external OSPF routes (1 to 255).

Default

The default is 110.

Command Mode

Router OSPF Config

7-149 distribute-list out (OSPF)

Specify the access list to filter routes received from the source protocol.

No command disables the filter.

distribute-list *1-199* **out {bgp | static | connected}**

no distribute-list *1-199* **out {bgp | static | connected}**

Parameters

bgp	Source protocol is BGP.
static	Source protocol is static.
connected	Source protocol is connected.

Default

The default is None.

Command Mode

Router OSPF Config

7-150 exit-overflow-interval (OSPF)

Configure the exit overflow interval for OSPF. It describes the number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave overflow state until restarted.

No command configures the default exit overflow interval for OSPF.

exit-overflow-interval *0-2147483647*

no exit-overflow-interval

Parameters

seconds	Indicates the interval in seconds (0-2147483647).

Default

The default is 0 second.

Command Mode

Router OSPF Config

7-151 external-lsdb-limit (OSPF)

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

No command configures the default external LSDB limit for OSPF.

external-lsdb-limit *-1-2147483647*

no external-lsdb-limit

Parameters

None

Default

The default is -1.

Command Mode

Router OSPF Config

7-152 log-adjacency-changes

To enable logging of OSPFv2 neighbor state changes, use the log-adjacency-changes command in router configuration mode. State changes are logged with INFORMATIONAL severity.

No command disables state change logging.

log-adjacency-changes [detail]

no log-adjacency-changes [detail]

Parameters

detail	(Optional) When this keyword is specified, all adjacency state changes are logged. Otherwise OSPF only logs transitions to FULL state and when a backwards transition Occurs.

Default

The default is as follows: adjacency state changes are logged, but without the detail option.

Command Mode

OSPFv2 Router Config

7-153 prefix-suppression (Router OSPF Config)

Suppresses the advertisement of all the IPv4 prefixes except for prefixes that are associated with secondary IPv4 addresses, loopbacks, and passive interfaces from the OSPFv2 router advertisements.

To suppress a loopback or passive interface, use the **ip ospf prefix-suppression** command in interface configuration mode. Prefixes associated with secondary IPv4 addresses can never be suppressed.

No command disables prefix-suppression. No prefixes are suppressed from getting advertised.

prefix-suppression

no prefix-suppression

Parameters

None

Default

The default is as follows: prefix suppression is disabled.

Command Mode

Router OSPF Config

7-154 prefix-suppression (Router OSPFv3 Config)

Suppresses the advertisement of all the IPv6 prefixes except for prefixes that are associated with secondary IPv6 addresses, loopbacks, and passive interfaces from the OSPFv3 router advertisements.

To suppress a loopback or passive interface, use the **ip ospf prefix-suppression** command in interface configuration mode. Prefixes associated with secondary IPv6 addresses can never be suppressed.

No command disables prefix-suppression. No prefixes are suppressed from getting advertised.

prefix-suppression

no prefix-suppression

Parameters

None

Default

The default is as follows: prefix suppression is disabled.

Command Mode

Router OSPFv3 Config

7-155 router-id (OSPF)

Set a 4-digit dotted-decimal number uniquely identifying the router OSPF ID. The ipaddress is a configured value.

router-id *ipaddress*

Parameters

ipaddress	Indicates the IP Address.

Default

The default is None.

Command Mode

Router OSPF Config

7-156 redistribute (OSPF)

Configure OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

No command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

redistribute {bgp | static | connected} [metric *0-16777214***] [metric-type {1 I 2}] [tag** *0-4294967295***] [subnets]**

no redistribute {bgp | static | connected} [metric] [metric-type] [tag] [subnets]

Parameters

bgp	Source protocol is BGP.
static	Source protocol is static.
connected	Source protocol is connected.
metric *0-16777214*	(Optional) Configures the OSPF route redistribution metric.
metric-type {1 l 2}	(Optional) Configures the OSPF route redistribution metric type.
tag *0-4294967295*	(Optional) Configures the OSPF route redistribution tag.
subnets	(Optional) Allow subnets to be redistributed into OSPF.

Default

The default is as follows:

- metric – unspecified
- type – 2
- tag – 0

Command Mode

Router OSPF Config

7-157 maximum-paths (OSPF)

Set the number of paths that OSPF can report for a given destination where maxpaths is platform dependent.

No command resets the number of paths that OSPF can report for a given destination back to its default value.

maximum-paths *maxpaths*

no maximum-paths

Parameters

maxpaths	Indicates a maximum path value from 1 to 48.

Default

The default is 4.

Command Mode

Router OSPF Config

7-158 passive-interface default (OSPF)

Enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF will not form adjacencies over a passive interface.

No command disables the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

passive-interface default

no passive-interface default

Parameters

None

Default

The default is Disabled.

Command Mode

Router OSPF Config

7-159 passive-interface (OSPF)

Set the interface as passive. It overrides the global passive mode that is currently effective on the interface.

No command sets the interface as non-passive. It overrides the global passive mode that is currently effective on the interface.

passive-interface {*slot/port* **| vlan** *vlan-id***}**

no passive-interface {*slot/port* **| vlan** *vlan-id***}**

Parameters

slot/port	Enter an interface in slot/port format.
vlan *vlan-id*	Enter an interface in VLAN format.

Default

The default is Disabled.

Command Mode

Router OSPF Config

7-160 timers pacing flood

To adjust the rate at which OSPFv2 sends LS Update packets, use the timers pacing flood command in router OSPFv2 global configuration mode. OSPF distributes routing information in Link State Advertisements (LSAs), which are bundled into Link State Update (LS Update) packets. To reduce the likelihood of sending a neighbor more packets than it can buffer, OSPF rate limits the transmission of LS Update packets. By default, OSPF sends up to 30 updates per second on each interface. Use this command to adjust this packet rate.

Use the **no** command to revert LSA transmit pacing to the default rate.

timers pacing flood *milliseconds*

no timers pacing flood

Parameters

milliseconds	Average time between transmission of LS Update packets. The range is 5 ms to 100 ms.

Default

The default is 33 milliseconds.

Command Mode

OSPFv2 Router Config

7-161 timers pacing lsa-group

To adjust how OSPF groups LSAs for periodic refresh, use the timers pacing lsa-group command in OSPFv2 Router Configuration mode. OSPF refreshes self-originated LSAs approximately once every 30 minutes. When OSPF refreshes LSAs, it considers all self-originated LSAs whose age is from 1800 to 1800 plus the pacing group size. Grouping LSAs for refresh allows OSPF to combine refreshed LSAs into a minimal number of LS Update packets. Minimizing the number of Update packets makes LSA distribution more efficient.

When OSPF originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPF refreshes the LSA. By selecting a random refresh delay, OSPF avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.

timers pacing lsa-group *seconds*

Parameters

seconds	Width of the window in which LSAs are refreshed. The range for the pacing group window is from 10 to 1800 seconds.

Default

The default is 60 seconds.

Command Mode

OSPFv2 Router Config

7-162 timers spf

Configure the SPF delay time and hold time. The valid range for both parameters is 0-65535 seconds.

timers spf *delay-time hold-time*

Parameters

delay-time	Indicates the delay timer value (0-65535) in seconds.
hold-time	Indicates the hold timer value (0-65535) in seconds.

Default

The default is as follows:

- delay-time – 5
- hold-time – 10

Command Mode

Router OSPF Config

7-163 trapflags (OSPF)

Enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at once. The different groups of trapflags, and each group's specific trapflags to enable or disable, are listed in Table 10.

Table 10: Trapflags Groups

Group	Flags
errors	• authentication-failure • bad-packet • config-error • virt-authentication-failure • virt-bad-packet • virt-config-error
lsa	• lsa-maxage • lsa-originate
overflow	• lsdb-overflow • lsdb-approaching-overflow

retransmit	• packets • virt-packets
state-change	• if-state-change • neighbor-state-change • virtif-state-change • virtneighbor-state-change

Use the **No** command to remove.

- To enable the individual flag, enter the group name followed by that particular flag.
- To enable all the flags in that group, give the group name followed by **all**.
- To enable all the flags, give the command as **trapflags all**.

trapflags {all | errors {all | authentication-failure | bad-packet | config-error | virt-authentication-failure | virt-bad-packet | virt-config-error} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} | state-change {all | if-state-change | neighbor-state-change | virtif-state-change | virtneighbor-state-change}}

no trapflags {all | errors {all | authentication-failure | bad-packet | config-error | virt-authentication-failure | virt-bad-packet | virt-config-error} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} | state-change {all I if-state-change | neighbor-state-change | virtif-state-change | virtneighbor-state-change}}

Parameters

all	Enable/Disable all Traps.
errors	Enable/Disable OSPF Trap errors.
authentication-failure	Authentication failure on non virtual interfaces.
bad-packet	Packet parse failure on non virtual interfaces.
config-error	Config mismatch errors on non virtual interfaces.
virt-authentication-failure	Authentication failure on virtual interfaces.
virt-bad-packet	Packet parse failure on virtual interfaces.
virt-config-error	Config mismatch errors on virtual interfaces.
all	Enable/Disable all Traps.
lsa-maxage	LSA aged to maxage.
lsa-originate	New LSA originated.
overflow	Enable/Disable overflow traps.
all	Enable/Disable all Traps.
lsdb-overflow	LSDB overflow.
lsdb-approaching-overflow	LSDB approaching overflow.
retransmit	Enable/Disable packet retransmit traps.
all	Enable/Disable all Traps.

packets	Packet retransmission on non virtual interfaces.
virt-packets	Packet retransmission on virtual interfaces.
state-change	Enable/Disable state change traps.
all	Enable/Disable all Traps.
if-state-change	Non virtual interface state changes.
neighbor-state-change	Neighbor state changes on non virtual interfaces.
virtif-state-change	Virtual interface state changes.
virtneighbor-state-change	Non virtual neighbor state changes.

Default

The default is Disabled.

Command Mode

Router OSPF Config

OSPF Interface Commands

7-164 ip ospf area

Enable OSPFv2 and set the area ID of an interface or range of interfaces. The area-id is an IP address formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0-4294967295. This command supersedes the effects of the **network area** command. It can also be used to configure the advertiseability of the secondary addresses on this interface into the OSPFv2 domain.

No command disables OSPF on an interface.

ip ospf area *area-id* **[secondaries none]**

no ip ospf area [secondaies none]

Parameters

area-id	Configure OSPF area to which the specified interface belongs. Indicate an OSPF area ID as decimal value (0-4294967295) or an IP address format.
secondaries none	Enable/Disable the advertisability of all secondary addresses.

Default

The default is Disabled.

Command Mode

Interface Config

7-165 bandwidth

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the **auto-cost** command. For the purpose of the OSPF link cost calculation, use the bandwidth command to specify the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface. You can use this command to configure a single interface or a range of interfaces.

No command sets the interface bandwidth to its default value.

bandwidth *1-10000000*

no bandwidth

Parameters

None

Default

The default is as follows: actual interface bandwidth.

Command Mode

Global Config

7-166 ip ospf authentication

Set the OSPF Authentication Type and Key for the specified interface or range of interfaces. The value of type is either none, simple, or encrypt. The *key* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. If the type is encrypt, a *keyid* in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

No command sets the default OSPF Authentication Type for the specified interface.

ip ospf authentication {none | {simple *key***} | {encrypt** *key keyid***}}**

no ip ospf authentication

Parameters

none	Configure authentication type none for an OSPF interface.
simple *key*	Configure authentication type simple for an OSPF interface.
encrypt *key keyid*	Configure MD5 encryption for an OSPF interface.

Default

The default is None.

Command Mode

Interface Config

7-167 ip ospf cost

Configure the cost on an OSPF interface or range of interfaces.

No command configures the default cost on an OSPF interface.

ip ospf cost *1-65535*

no ip ospf cost

Parameters

None

Default

The default is 10.

Command Mode

Interface Config

7-168 ip ospf database-filter all out

Use the **ip ospf database-filter all out** command in Interface Configuration mode to disable OSPFv2 LSA flooding on an interface.

Use the **no** command in Interface Configuration mode to enable OSPFv2 LSA flooding on an interface.

ip ospf database-filter all out

no ip ospf database-filter all out

Parameters

None

Default

The default is Disabled.

Command Mode

lnterface Config

7-169 ip ospf dead-interval

Set the OSPF dead interval for the specified interface or range of interfaces. The value for *seconds* is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello interval (i.e. 4). Valid values range in seconds from 1 to 65535.

No command sets the default OSPF dead interval for the specified interface.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameters

seconds	Indicates the interval in seconds (1-65535).

Default

The default is None.

Command Mode

Interface Config

7-170 ip ospf hello-interval

Set the OSPF hello interval for the specified interface or range of interfaces. The value for *seconds* is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network. Valid values range from 1 to 65535.

No command sets the default OSPF hello interval for the specified interface.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameters

seconds	Indicates the interval in seconds (1-65535).

Default

The default is 10.

Command Mode

Interface Config

7-171 ip ospf network

Configure OSPF to treat an interface or range of interfaces as a point-to-point rather than broadcast interface. The **broadcast** option sets the OSPF network type to broadcast. The **point-to-point** option sets the OSPF network type to point-to-point. OSPF treats interfaces as broadcast interfaces by default. (Loopback interfaces have a special loopback network type, which cannot be changed.) When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

Use the **no** command to return the OSPF network type to the default.

ip ospf network (broadcast | point-to-point}

no ip ospf network

Parameters

broadcast	Set the OSPF network type to Broadcast.
point-to-point	Set the OSPF network type to Point-to-Point.

Default

The default is Broadcast.

Command Mode

Interface Config

7-172 ip ospf prefix-suppression

Suppresses the advertisement of the IPv4 prefixes that are associated with an interface, except for those associated with secondary IPv4 addresses. This command takes precedence over the global configuration. If this configuration is not specified, the global prefix-suppression configuration applies.

Prefix-suppression can be disabled at the interface level by using the disable option. The disable option is useful for excluding specific interfaces from performing prefix-suppression when the feature is enabled globally.

Note that the disable option disable is not equivalent to not configuring the interface specific prefix-suppression. If prefix-suppression is not configured at the interface level, the global prefix-suppression configuration is applicable for the IPv4 prefixes associated with the interface.

No command removes prefix-suppression configurations at the interface level. When no ip ospf prefix-suppression command is used, global prefix-suppression applies to the interface. Not configuring the command is not equal to disabling interface level prefix-suppression.

ip ospf prefix-suppression [disable]

no ip ospf prefix-suppression

Parameters

disable	Disable prefix-suppression on the interface.

Default

The default is as follows: prefix-suppression is not configured.

Command Mode

Interface Config

7-173 ip ospf priority

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

No command sets the default OSPF priority for the specified router interface.

ip ospf priority *0-255*

no ip ospf priority

Parameters

None

Default

The default is 1 (highest router priority).

Command Mode

Interface Config

7-174 ip ospf retransmit-interval

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

No command sets the default OSPF retransmit interval for the specified interface.

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Parameters

seconds	Indicates interval time in seconds.

Default

The default is 5.

Command Mode

Interface Config

7-175 ip ospf transmit-delay

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

No command sets the default OSPF Transit Delay for the specified interface.

ip ospf transmit-delay *1-3600*

no ip ospf transmit-delay

Parameters

None

Default

The default is 1.

Command Mode

Interface Config

7-176 ip ospf mtu-ignore

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

Use the **no** command to enable the OSPF MTU mismatch detection.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

OSPF Graceful Restart Commands

The OSPF protocol can be configured to participate in the checkpointing service, so that these protocols can execute a “graceful restart” when the management unit fails. In a graceful restart, the hardware continues forwarding IPv4 packets using OSPF routes while a backup switch takes over management unit responsibility

Graceful restart uses the concept of “helpful neighbors". A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. A planned restart is initiated by the operator through the management command initiate failover. The operator may initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.

7-177 nsf

Enable the OSPF graceful restart functionality on an interface.

No command disables graceful restart for all restarts.

nsf [ietf] [helper] [planned-only]

no nsf [ietf] [planned-only]

Parameters

ietf	(Optional) Keyword is accepted but not required.
helper	(Optional) Configure to act as a graceful restart helpful neighbor.
planned-only	(Optional) This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).

Default

The default is Disabled.

Command Mode

OSPF Router Config

7-178 nsf helper

Enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

No command disables helpful neighbor functionality for OSPF.

nsf helper [planned-only]

no nsf helper

Parameters

planned-only	(Optional) This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

Default

The default is as follows: OSPF acts as a helpful neighbor for both planned and unplanned restarts.

Command Mode

OSPF Router Config

7-179 nsf ietf helper disable

Disable helpful neighbor functionality for OSPF.

nsf ietf helper disable

Parameters

None

Default

The default is None.

Command Mode

OSPF Router Config

7-180 nsf helper strict-lsa-checking

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router. A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

Use the **no** command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

nsf [ietf] helper strict-lsa-checking

no nsf [ietf] helper strict-lsa-checking

Parameters

ietf	(Optional) This keyword is accepted but not required.

Default

The default is Enabled.

Command Mode

OSPF Router Config

OSPFv2 Stub Router Commands

7-181 max-metric router-lsa

To configure OSPF to enter stub router mode, use this command in Router OSPF Global Configuration mode. When OSPF is in stub router mode, as defined by RFC 3137, OSPF sets the metric in the non-stub links in its router LSA to Lslnfinity. Other routers therefore compute very long paths through the stub router, and prefer any alternate path. Doing so eliminates all transit traffic through the stub router, when alternate routes are available. Stub router mode is useful when adding or removing a router from a network or to avoid transient routes when a router reloads.

You can administratively force OSPF into stub router mode, where it will remain until you take it out of stub router mode. Alternatively, you can configure OSPF to start in stub router mode for a configurable period of time after the router boots up.

If you set the summary LSA metric to 16,777,215, other routers will skip the summary LSA when they compute routes.

if you have configured the router to enter stub router mode on startup (max-metric router-lsa on-startup), and then enter max-metric router lsa, there is no change. If OSPF is administratively in stub router mode (the max-metric router-lsa command has been given), and you configure OSPF to enter stub router mode on startup (max-metric router-lsa on-startup), OSPF exits stub router mode (assuming the startup period has expired) and the configuration is updated.

Use the **no** command in OSPFv2 Router Configuration mode to disable stub router mode. The command clears either type of stub router mode (always or on-startup) and resets the summary-lsa option. If OSPF is configured to enter global configuration mode on startup, and during normal operation you want to immediately place OSPF in stub router mode, issue the command no max-metric router-lsa on-startup. The command no max-metric router-lsa summary-lsa causes OSPF to send summary LSAs with metrics computed using normal procedures defined in RFC 2328.

max-metric router-lsa [on-startup seconds] [summary-lsa {metric}]

no max-metric router-lsa [on-startup] [summary-lsa

Parameters

on-startup	(Optional) OSPF starts in stub router mode after a reboot.
seconds	(Required if on-startup) Number of seconds that OSPF remains in stub router mode after a reboot. The range is 5 to 86,400 seconds. There is no default value.
summary-lsa	(Optional) Set the metric in type 3 and type 4 summary LSAs to LsInfinity (0xFFFFFF).
metric	(Optional) Metric to send in summary LSAs when in stub router mode. The range is 1 to 16,777,215. The default is 16,711,680 (0xFF0000).

Default

The default is as follows: OSPF not in stub router mode.

Command Mode

OSPFv2 Router Config

7-182 clear ip ospf stub-router

Use the **clear ip ospf stub-router** command in Privileged EXEC mode to force OSPF to exit stub router mode for the specified virtual router when it has automatically entered stub router mode because of a resource limitation. OSPF only exits stub router mode if it entered stub router mode because of a resource limitation or it if is in stub router mode at startup. If no virtual router is specified, the command is executed for the default router. This command has no effect if OSPF is configured to be in stub router mode permanently.

clear ip ospf stub-router [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	Exit stub router mode of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

OSPF Show Commands

7-183 show ip ospf

Display OSPF global configuration information for the specified virtual router. If no router is specified, it displays information for the default router.

show ip ospf [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Exit stub router mode of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip ospf

Router ID..................................... 3.3.3.3
OSPF Admin Mode............................... Enable
RFC 1583 Compatibility........................ Enable
External LSDB Limit........................... No Limit
Exit Overflow Interval........................ 0
Spf Delay Time................................ 5 sec
Spf Hold Time................................. 10 sec
Flood Pacing Interval......................... 33 ms
LSA Refresh Group Pacing Time................. 60 sec
Opaque capability............................. Enable
AutoCost Ref BW............................... 100 Mbps
Default Passive Setting....................... Disabled
Prefix Suppression............................ Disabled
Maximum Paths................................. 48
Maximum Routes................................ 8160
Default Metric................................ Not configured
Stub Router Configuration..................... None
Summary LSA Metric Override................... Disabled
BFD Enabled................................... NO
```

```
Default Route Advertise..................... Disabled
Always...................................... False
Metric...................................... Not configured
Metric Type................................. External Type 2
Number of Active Areas...................... 1 (1 normal, 0 stub, 0 nssa)
ABR Status.................................. Disable
ASBR Status................................. Disable
Stub Router................................. FALSE
Stub Router Status.......................... Inactive
Stub Router Reason.......................... <reason>
Stub Router Startup Time Remaining.......... <duration> seconds
Stub Router Duration........................ <duration>
External LSDB Overflow...................... FALSE
External LSA Count.......................... 0
External LSAChecksum........................ 0
AS_OPAQUE LSA Count......................... 0
AS_OPAQUE LSA Checksum...................... 0
New LSAs Originated......................... 55
LSAs Received............................... 82
LSA Count................................... 1
Maximum Number of LSAs...................... 24200
LSA High water Mark......................... 9
AS Scope LSA Flood List Length.............. 0
Retransmit List Entries..................... 0
Maximum Number of Retransmit Entries........ 96800
Retransmit Entries High water Mark.......... 1
NSF Helper Support.......................... Always
NSF Helper Strict LSA Checking.............. Enabled
Prefix-suppression.......................... Disabled
```

Display Parameters

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

Router ID	32-bit integer in dotted decimal format identifying the router, about which information is displayed.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled.
RFC 1583 Compatibility	Indicates whether 1583 compatibility is enabled or disabled.
External LSDB Limit	Maximum number of nondefault AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.
Exit Overflow Interval	Number of seconds after entering overflow state that a router will attempt to leave overflow state.
Spf Delay Time	Number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.
Spf Hold Time	Number of seconds between two consecutive SPF calculations.
Flood Pacing Interval	Average time, in milliseconds, between LS Update packet transmissions

	on an interface. This is the value configured with the command "timers pacing flood".
LSA Refresh Group Pacing Time	Size in seconds of the LSA refresh group window. This is the value configured with the command "timers pacing lsa-group".
Opaque Capability	Shows whether the router is capable of sending Opaque LSAs.
Autocost Ref BW	Shows the value of auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.
Prefix suppression	Displays whether the prefix-suppression is enabled or disabled.
Maximum Paths	Maximum number of paths that OSPF can report for a given destination.
Maximum routes	Shows the maximum IPv6 route table size.
Default Metric	Default value for redistributed routes.
Stub Router Configuration	When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF reoriginates its own router LSAs, setting the cost of all nonstub interfaces to infinity. Use this field to set stub router configuration to one of **Always**, **Startup**, **None**.
Stub Router Startup Time	Displays the remaining time, in seconds, until OSPF exits stub router mode. The parameter is listed once OSPF is in startup stub router mode.
Summary LSA Metric Override	One of **Enabled** (met), **Disabled**, where met is the metric to be sent in summary LSAs when in stub router mode.
BFD Enabled	Displays the BFD status.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not.
Always	Shows whether default routes are always advertised.
Metric	Metric of the routes being redistributed. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Number of Active Areas	Number of active OSPF areas. An "active" OSPF area is an area with at least one interface up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. The router automatically becomes an ASBR when it is configured to redistribute routes learned from other protocols. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router Status	One of **Active**, **Inactive**.
Stub Router Reason	One of **Configured**, **Startup**, **Resource Limitation**. **Note:** The row is only listed if stub router is active.
Stub Router Startup Time Remaining	Remaining time, in seconds, until OSPF exits stub router mode. This row is only listed if OSPF is in startup stub router mode.

Stub Router Duration	Time elapsed since the router last entered the stub router mode. The row is only listed if stub router is active and the router entered stub mode because of a resource limitation. The duration is displayed in DD:HH:MM:SS format.
External LSDB Overflow	When the number of nondefault external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated nondefault external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	Number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	Sum of the LS checksums of external link-state advertisements contained in the link-state database.
AS_OPAQUE LSA Count	Shows the number of AS Opaque LSAs in the link-state database.
AS_OPAQUE LSA Checksum	Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.
New LSAs Originated	Number of new link-state advertisements that have been originated.
LSAs Received	Number of link-state advertisements received determined to be new instantiations.
LSA Count	Total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	Maximum number of LSAs that OSPF can store.
LSA High Water Mark	Maximum size of the link state database since the system started.
AS Scope LSA Flood List Length	Number of LSAs currently in the global flood queue waiting to be flooded through the OSPF domain. LSAs with AS flooding scope, such as type 5 external LSAs and type 11 Opaque LSAs.
Retransmit List Entries	Total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
Maximum Number of Retransmit Entries	Maximum number of LSAs that can be waiting for acknowledgment at any given time.
Retransmit Entries High Water Mark	Maximum number of LSAs on all neighbors' retransmit lists at any given time.
NSF Helper Support	Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).
NSF help Strict LSA checking	Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.

7-184 show ip ospf abr

Display the internal OSPF routing table entries to Area Border Routers (ABR) for the specified virtual router. If no router is specified, it displays information for the default router.

show ip ospf abr [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display the OSPF Area Border Routers information of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Router) #show ip ospf abr

Type    Router Id         Cost   Area ID      Next Hop          Next Hop Intf
-----   ---------------   -----  ----------   ---------------   ---------------
Intra   192.168.1.14      100    1            192.168.2.1       0/1
```

Display Parameters

Type	Type of route to the destination: • intra – intra-area route • inter – Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	Outgoing router interface to use when forwarding traffic to the next hop.

7-185 show ip ospf area

Display information about the area for the specified virtual router. If no router is specified, it displays information for the default router. The *areaid* identifies the OSPF area that is being displayed.

show ip ospf area *areaid* **[vrf** *vrf-name***]**

Parameters

areaid	Indicates the area ID.
vrf *vrf-name*	(Optional) Display the OSPF Area Border Routers information of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(R1)#show ip ospf area 1

AreaID..................................... 0.0.0.1
External Routing........................... Import External LSAs
Spf Runs................................... 10
Area Border Router Count................... 0
Area LSA Count............................. 3004
Area LSA Checksum.......................... 0x5e0abed
Flood List Length.......................... 0
Import Summary LSAs........................ Enable
```

Display Parameters

AreaID	Area ID of the requested OSPF area.
External Routing	Number representing the external routing capabilities for this area.
Spf Runs	Number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	Total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	Number representing the Area LSA Checksum for the specified Area ID excluding the external (LS type 5) link-state advertisements.
Flood List Length	Number of LSAs waiting to be flooded within the area.
Import Summary LSAs	Shows whether to import summary LSAs.
OSPF Stub Metric Value	Metric value of the stub area. This field displays only if the area is a configured as a stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA:

Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.
Default Information Originate	Shows whether to advertise a default route into the NSSA.
Default Metric	Metric value for the default route advertised into the NSSA.
Default Metric Type	Metric type for the default route advertised into the NSSA.
Translator Role	NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	Amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

7-186 show ip ospf asbr

Display the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR) for the specified virtual router. If no router is specified, it displays information for the default router.

show ip ospf asbr [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display the OSPF Autonomous System Boundary Routers information of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Type	Type of the route to the destination: • intra – intra-area route • inter – Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	Area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	Outgoing router interface to use when forwarding traffic to the next hop.

7-187 show ip ospf database

Display information about the link state database when OSPF is enabled for the specified virtual router. If no router is specified, it displays information for the default router. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional *areaid* parameter to display database information about a specific area. Use the optional parameters to specify the type of link state advertisements to display.

show ip ospf {*lsid* **| adv-router [rtrid] | asbr-summary [*lsid* | adv-router | self-originate] | database-summary | external [*lsid* | adv-router | self-originate] | network [***lsid*** | adv-router | self-originate] | nssa-external [***lsid*** | adv-router | self-originate] | opaque-area [***lsid*** | adv-router | self-originate] | opaque-as [***lsid*** | adv-router | self-originate] | opaque-link [***lsid*** | adv-router | self-originate] | router [***lsid*** | adv-router | self-originate] | self-originate | summary [***lsid*** | adv-router | self-originate] | vrf *vrf-name***}**

Parameters

lsid	(Optional) Use *lsid* to specify the link state ID (LSID). The value of *lsid* can be an IP address or an integer in the range of 0-4294967295.
adv-router	(Optional) Use **adv-router** to show the LSAs that are restricted by the advertising router.
asbr-summary	(Optional) Use **asbr-summary** to show the autonomous system boundary router (ASBR) summary LSAs.
database-summary	Display LSA database summary information.
external	(Optional) Use **external** to display the external LSAs.
network	(Optional) Use **network** to display the network LSAs.
nssa-external	(Optional) Use **nssa-external** to display NSSA external LSAs.
opaque-area	(Optional) Use **opaque-area** to display area opaque LSAs.
opaque-as	(Optional) Use **opaque-as** to display AS opaque LSAs.
opaque-link	(Optional) Use **opaque-link** to display link opaque LSAs.
router	(Optional) Use **router** to display router LSAs.
self-originate	(Optional) Use **self-originate** to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled.
summary	(Optional) Use **summary** to show the LSA database summary information.
vrf *vrf-name*	(Optional) Specifies the virtual router for which to display information.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Router) #show ip ospf database

                        Router Link States (Area 0.0.0.100)

Link Id         Adv Router         Age     Sequence     Chksm   Options      Rtr Opt
--------------- ---------------    -----   ----------   -----   ----------   --------
192.168.1.10    192.168.1.10       1282    80000e14     feeb    -E----       -----
192.168.1.11    192.168.1.11       1273    800007f2     8186    -E----       -----
192.168.1.12    192.168.1.12       1782    80000df3     985d    -E----       -----
192.168.1.13    192.168.1.13       1335    80000c66     e197    -E----       -----
192.168.1.14    192.168.1.14       1278    80000c09     20ca    -E----       -----
192.168.1.15    192.168.1.15       1338    80000b41     f19e    -E----       -----
192.168.1.101   192.168.1.101      773     800009cc     8c99    -E----       -----
192.168.1.102   192.168.1.102      718     80000c24     c2e5    -E----       -----


                        Network Link States (Area 0.0.0.100)

Link Id         Adv Router         Age     Sequence     Chksm   Options      Rtr Opt
--------------- ---------------    -----   ----------   -----   ----------   --------
192.168.8.2     192.168.1.101      593     80000839     a8ec    -E----
192.168.8.6     192.168.1.102      538     800001fe     0ec2    -E----
192.168.8.66    192.168.1.14       1458    800001d1     acc5    -E----
192.168.8.70    192.168.1.15       1398    800001fd     3010    -E----
192.168.9.2     192.168.1.101      893     80000742     9cee    -E----
192.168.9.6     192.168.1.102      718     80000742     780d    -E----
192.168.9.66    192.168.1.14       1278    8000021b     1a0c    -E----
192.168.9.70    192.168.1.15       1338    800001fd     330b    -E----
192.168.10.2    192.168.1.101      773     80000862     5c0c    -E----
192.168.10.6    192.168.1.102      59      800001fe     14b8    -E----
192.168.10.66   192.168.1.14       1278    80000a3e     be3a    -E----
192.168.10.70   192.168.1.15       1038    800001d2     8cda    -E----
192.168.11.2    192.168.1.101      773     80000869     510e    -E----
192.168.11.6    192.168.1.102      1018    800001fd     19b2    -E----
192.168.11.66   192.168.1.14       1278    8000021a     2201    -E----
192.168.11.70   192.168.1.15       1338    800001fd     3901    -E----
```

Display Parameters

The information below is only displayed if OSPF is enabled.

For each link-type and area, the following information is displayed:

Link Id	Number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Adv Router	Advertising Router. Is a 32-bit dotted decimal number representing the LSDB interface.

Age	Number representing the age of the link state advertisement in seconds.
Sequence	Number that represents which LSA is more recent.
Checksum	Total number LSA checksum.
Options	This is an integer. It indicates that the LSA receives special handling during routing calculations.
Rtr Opt	Router Options are valid for router links only.

7-188 show ip ospf database database-summary

Display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database.

show ip ospf database database-summary

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Router)#show ip ospf database database-summary

OSPF Router with ID (192.168.1.14)

Area 0.0.0.100 database summary
Router.......................................... 8
Network......................................... 16
Summary Net..................................... 0
Summary ASBR.................................... 0
Type-7 Ext...................................... 0
  Self Originated Type-7........................ 0
Opaque Link..................................... 0
Opaque area..................................... 0
Subtotal........................................ 24

Router database summary
Router.......................................... 8
```

```
Network..................................... 16
Summary Net................................. 0
Summary ASBR................................ 0
Type-7 Ext.................................. 0
Opaque Link................................. 0
Opaque area................................. 0
Type-5 Ext.................................. 0
  Self-Originated Type-5 Ext................ 0
Opaque AS................................... 0
Total....................................... 24
```

Display Parameters

Router	Total number of router LSAs in the OSPF link state database.
Network	Total number of network LSAs in the OSPF link state database.
Summary Net	Total number of summary network LSAs in the database.
Summary ASBR	Number of summary ASBR LSAs in the database.
Type-7 Ext	Total number of Type-7 external LSAs in the database.
Self Originated Type-7	Total number of self originated AS external LSAs in the OSPF link state database.
Opaque Link	Number of opaque link LSAs in the database.
Opaque Area	Number of opaque area LSAs in the database.
Subtotal	Number of entries for the identified area.
Opaque AS	Number of opaque AS LSAs in the database.
Total	Number of entries for all areas.

7-189 show ip ospf interface

Display the information for the OSPF information for the specific interface.

show ip ospf interface {*slot/port* **| vlan** *vlan-id* **| loopback** *loopback-id* **| brief | stats}**

Parameters

slot/port	Enter an interface in slot/port format.
vlan *vlan-id*	Enter an interface in VLAN format.
loopback *loopback-id*	Display the configured Loopback interface information.
brief	Display snapshot of OSPF interfaces configured.
stats	Display OSPF interface statistical information.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command when the OSPF Admin Mode is disabled.

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

IP Address..................................... 0.0.0.0
Subnet Mask.................................... 0.0.0.0
Secondary IP Address(es)....................
OSPF Admin Mode................................ Disable
OSPF Area ID................................... 0.0.0.0
OSPF Network Type.............................. Broadcast
Router Priority................................ 1
Retransmit Interval............................ 5
Hello Interval................................. 10
Dead Interval.................................. 40
LSA Ack Interval............................... 1
Transmit Delay................................. 1
Authentication Type............................ None
Metric Cost.................................... 1 (computed)
Passive Status................................. Non-passive interface
OSPF Mtu-ignore................................ Disable
Flood Blocking................................. Disable

OSPF is not enabled on this interface.
```

Display Parameters

IP Address	IP address for the specified interface.
Subnet Mask	Mask of the network and host portion of the IP address for the OSPF interface.
Secondary IP Address(es)	Secondary IP addresses if any are configured on the interface.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	OSPF Area ID for the specified interface.
OSPF Network Type	Type of network on this interface that the OSPF is running on.
Router Priority	Number representing the OSPF Priority for the specified interface.
Retransmit Interval	Number representing the OSPF Retransmit Interval for the specified interface.
Hello Interval	Number representing the OSPF Hello Interval for the specified interface.

Dead Interval	Number representing the OSPF Dead Interval for the specified interface.
LSA Ack Interval	Number representing the OSPF LSA Acknowledgment Interval for the specified interface.
Transmit Delay	Number representing the OSPF Transmit Delay Interval for the specified interface.
Authentication Type	OSPF Authentication Type for the specified interface are: none, simple, and encrypt.
Metric Cost	Cost of the OSPF interface.
Passive Status	Shows whether the interface is passive or not.
OSPF MTU-ignore	Indicates whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.
Flood Blocking	Indicates whether flood blocking is enabled on the interface.

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

OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value broadcast. The OSPF interface Type will be 'broadcast'.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	Router ID representing the designated router.
Backup Designated Router	Router ID representing the backup designated router.
Number of Link Events	Number of link events.
Local Link LSAs	Number of Link Local Opaque LSAs in the link-state database.
Local Link LSA Checksum	Sum of LS Checksums of Link Local Opaque LSAs in the link-state database.
Prefix-suppression	Displays whether prefix-suppression is enabled, disabled, or unconfigured on the given interface.

7-190 show ip ospf interface brief

Display brief information for the IFO object or virtual interface tables for the specified virtual router. If no router is specified, it displays information for the default router.

show ip ospf interface brief [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display snapshot of OSPF interfaces configured of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Interface	*slot/port*
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	OSPF Area ID for the specified interface.
Router Priority	Number representing the OSPF Priority for the specified interface.
Cost	Metric cost of the OSPF interface.
Hello Interval	Number representing the OSPF Hello Interval for the specified interface.
Dead Interval	Number representing the OSPF Dead Interval for the specified interface.
Retransmit Interval	Number representing the OSPF Retransmit lnterval for the specified interface.
Interface Transmit Delay	Number representing the OSPF Transmit Delay for the specified interface.
LSA Ack Interval	Number representing the OSPF LSA Acknowledgment lnterval for the specified interface.

7-191 show ip ospf interface stats

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

show ip ospf interface stats {*slot/port* **| vlan** *vlan-id***}**

Parameters

slot/port	Enter an interface in slot/port format.
vlan *vlan-id*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing) #show ip ospf interface stats 0/49

OSPF Area ID..................................... 100
Area Border Router Count......................... 0
AS Border Router Count........................... 0
Area LSA Count................................... 24
IP Address....................................... 192.168.8.6
OSPF interface events............................ 2
Neighbor Events.................................. 6

Sent Packets..................................... 5913
Received Packets................................. 5904
Discards......................................... 0
Bad Version...................................... 0
Source Not On Local Subnet....................... 0
Virtual Link Not Found........................... 0
Area Mismatch.................................... 0
Invalid Destination Address...................... 0
Wrong Authentication Type........................ 0
Authentication Failure........................... 0
No Neighbor at Source Address.................... 0
Invalid OSPF Packet Type......................... 0
Hellos Ignored................................... 0

Packet Type                     Sent     Received
------------------------- ----------   ----------
Hello                           5231         5230
Database Description               3            3
LS Request                         1            0
LS Update                        300          259
LS Acknowledgement               378          412
```

Display Parameters

OSPF Area ID	Area ID of this OSPF interface.
Area Border Router Count	Total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
AS Border Router Count	Total number of Autonomous System border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IP Address	IP address associated with this OSPF interface.
OSPF Interface Events	Number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	Number of state changes or errors that occurred on this virtual link.

Neighbor Events	Number of times this neighbor relationship has changed state, or an error has occurred.
Sent Packets	Number of OSPF packets transmitted on the interface.
Received Packets	Number of valid OSPF packets received on the interface.
Discards	Number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	Number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Source Not On Local Subnet	Number of received packets discarded because the source IP address is not within a subnet configured on a local interface. **Note:** This field applies only to OSPFv2.
Virtual Link Not Found	Number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.
Area Mismatch	Number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	Number of OSPF packets discarded because the packets destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
Wrong Authentication Type	Number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface. **Note:** This field applies only to OSPFv2.
Authentication Failure	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender does not exist or the sender's address does not match the previously recorded IP address for that neighbor.
Invalid OSPF Packet Type	Number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	Number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Table 11 lists the number of OSPF packets of each type sent and received on the interface.

Table 11: Type of OSPF Packets Sent and Received on the Interface

Packet Type	Sent	Received
Hello	6960	6960
Database Description	3	3
LS Request	1	1

LS Update	141	42
LS Acknowledgment	40	135

7-192 show ip ospf lsa-group

Display the number of self-originated LSAs within each LSA group for the specified virtual router. If no router is specified, it displays information for the default router.

show ip ospf lsa-group [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display the LSA group information of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ip ospf lsa-group

Total self-originated LSAs: 5
Average LSAs per group: 0
Pacing group limit: 75
Number of self-originated LSAs within each LSA group...
Group Start Age           Group End Age        Count
--------------------    ---------------   ----------
              0                      59            0
             60                     119            0
            120                     179            1
            180                     239            0
            240                     299            2
            300                     359            0
            360                     419            0
            420                     479            0
            480                     539            0
            540                     599            1
            600                     659            0
            660                     719            0
```

720	779	0
780	839	0
840	899	0
900	959	0
960	1019	0
1020	1079	0
1080	1139	0
1140	1199	0
1200	1259	0
1260	1319	0
1320	1379	0
1380	1439	0
1440	1499	0
1500	1559	1
1560	1619	0
1620	1679	0
1680	1739	0
1740	1799	0
1800	1859	0
1860	1919	0

Display Parameters

Total self-originated LSAs	Number of LSAs the router is currently originating.
Average LSAs per group	Number of self-originated LSAs divided by the number of LSA groups. The number of LSA groups is the refresh interval (1800 seconds) divided by the pacing interval (configured with timers pacing lsa-group) plus two.
Pacing group limit	Maximum number of self-originated LSAs in one LSA group. If the number of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout the refresh interval to achieve better balance.
Groups	For each LSA pacing group, the output shows the range of LSA ages in the group and the number of LSAs in the group.

7-193 show ip ospf neighbor

Display information about OSPF neighbors for the specified virtual router. If no router is specified, it displays information for the default router. If you do not specify a neighbor IP address, the output displays summary information in a table. When an interface or tunnel is specified, only the information for that interface or tunnel is displayed if the interface is a physical routing interface and the interface VLAN format is a routing VLAN. When *ip-address* of the neighbor is specified, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

show ip ospf neighbor [vrf *vrf-name*]**[interface {***slot/port* **| vlan** *1-4093***}] [***ip-address***]**

Parameters

vrf *vrf-name*	(Optional) Display the VRF name which includes maximum 64 ASCII characters.
slot/port	(Optional) Enter an interface in slot/port format.
vlan	(Optional) Indicates an interface in VLAN format (1-4093).
ip-address	(Optional) Enter the neighbor's Router ID.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip ospf neighbor 170.1.1.50

Interface..................................... 0/17
Neighbor IP Address........................... 170.1.1.50
Interface Index............................... 17
Area Id....................................... 0.0.0.2
Options....................................... 0x2
Router Priority............................... 1
Dead timer due in (secs)...................... 15
Up Time....................................... 0 days 2 hrs 8 mins 46 secs
State......................................... Full/BACKUP-DR
Events........................................ 4
Retransmitted LSAs............................ 32
Retransmission Queue Length................... 0
Restart Helper Status......................... Helping
Restart Reason................................ Software Restart (1)
Remaining Grace Time.......................... 10 sec
Restart Helper Exit Reason.................... In Progress
```

Display Parameters

If you specify an IP address for the neighbor router, the following fields display.

Interface	*Indicates the slot/port ID.*
Neighbor IP Address	IP address of the neighbor router.
Interface Index	Interface ID of the neighbor router.
Area ID	Area ID of the OSPF area associated with the interface.
Options	Integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed

	in its Hello packets This enables received Hello Packets to be rejected if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of'0' indicates that the router is not eligible to become the designated router on this network.
Dead Timer Due	Amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Up Time	Neighbor uptime; how long since the adjacency last reached the Full state.
State	State of the neighboring routers.
Events	Number of times this neighbor relationship has changed state, or an error has occurred.
Retransmitted LSAs	Number of LSAs retransmitted to this neighbor.
Retransmission Queue Length	Integer representing the current length of the retransmission queue of the specified neighbor router ID of the specified interface.
Restart Helper Status	Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: • Helping – This router is acting as a helpful neighbor to this neighbor. A helpful neighbor does not report an adjacency change during graceful restart, but continues to advertise the restarting router as a FULL adjacency. A helpful neighbor continues to forward data packets to the restarting router. Trusting that the restarting router's forwarding table is maintained during the restart. • Not Helping – This router is not a helpful neighbor at this time.
Restart Reason	When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router: • Unknown (0) • Software restart (1) • Software reload/upgrade (2) • Switch to redundant control processor (3) • Unrecognized - a value not defined in RFC 3623 When D-LINK OS sends a grace LSA, it sets the Restart Reason to Software Restart on a planned warm restart (when the initiate failover command is invoked), and to Unknown on an unplanned warm restart.
Remaining Grace Time	Number of seconds remaining the in current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command.
Restart Helper Exit Reason	Indicates the reason that the specified router last exited a graceful restart. • None – Graceful restart has not been attempted • In Progress – Restart is in progress • Completed – Previous graceful restart completed successfully • Timed Out – Previous graceful restart timed out • Topology Changed – Previous graceful restart terminated prematurely because of a topology change

If an IP address is not specified, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify.

Router ID	4-digit dotted-decimal number of the neighbor router.
Priority	OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of'0' indicates that the router is not eligible to become the designated router on this network.
IP Address	IP address of the neighbor.
Interface	Physical routing interface or VLAN routing interface of the local router in slot/port format.
State	State of the neighboring routers. Possible values are: • Down – Initial state of the neighbor conversation; no recent information has been received from the neighbor. • Attempt – No recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. • Init – An Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. • 2 way – Communication between the two routers is bidirectional. • Exchange start – The first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number. • Exchange – The router is describing its entire link state database by sending Database Description packets to the neighbor. • Loading – Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • Full – The neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	Amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

7-194 show ip ospf range

Display the set of OSPFv2 area ranges configured for a given area for the specified virtual router. If no router is specified, it displays information for the default router.

show ip ospf range *areaid* **[vrf** *vrf-name***]**

Parameters

areaid	Identifies the area ID for the range.
vrf *vrf-name*	(Optional) Display OSPF area range information of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(R1)#show ip ospf range 0

       Prefix     Subnet Mask       Type          Action       Cost     Active
     10.1.0.0     255.255.0.0          S       Advertise       Auto          N
   172.20.0.0     255.255.0.0          S       Advertise        500          Y
```

Display Parameters

Prefix	Summary prefix.
Subnet Mask	Subnetwork mask of the summary prefix.
Type	**S** (Summary Link) or **E** (External Link).
Action	**Advertise** or **Suppress**.
Cost	Metric to be advertised when the range is active. If a static cost is not configured, the field displays **Auto**. If the action is **Suppress**, the field displays **N/A**.
Active	Indicate whether the range is currently active. **Y** or **N**.

7-195 show ip ospf statistics

Display information about recent Shortest Path First (SPF) calculations for the specified virtual router. If no router is specified, displays information for the default router. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the command shows statistics for how long ago the SPF ran, how long the SPF took, the reasons why the SPF was scheduled, the individual components of the routing table calculation time and to show the RIB update time. The most recent statistics are displayed at the end of the table.

show ip ospf statistics [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display the statistics of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Router)#show ip ospf statistics

Area 0.0.0.0: SPF algorithm executed 15 times
Delta T      Intra       Summ     Ext    SPF Total      RIB Update     Reason
00:05:33         0          0       0            0               0     R
00:05:30         0          0       0            0               0     R
00:05:19         0          0       0            0               0     N, SN
00:05:15         0         10       0           10               0     R, N, SN
00:05:11         0          0       0            0               0     R
00:04:50         0         60       0           60             460     R, N
00:04:46         0         90       0          100              60     R, N
00:04:42         0         70      10           90             160     R
00:03:39         0         70      40          120             240     X
00:03:36         0         60      60          130             160     X
00:01:28         0         60      50          130             240     X
00:01:25         0         30      50          110             310     SN
00:01:22         0          0      40           50             260     SN
00:01:19         0          0      20           20             190     X
00:01:16         0          0       0            0             110     R, X
```

Display Parameters

Delta T	Time since the routing table was computed. The time is in the format hours, minutes, and seconds (hh:mm:ss).
Intra	Time taken to compute intra-area routes, in milliseconds.
Summ	Time taken to compute inter-area routes, in milliseconds.
Ext	Time taken to compute external routes, in milliseconds.
SPF Total	Total time to compute routes, in milliseconds The total may exceed the sum of the lntra, Summ, and Ext times.
RIB Update	Time from the completion of the routing table calculation until all changes have been made in the common routing table [the Routing information Base (RIB)], in milliseconds.
Reason	Event or events that triggered the SPF: • R – new router LSA

	• N – new network LSA • SN – new network summary LSA • SA – new ASBR summary LSA • X – new external LSA

7-196 show ip ospf stub table

Display the OSPF stub table for the virtual router. If no router is specified, the information for the default router will be displayed. The information below will only be displayed if OSPF is initialized on the switch.

show ip ospf stub table [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display the statistics of a virtual router.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Area ID	32-bit identifier for the created stub area.
Type of Service	Type of service associated with the stub metric. D-LINK OS only supports Normal TOS.
Metric Val	Metric value is applied based on the TOS. lt defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

7-197 show ip ospf traffic

Display OSPFv2 packet and LSA statistics and OSPFv2 message queue statistics for the virtual router. If no router is specified, the information for the default router will be displayed. Packet statistics count packets and LSAs since OSPFv2 counters were last cleared (using the command "clear ip ospf counters").

show ip ospf traffic [vrf *vrf-name***]**

Parameters

vrf *vrf-name*	(Optional) Display the statistics of a virtual router.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip ospf traffic

Time Since Counters Cleared: 4000 seconds

OSPFv2 Packet Statistics

        Hello   Database Desc      LS Request       LS Update     LS ACK      Total
Recd:     500              10              20              50         20        600
Sent:     400               8              16              40         16        480

LSAs Retransmitted.............................. 0
LS Update Max Receive Rate...................... 20 pps
LS Update Max Send Rate......................... 10 pps

Number of LSAs Received

T1 (Router)..................................... 10
T2 (Network).................................... 0
T3 (Net Summary)................................ 300
T4 (ASBR Summary)............................... 15
T5 (External)................................... 20
T7 (NSSA External).............................. 0
T9 (Link Opaque)................................ 0
T10 (Area Opaque)............................... 0
T11 (AS Opaque)................................. 0
Total........................................... 345

OSPFv2 Queue Statistics

           Current        Max      Drops      Limit
Hello            0         10          0        500
ACK              2         12          0       1680
Data            24         47          0        500
Event            1          8          0       1000
```

Display Parameters

OSPFv2 Packet Statistics	Number of packets of each type sent and received since OSPF counters were last cleared.
LSAs Retransmitted	Number of LSAs retransmitted by this router since OSPF counters were last cleared.
LS Update Max Receive Rate	Maximum rate of LS Update packets received during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.
LS Update Max Send Rate	Maximum rate of LS Update packets transmitted during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.
Number of LSAs Received	Number of LSAs of each type received since OSPF counters were last cleared.
OSPFv2 Queue Statistics	For each OSPFv2 message queue, the current count, the high water mark, the number of packets that failed to be enqueued, and the queue limit. The high water marks are not cleared when OSPF counters are cleared.

7-198 show ip ospf virtual-link

Display the OSPF Virtual Interface information for a specific area and neighbor for the virtual router. If no router is specified, the information for the default router will be displayed. The *areaid* parameter identifies the area and the *neighbor* parameter identifies the neighbor's Router ID.

show ip ospf virtual-link [vrf *vrf-name***]** *areaid neighbor*

Parameters

vrf *vrf-name*	(Optional) Display the statistics of a virtual router.
areaid	Indicates the area ID.
neighbor	Enter the router ID of the virtual neighbor.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Area ID	Area ID of the requested OSPF area.
Neighbor Router ID	Input neighbor Router ID.

Hello Interval	Configured hello interval for the OSPF virtual interface.
Dead Interval	Configured dead interval for the OSPF virtual interface.
Interface Transmit Delay	Configured transmit delay for the OSPF virtual interface.
Retransmit Interval	Configured retransmit interval for the OSPF virtual interface.
Authentication Type	Configured authentication type of the OSPF virtual interface.
State	OSPF interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	Neighbor state.

7-199 show ip ospf virtual-link brief

Display the OSPF Virtual lnterface information for all areas in the system.

show ip ospf virtual-link brief

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Area ID	Area ID of the requested OSPF area.
Neighbor	Neighbor interface of the OSPF virtual interface.
Hello Interval	Configured hello interval for the OSPF virtual interface.
Dead Interval	Configured dead interval for the OSPF virtual interface.
Retransmit Interval	Configured retransmit interval for the OSPF virtual interface.
Transmit Delay	Configured transmit delay for the OSPF virtual interface.

ICMP Throttling Commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

7-200 ip unreachable

Enable the generation of ICMP Destination Unreachable messages on an interface or range of interfaces.

No command prevents the generation of ICMP Destination Unreachable messages.

ip unreachables

no ip unreachables

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

7-201 ip redirects

Enable the generation of ICMP Redirect messages by the router. You can use this command to configure an interface, a range of interfaces, or all interfaces.

No command prevents the generation of ICMP Redirect messages by the router.

ip redirects

no ip redirects

Parameters

None

Default

The default is Enabled.

Command Mode

- Global Config
- Interface Config
- Virtual Router Config

7-202 ipv6 redirects

Enable the generation of lCMPv6 Redirect messages by the router. You can use this command to configure an interface, a range of interfaces, or all interfaces.

No command prevents the generation of lCMPv6 Redirect messages by the router.

ipv6 redirects

no ipv6 redirects

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

7-203 ip icmp echo-reply

Enable the generation of ICMP Echo Reply messages by the router.

No command prevents the generation of ICMP Echo Reply messages by the router.

ip icmp echo-reply

no ip icmp echo-reply

Parameters

None

Default

The default is Enabled.

Command Mode

- Global Config
- Virtual Router Config

7-204 ip icmp error-interval

Limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. Burst-interval is from 0 to 2147483647 milliseconds (msec). The burst-size is the number of ICMP error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. To disable ICMP rate limiting, set burst-interval to zero (0).

Use the **no** command to return burst-interval and burst-size to their default values.

ip icmp error-interval *burst-interval* **[***burst-size***]**

no ip icmp error-interval

Parameters

burst-interval	Indicates the range for error interval in milliseconds (0-2147483647).
burst-size	(Optional) Indicates the burst size for ICMP rate limiting (1-200).

Default

The default is as follows:

- burst-interval of 1000 msec
- burst-size of 100 messages

Command Mode

- Global Config
- Virtual Router Config

Bidirectional Forwarding Detection Commands

Bidirectional Forwarding Detection (BFD) verifies bidirectional connectivity between forwarding engines, which can be a single or multi-hop away. The protocol works over any underlying transmission mechanism and protocol layer with a wide range of detection times, especially in scenarios where fast failure detection is required in data plane level for multiple concurrent sessions.

Use the following commands to configure Bidirectional Forwarding Detection commands (BFD).

7-205 bfd

Enable BFD on all interfaces associated with the OSPF process. BFD must be enabled on the individual interface to trigger BFD on that interface.

No command disables BFD globally on all interfaces associated with the OSPF process.

bfd

no bfd

Parameters

None

Default

The default is Disabled.

Command Mode

Router OSPF Config

Example

Do the following to trigger BFD processing through OSPF globally on all the interfaces that are associated with it.

```
(Router)(Config)#router ospf
(Router)(Config-router)#bfd
(Router)(Config-router)#exit
```

7-206 feature bfd

Enable BFD on the device. Note that BFD must be enabled in order to configure other protocol and interface parameters.

No command disables BFD globally and removes runtime session data. Static configurations are retained.

feature bfd

no feature bfd

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

Example

The following shows an example of the command.

```
(Router)#configure
(Router)(Config)#feature bfd
(Router)(Config)#exit
```

7-207 bfd echo

Enable BFD echo mode on an IP interface.

No command disables BFD echo mode on an IP interface.

bfd echo

no bfd echo

Parameters

None

Default

The default is Disable.

Command Mode

Interface Config

Example

The following shows an example of the command.

```
(Router)(Config)#interface 0/1
(Router)(Interface 0/1)#no bfd echo
(Router)(Interface 0/1)#exit
```

7-208 bfd interval

Configure the BFD session parameters for all available interfaces on the device (Global Config mode) or IP interface (Interface Config mode). It overwrites any BFD configurations present on individual interfaces (Global Config mode) or globally configured BFD session parameters (Interface Config).

No command in Global Config mode resets the BFD session parameters for all available interfaces on the device to their default values. In Interface Config mode, this command resets the BFD session parameters for all sessions on an IP interface to their default values.

bfd interval *transmit-interval* **min_rx** *minimum-receive-interval* **multiplier** *detection-time-multiplier*

no bfd interval

Parameters

transmit-interval	Desired minimum transmit interval, which is the minimum interval that the user wants to use while transmitting BFD control packets. It is represented in milliseconds. Its range is 40 ms to 1000 ms (with a change granularity of 100) a with default value of 100 ms.
minimum-receive-interval	Required minimum receive interval, which is the minimum interval at which the system can receive BFD control packets. It is represented in milliseconds. Its range is 40 ms to 1000 ms (with a change granularity of 100) with a default value of 100 ms.
detection-time-multiplier	Number of BFD control packets that must be missed in a row to declare a session down. Its range is 3 to 50 with default value of 3.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

Example

The following steps configure BFD session parameters on the device, in Privileged EXEC mode.

```
(Router)#configure
(Router)(Config)#bfd interval 100 min_rx 200 multiplier 5
(Router)(Config)#exit
```

The following steps configure BFD session parameters on an interface (for example, 0/1).

```
(Router)(Config)#interface 0/1
(Router)(Interface 0/1)#bfd interval 100 min_r-x 200 multiplier 5
(Router)(Interface 0/1)#exit
```

7-209 bfd slow-timer

Set up the required echo receive interval preference value. This value determines the interval the asynchronous sessions use for BFD control packets when echo function is enabled. The slow-timer value is used as the new control packet interval, while the echo packets use the configured BFD intervals.

No command resets the BFD slow-timer preference value to its default.

bfd slow-timer *echo-receive-interval*

no bfd slow-timer

Parameters

echo-receive-interval	Value is represented in milliseconds. Its range is 1000 ms to 30000 ms (with a change granularity of 100) with default value of 2000 ms.

Default

The default is 2000.

Command Mode

Global Config

Example

The following shows an example of the command.

```
(Router)#configure
(Router)(Config)#bfd slow-timer 10000
(Router)(Config)#exit
```

7-210 ip ospf bfd

Enable BFD on interfaces associated with the OSPF process.

No command disables BFD on interfaces associated with the OSPF process.

ip ospf bfd

no ip ospf bfd

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

7-211 neighbor fall-over bfd

Enable BFD support for fast failover for a BGP neighbor.

No command disables BFD support for fast failover for a BGP neighbor.

neighbor *ipaddress* **fall-over bfd**

no neighbor *ipaddress* **fall-over bfd**

Parameters

ipaddress	Enter the IP address (IPv4/IPv6) of the peer.

Default

The default is Disabled.

Command Mode

Router BGP Config

Example

Do the following to trigger BFD processing through BGP on an interface that is associated with it.

```
(Router)(Config)#router bgp [bgp ID]
(Router)(Config-router)#neighbor 172.16.11.6 fall-over bfd
(Router)(Config-router)#exit
```

7-212 show bfd neighbors

Display the BFD adjacency list showing the active BFD neighbors.

show bfd neighbors [details]

Parameters

details	(Optional) Provides additional details with the routing protocol BFD has registered and displays the Admin Mode status as Enabled or Disabled.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Router)#show bfd neighbors

Admin Mode: Enabled

OurAddr           NeighAddr          State   Interface    Uptime
---------------   ---------------    -----   ----------   ----------
192.168.20.1      192.168.20.2       Up      1/0/77       0:0:21:30
2601: :1          2001: :2           Up      1/0/78       0:0:0:18
```

```
(Router)#show bfd neighbors details

Admin Mode: Enabled

Our IP address..................................... 2.1.1.1
Neighbor IP address................................ 2.1.1.2
State.............................................. Up
Interface.......................................... 0/15
Uptime............................................. 0:0:0:10
Registered Protocol................................ BGP
Local Diag......................................... None
Demand mode........................................ FALSE
Minimum transmit interval.......................... 100
Minimum receive interval........................... 100
Actual tx interval................................. 100
Actual tx echo interval............................ 0
Detection interval multiplier...................... 3
```

```
My discriminator.............................. 1
Your discriminator............................ 1
Tx Count...................................... 105
Rx Count...................................... 107
Drop Count.................................... 0
```

Display Parameters

Our IP address	Current IP address.
Neighbor IP address	IP address of the active BFD neighbor.
State	Current state, either Up or Down.
Interface	Current interface.
Uptime	Amount of time the interface has been up.
Registered Protocol	Protocol from which the BFD session was initiated and that is registered to receive events from BFD. (for example, BGP).
Local Diag	Diagnostic state specifying the reason for the most recent change in the local session state.
Demand mode	Indicates if the system wishes to use Demand mode.
Minimum transmit interval	Minimum interval to use when transmitting BFD control packets.
Actual TX Interval	Transmitting interval being used for control packets.
Actual TX Echo interval	Transmitting interval being used for echo packets.
Minimum receive interval	Minimum interval at which the system can receive BFD control packets.
Detection interval multiplier	Number of BFD control packets that must be missed in a row to declare a session down.
My discriminator	Unique Session Identifier for Local BFD Session.
Your discriminator	Unique Session Identifier for Remote BFD Session.
Tx Count	Number of transmitted BFD packets.
Rx Count	Number of received BFD packets.
Drop Count	Number of dropped packets.

7-213 debug bfd event

Display BFD state transition information.

debug bfd event

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

7-214 debug bfd packet

Display BFD control packet debugging information.

debug bfd packet

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

---

8. IPv6 Routing Commands

Loopback Interface Commands

The commands described in this section are used to create, delete, and otherwise manage loopback interfaces. A loopback interface is expected to be up on a constant basis, provides the source address for sent packets, and can be used to receive both local and remote packets. Typically, a loopback interface is used by routing protocols.

Please see “ip address” for information on how to assign an IP address to the loopback interface.

8-1 interface loopback

Enters the interface Config mode for the loopback interface.

The **no** command removes the loopback interface and related configuration parameters for the given loopback interface.

interface loopback *0-63*

no interface loopback *0-63*

Parameters

None

Default

The default is None.

Command Mode

Global Config

8-2 show interface loopback

Displays information about the configured loopback interfaces.

show interface loopback [*loopback-id***]**

Parameters

loopback-id	(Optional) Indicates the configured Loopback interface information (0-63).

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show interface loopback

Loopback Id   Interface   IP Address
-----------  ----------- -----------------------------------
50            loopback 50  10.1.1.1
```

Display Parameters

If a loopback ID is not specified, the following information is shown for each loopback interface in the system.

Loopback ID	The loopback ID associated with the rest of the information in the row.
Interface	The interface name.
IP Address	The IPv4 address of the interface.

If a loopback ID is specified, the following information is shown.

Interface Link Status	Shows whether the link is up or down.
IP Address	The IPv4 address of the interface.
MTU size	The maximum transmission size for packets on this interface, in bytes.

Tunnel Interface Commands

The commands described in this section are used to create, delete, and manage tunnel interfaces. Functionality to facilitate the transition of IPv4 networks to IPv6 networks is provided by several different types of tunnels, which are divided into two classes, namely, configured and automatic tunnels. Configured tunnels are explicitly configured to have a specific destination or endpoint. In contrast, automatic tunnels infer the endpoint for the given tunnel from the destination address of the packets routed into the tunnel.

8-3 interface tunnel

Enters the Interface Config mode for a given tunnel interface.

The **no** command removes the specified tunnel interface and the associated configuration parameters for the given tunnel interface.

interface tunnel *0-7*

no interface tunnel *0-7*

Parameters

None

Default

The default is None.

Command Mode

Global Config

8-4 tunnel source

Specifies the source transport address for the tunnel, either by reference to an interface or explicitly.

tunnel source {*ipv4-address* **| ethernet** *slot/port* **|** *loopback* **|** *vlan***}**

Parameters

ipv4-address	Enter a valid IP address (IPv4).
ethernet *slot/port*	Configure the interface for IP tunnel.
loopback	Indicates the configured Loopback interface information (0-63).
vlan	Indicates the VLAN ID.

Default

The default is None.

Command Mode

Interface Tunnel Config

8-5 tunnel destination

Specifies the destination transport address for the tunnel.

tunnel destination {*ipv4-address***}**

Parameters

ipv4-address	Enter a valid IP address.

Default

The default is None.

Command Mode

Interface Config

8-6 tunnel mode ipv6ip

Specifies the mode of the tunnel. By using the optional 6to4 argument, the tunnel mode can be set to 6to4 automatic. If the optional 6to4 argument is not used, the tunnel mode is configured.

tunnel mode ipv6ip [6 to 4]

Parameters

6to4	Configure 6 to 4 tunnel mode.

Default

The default is None.

Command Mode

Interface Config

8-7 show interface tunnel

Displays the parameters related to the specified tunnel, such as the tunnel source address, tunnel mode, and tunnel destination address.

show interface tunnel [*tunnel-id***]**

Parameters

tunnel-id	(Optional) Indicates the tunnel interface information (0-7).

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Switch)(Interface tunnel 1)#show interface tunnel

Tunnel Id    Interface    TunnelMode   Source Address    Destination Address
```

```
----------   ----------   ----------   ---------------   --------------------
1            tunnel 1     6to4         192.168.1.1       192.168.2.1
```

Display Parameters

If a tunnel ID is not specified, the following information is shown for each configured tunnel:

Tunnel ID	The tunnel identification number.
Interface	The name of the tunnel interface.
Tunnel Mode	The tunnel mode.
Source Address	The source transport address of the tunnel.
Destination Address	The destination transport address of the tunnel.

lf a tunnel ID is specified, the following information is shown for the specified tunnel:

Interface Link Status	Shows whether the link is up or down.
MTU Size	The maximum transmission unit for packets on the interface.
IPv6 Address/Length	lf you enable IPv6 on the interface and assign an address, the IPv6 address and prefix display.

IPv6 Routing Commands

In this section, the IPv6 commands used to configure IPv6 on the system and on the interfaces are described. The IPv6 management commands and show commands are also described.

8-8 ipv6 hop-limit

Defines the unicast hop count utilized in ipv6 packets originated by the node. The same value is also indicated in router advertisements. The range of valid values for such hops is 1-255 inclusive. The “not configured” default results in a value of zero being sent in router advertisements and a value of 64 being sent in packets originated by the node. Note that use of the default value is not the same as configuring a value of 64.

The **no** command is used to return the unicast hop count to the default.

ipv6 hop-limit *1-255*

no ipv6 hop-limit

Parameters

None

Default

The default is as follows: not configured.

Command Mode

Global Config

8-9 ipv6 unicast-routing

Enables the forwarding of IPv6 unicast datagrams.

The **no** command disables the forwarding of IPv6 unicast datagrams.

ipv6 unicast-routing

no ipv6 unicast-routing

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

8-10 ipv6 enable

Enables IPv6 routing on a single interface or on a range of interfaces, including tunnel and loopback interfaces, that have not been configured with an explicit IPv6 address. When this command is used, the interface is configured automatically with a link-local address. It is not necessary to use this command if an IPv6 global address has been configured on the interface.

The **no** command disables IPv6 routing on an interface.

ipv6 enable

no ipv6 enable

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

8-11 ipv6 address

Configures an IPv6 address on a single interface or a range of interfaces, including tunnel and loopback interfaces, enables IPv6 processing on the interface or interfaces. Multiple globally reachable addresses can be assigned to an interface by using this command. It is not necessary to assign a link-local address by using this command because one is automatically created. The *prefix* field is made up of the bits of the address to be configured. The *prefix_length* field designates the number of high-order contiguous bits of the address that make up the prefix.

IPv6 addresses can be expressed in eight blocks, where instead of a period, a colon is now used to separate each block. For simplification, the leading zeros for each 16 bit block can be omitted. Relatedly, a single sequence of 16 bit blocks that contains only zeros can be replaced with a double colon, as in "::", but this cannot be done for more than one sequence at a time (as doing so would result in non-unique representations).

- Dropping zeros: **3ffe:ffff:100:f101 :0:0:0:1** becomes **3ffe:ffff:100:f101::1**
- Local host: **0000:0000:0000:0000:0000:0000:0000:0001** becomes **::1**
- Any host: **0000:0000:0000:0000:0000:0000:0000:0000** becomes **::**

The hexadecimal letters included in IPv6 addresses are not case-sensitive. One example of an IPv6 prefix and its prefix length is **3ffe:1::1234/64**.

The optional **[eui-64]** field is used to indicate that IPv6 processing on the interfaces was enabled by use of an EUI-64 interface ID in the low order 64 bits of the address. If this option is used, then the value of the *prefix_length* must be 64 bits.

The **no** command removes all of the IPv6 addresses on an interface or a specified IPv6 address. The *prefix* field is composed of the bits of the address to be configured. The *prefix_length* field is used to indicate the number of high-order contiguous bits of the address that comprise the prefix. The optional **[eui-64]** field is used to indicate that IPv6 processing on the interfaces was enabled by use of an EUI-64 interface ID in the low order 64 bits of the address.

If no parameters are supplied, then the command deletes all the IPv6 addresses on an interface.

ipv6 address *prefix/prefix_length* **[eui64]**

no ipv6 address [*prefix/prefix_length***] [eui64]**

Parameters

prefix/prefix_length	Enter the IPv6 prefix and prefix length.
eui64	(Optional) Use eui-64 Interface Identifier.

Default

The default is None.

Command Mode

Interface Config

8-12 ipv6 address autoconfig

Allows an in-band interface to obtain an IPv6 address through the IPv6 Neighbor Discovery Protocol (NDP) and by using Router Advertisement messages.

The **no** command sets the IPv6 autoconfiguration status of an interface to the default value.

ipv6 address autoconfig

no ipv6 address autoconfig

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

8-13 ipv6 address dhcp

Enables the DHCPv6 client on an in-band interface such that it can obtain network information, e.g., the IPv6 address, from a network DHCP server.

The **no** command releases a leased address and disables the DHCPv6 client on an interface.

ipv6 address dhcp

no ipv6 address dhcp

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

8-14 ipv6 route

This command configures an IPv6 static route. The *ipv6-prefix* field indicates the IPv6 network that is the destination for the static route. The *prefix_length* field indicates the length of the IPv6 prefix – this is indicated by a decimal value (usually 0-64) and shows the number of high-order contiguous bits of the address that comprise the prefix (i.e., the network portion of the address). A slash mark has to precede

the *prefix_length*. The *next-hop-address* field indicates the IPv6 address of the next hop that can be utilized to reach the specified network. Specifying **Null0** in the nexthop fields adds a static reject route. The *preference* field indicates the value the router uses to compare the given route with other routes from other route sources that have the same destination. The range of acceptable values for *preference* is 1-255, with the default value being 1. The *slot/port* argument corresponds to a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is used to directly specify the VLAN ID of the routing VLAN rather than by using a slot/port format. A *slot/ port* or **VLAN** *vlan-id* or **tunnel** *tunnel_id* interface can be specified in order to identify direct static routes from point-to-point and from broadcast interfaces. When using a link-local address as the next hop, the interface must be specified. A route with a preference of 255 cannot be used to forward traffic.

The **no** command deletes an lPv6 static route. If used without the optional parameters, it deletes all the static routes to the specified destination. If used with the preference parameter, it reverts the preference of a route to the default preference.

ipv6 route *ipv6-prefix/prefix_length* **{***next-hop-address* **| Null0 | interface {***slot/port* **| vlan** *vlan-id* **| tunnel** *tunnel_id***}** *next-hop-address***} [***preference***]**

no ipv6 route *ipv6-prefix/prefix_length* **[{***next-hop-address* **| Null0 | interface (***slot/port* **| vlan** *vlan-id* **| tunnel** *tunnel_id* **}** *next-hop-address* **|** *preference***}]**

Parameters

ipv6-prefix/prefix_length	Enter the IPv6 prefix and prefix length.
next-hop-address	Enter the Global IPv6 Address of Next-Hop.
Null0	Indicates the Null Interface.
slot/port	Indicates the slot or port to be identified.
vlan *vlan-id*	Indicates the VLAN ID.
tunnel *tunnel_id*	Indicates the IPv6 Tunnel ID.
Preference	Indicates the route preference (1-255).

Default

The default is Disabled.

Command Mode

Global Config

8-15 ipv6 route distance

Sets the default distance (i.e., preference) for IPv6 static routes. When determining the best route, lower route distance values are preferred. The **ipv6 route** command allows the user the option to set the distance (i.e., preference) for an individual static route. When no distance is specified in this command, the default distance is used.

Altering the default distance does not cause the distance of existing static routes to be updated, even if those routes were assigned the original default distance. Rather, the newly set default distance will only apply to those static routes created after invoking the **ipv6 route distance** command.

The **no** command resets the default static route preference value for the router to the original default preference. When determining the best route, lower route preference values are preferred.

ipv6 route distance *1-255*

no ipv6 route distance

Parameters

None

Default

The default is 1.

Command Mode

Global Config

8-16 ipv6 route net-prototype

Adds net prototype IPv6 routes to the hardware.

The **no** command deletes all the net prototype IPv6 routes that have been added to the hardware.

ip route net-prototype *prefix-/prefix-length nexthopip num-routes*

no ip route net-prototype *prefix-/prefix-length nexthopip num-routes*

Parameters

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.

Default

The default is None.

Command Mode

Global Config

8-17 ipv6 mtu

Sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets for a single interface or a range of interfaces. More specifically, using this command replaces the default or link MTU value with a new MTU value.

The **no** command resets the MTU value to the default value.

Note: For a tunnel interface, the default MTU value is 1480, and this value cannot be changed.

ipv6 mtu *1280-12270*

no ipv6 mtu

Parameters

None

Default

The default is 0 or the link speed, MTU value (1500).

Command Mode

Interface Config

8-18 ipv6 nd dad attempts

Sets the number of duplicate address detection probes that are transmitted on a single interface or a range of interfaces. Duplicate address detection confirms that a given IPv6 address on an interface is unique.

The **no** command reset the number of duplicate address detection probes to the default value.

ipv6 nd dad attempts *0-600*

no ipv6 nd dad attempts

Parameters

None

Default

The default is 1.

Command Mode

Interface Config

8-19 ipv6 nd managed-config-flag

Sets the “managed address configuration” flag used in router advertisements on a given interface or a range of interfaces. The end nodes use DHCPv6 when the value is set to true. In contrast, the end nodes automatically configure addresses when the value is set to false.

The **no** command resets the “managed address configuration” flag used in router advertisements to the default value.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameters

None

Default

The default is False.

Command Mode

Interface Config

8-20 ipv6 nd ns-interval

Sets the length of the interval, in milliseconds, between router advertisements for advertised neighbor solicitations. An advertised value of 0 indicates that the interval is not specified. This command can be used to configure a single interface or a range of interfaces.

The **no** command resets the length of the neighbor solicit retransmission interval for the specified interface to the default value.

ipv6 nd ns-interval {*1000-4294967295* **|** *0***}**

no ipv6 nd ns-interval

Parameters

None

Default

The default is 0.

Command Mode

Interface Config

8-21 ipv6 nd other-config-flag

Sets the “other stateful configuration” flag used in router advertisements sent from the given interface.

The **no** command resets the “other stateful configuration” flag used in router advertisements sent from the given interface back to its default value.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameters

None

Default

The default is False.

Command Mode

Interface Config

8-22 ipv6 nd ra-interval-max

Sets the length of the transmission interval between router advertisements on a given interface or a range of interfaces.

The **no** command sets the length of the router advertisement interval back to the default.

ipv6 nd ra-interval-max *4-1800*

no ipv6 nd ra-interval-max

Parameters

None

Default

The default is 600.

Command Mode

Interface Config

8-23 ipv6 nd raguard attach-policy

Enables the IPv6 RA Guard host mode on the configured interface. All router redirect packets and router advertisements received on the given interface will be dropped by the hardware

The **no** command disables the IPv6 RA Guard host mode on the interface.

ipv6 nd raguard attach-policy

no ipv6 nd raguard attach-policy

Parameters

None

Default

Non configured.

Command Mode

Interface Config

8-24 ipv6 nd ra-lifetime

Sets the value, in seconds, for the Router Lifetime field of the router advertisements sent from the given interface or a range of interfaces. The *lifetime* value must either be zero or an integer between the value for the router advertisement transmission interval and 9000. A value of zero indicates that the router in question is not to be used as the default router.

The **no** command resets the router lifetime value back to the default value.

ipv6 nd ra-lifetime *lifetime*

no ipv6 nd ra-lifetime

Parameters

lifetime	Indicates the router Advertisement Lifetime in seconds (0-9000).

Default

The default is 1800.

Command Mode

Interface Config

8-25 ipv6 nd ra hop-limit unspecified

Configures the router to transmit Router Advertisements on an interface with an unspecified (0) Current Hop Limit value. Doing so tells the hosts on that link to ignore the Hop Limit for the router in question.

The **no** command configures the router to send Router Advertisements on an interface using the global configured Hop Limit value.

ipv6 nd ra hop-limit unspecified

no ipv6 nd ra hop-limit unspecified

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

8-26 ipv6 nd reachable-time

Sets the amount of router advertisement time used to consider a neighbor reachable after neighbor discovery confirmation. The reachable time is specified in milliseconds, and a value of zero indicates that the time is not specified by the router. This command can be used to configure a single interface or a range of interfaces.

The **no** command indicates that the reachable time for the router is not specified.

ipv6 nd reachable-time *0-3600000*

no ipv6 nd reachable-time

Parameters

None

Default

The default is 0.

Command Mode

Interface Config

8-27 ipv6 nd router-preference

Configures the default router preference that the interface advertises in its router advertisement messages.

The **no** command resets the router preference that is advertised by the interface to the default value.

ipv6 nd router-preference {low | medium | high}

no ipv6 nd router-preference

Parameters

low	Indicates the low preference for Default Router use.
medium	Indicates the medium preference for Default Router use.
high	Indicates the high preference for Default Router use.

Default

The default is medium.

Command Mode

Interface Config

8-28 ipv6 nd suppress-ra

Suppresses router advertisement transmission on a single interface or a range of interfaces.

The **no** command enables router transmission on the given interface.

ipv6 nd suppress-ra [all]

no ipv6 nd suppress-ra

Parameters

all	(Optional) Select to suppress all transmission on the selected interface.

Default

The default is Disabled.

Command Mode

lnterface Config

8-29 ipv6 nd prefix

The ipv6 nd prefix command is used to configure the parameters associated with the prefixes that the router advertises in its router advertisements. The valid lifetime of the router, in seconds, is the first optional parameter. The user can specify a specific value or indicate that the lifetime value is infinite. The preferred lifetime of the router is the second optional parameter.

This command can be utilized to configure either a single interface or a range of interfaces.

A router uses its router advertisements (RAs) to advertise its global IPv6 prefixes. An RA includes only the prefixes of those IPv6 addresses configured on the interface to which the RA is transmitted. The IPv6 address interface configuration command is used to configure the addresses. Each prefix advertisement contains information regarding the prefix in question, such as the lifetime values of the prefix and whether hosts should utilize the prefix for on-link determination or address auto-configuration. The ipv6 nd prefix command is used to configure these values.

The ipv6 nd prefix command also allows the user to preconfigure RA prefix values before the user configures the associated interface address. ln order for a prefix to be included in the RAs, the user must configure an address that matches the prefix by utilizing the IPv6 address command. Any prefixes specified using the IPv6 nd prefix command without an associated interface address will not be contained in RAs or committed to the device configuration.

The **no** command sets the prefix configuration back to default values.

ipv6 nd prefix *prefix/prefix_length* **[{**<*lifetime*> *0-4294967295* **| infinite} {***0-4294967295* **| infinite}] [no-autoconfig off-link]**

no ipv6 nd prefix *prefix/prefix_length*

Parameters

prefix/prefix_length	Indicates the IPv6 prefix and prefix length.
lifetime	Valid lifetime value in seconds (0-4294967295).
infinite	(Optional) Infinite Valid Lifetime.
no-autoconfig off-link	(Optional) Do not use Prefix for autoconfiguration.
Off-link	Do not use Prefix for onlink determination.

Default

The default is as follows:

- valid-lifetime – 2592000
- preferred-lifetime – 604800
- autoconfig – enabled
- on-link – enabled

Command Mode

Interface Config

8-30 ipv6 neighbor

Configures the static IPv6 neighbor with the specified IPv6 address and MAC address on a host interface or routing interface.

The **no** command removes the static IPv6 neighbor with the specified IPv6 address from a host interface or routing interface.

ipv6 neigfior *ipv6address* **{***slot/port* **| vlan** *1-4093***}** *macaddr*

no ipv6 neigfior *ipv6address* **{***slot/port* **| vlan** *1-4093***}**

Parameters

ipv6address	The IPv6 address of the neighbor.

slot/port	The slot/port for the interface.
vlan *1-4093*	The VLAN for the interface.
macaddr	The MAC address for the neighbor.

Default

The default is None.

Command Mode

Global Config

8-31 ipv6 neighbors dynamicrenew

Automatically renews the IPv6 neighbor entries. Also, based on the activity of the neighbor entries in the hardware, this command enables/disables the periodic NUD (neighbor unreachability detection) to be run on the existing IPv6 neighbor entries. In the event that the setting is disabled, then only those entries that are actively used in the hardware will be triggered for NUD at the end of the STALE timeout of 1200 seconds. If, on the other hand, the setting is enabled, a set of 300 entries are triggered for NUD every 40 seconds, irrespective of their usage in the hardware.

The **no** command disables automatic renewing of the IPv6 neighbor entries.

ipv6 neighbors dynamicrenew

no ipv6 neighbors dynamicrenew

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

8-32 ipv6 nud

Configures Neighbor Unreachability Detection (NUD). NUD is used to verify that communication with a neighbor exists.

ipv6 nud {backoff-multiple | max-multicast-solicits | max-unicast-solicits}

Parameters

backoff-multiple	Sets the exponential backoff multiple to calculate time outs in NS transmissions during NUD. The value ranges from 1 to 5. 1 is the default. The next timeout value is limited to a maximum value of 60 seconds if the value with exponential backoff calculation is greater than 60 seconds.
max-multicast-solicits	Sets the maximum number of multicast solicits sent during Neighbor Unreachability Detection. The value ranges from 3 to 255. 3 is the default.
max-unicast-solicits	Sets the maximum number of unicast solicits sent during Neighbor Unreachability Detection. The value ranges from 3 to 10. 3 is the default.

Default

The default is None.

Command Mode

Global Config

8-33 ipv6 prefix-list

This command is used in the Global Configuration mode to create a prefix list or to add a prefix list entry. Prefix lists allow route prefixes to be matched with those specified in the prefix list, with each such list including a sequence of prefix list entries that are ordered by their sequence numbers. Each prefix list entry is sequentially examined by a router to determine if the route's prefix matches that of the given entry. A nonexistent or empty prefix list permits all prefixes. An implicit denial is assumed in the event that a given prefix does not match any of the entries in a prefix list. Once a match or denial occurs, the router does not continue examining the rest of the list.

A maximum of 128 prefix lists may be configured. In each prefix list, the maximum number of statements allowed is 64.

The **no** command deletes a given prefix list or a statement within a prefix list. More specifically, the command no ip prefix-list list-name deletes the entire prefix list in question. Meanwhile,, you must specify a statement exactly, with all its options, in order to remove that individual statement from a prefix list.

ip prefix-list *list-name* **([***seq number***] {permit | deny}** *ipv6-prefix/prefix-length* **[ge** *length***] [le** *length***] | renumber** *renumber-interval first-statement-number***}**

no ipv6 prefix-list *list-name* **[***seq number***] {permit | deny}** *ipv6-prefix/prefix-length* **[ge** *length***] [le** *length***]**

Parameters

list-name	The text name of the prefix list Up to 32 characters.
seq number	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured

	with the same sequence number. The value ranges from 1 to 4,294,967,294.
permit	Permit routes whose destination prefix matches the statement.
deny	Deny routes whose destination prefix matches the statement.
ipv6-prefix/prefix-length	Specifies the match criteria for routes being compared to the prefix list statement. The ipv6- prefix can be any valid IP prefix. The length is any IPv6 prefix length from 0 to 32.
ge *length*	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.
le *length*	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the ge length and less than or equal to 32.
renumber-interval first-statement-number	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for renumber-interval is 1-100, and the valid range for first-statement-number is 1-1000.

Default

The default is Prefix lists are not configured. When neither the **le** nor the **ge** option is configured, the destination prefix must match the network/length. If the **ge** option is configured but the **le** option is not, then any prefix with a network mask value greater than or equal to the **ge** value is considered a match. Similarly, if the **le** option is configured but the **ge** option is not, then any prefix with a network mask value less than or equal to the **le** value is considered a match.

Command Mode

Global Config

8-34 ipv6 unreachables

Enables the generation of ICMPv6 Destination Unreachable messages on a single interface or a range of interfaces. The generation of such messages is enabled by default.

The **no** command prevents the generation of ICMPv6 Destination Unreachable messages.

ipv6 unreachables

no ipv6 unreachables

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

8-35 ipv6 unresolved-traffic

Controls the rate at which IPv6 data packets are transmitted into the CPU, with rate limiting being disabled by default. When rate limiting is enabled, the rate allowed can range from 50 to 1024 packets per second.

The **no** command disables any rate limiting.

ipv6 unresolved-traffic rate-limit *50-1024*

no ipv6 unresolved-traffic rate-limit

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

8-36 ipv6 icmp error-interval

Limits the rate at which lCMPv6 error messages are transmitted. The rate limit is configured in the form of a token bucket that has two configurable parameters, namely, *burst-size* and *burst-interval*.

The *burst-interval* parameter specifies how frequently the token bucket is initialized with *burst-size* tokens. The acceptable range for the *burst-interval* is from 0 to 2147483647 milliseconds (msec).

The *burst-size* parameter specifies the number of lCMPv6 error messages that may be sent during a single *burst-interval*, with the allowable range being 1 to 200 messages.

Set the *burst-interval* to zero (0) to disable ICMP rate limiting.

The **no** command resets the burst-interval and burst-size parameters to their default values.

ipv6 icmp error-interval *burst-interval* **[***burst-size***]**

no ipv6 icmp error-interval

Parameters

burst-interval	Indicates the burst interval value (0-2147483647).
burst-size	(Optional) Indicates the burst-size for ICMP rate limiting (1-200).

Default

The default is as follows:

- burst-interval of 1000 msec.
- burst-size of 100 messages

Command Mode

Global Config

8-37 show ipv6 brief

Displays the IPv6 status of the forwarding mode and the IPv6 unicast routing mode.

show ipv6 brief

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 brief

IPv6 Unicast Routing Mode..................... Disable
IPv6 Hop Limit................................ 0
ICMPv6 Rate Limit Error Interval.............. 1000 msec
ICMPv6 Rate Limit Burst Size.................. 100 messages
Maximum Routes................................ 4096

IPv6 Unresolved Data Rate Limit............... 1024 pps
IPv6 Neighbors Dynamic Renew.................. Disable
IPv6 NUD Maximum Unicast Solicits............. 3
IPv6 NUD Maximum Multicast Solicits........... 3
IPv6 NUD Exponential Backoff Multiple......... 1
```

Display Parameters

IPv6 Unicast Routing Mode	Shows whether the IPv6 unicast routing mode is enabled.
IPv6 Hop Limit	Shows the unicast hop count used in IPv6 packets originated by the

	node. For more information, see "ipv6 hop-limit".
ICMPv6 Rate Limit Error Interval	Shows how often the token bucket is initialized with burst-size tokens. For more information, see "ipv6 icmp error-interval".
ICMPv6 Rate Limit Burst Size	Shows the number of ICMPv6 error messages that can be sent during one burst-interval. For more information, see "ipv6 icmp error-interval".
Maximum Routes	Shows the maximum IPv6 route table size.
IPv6 Unresolved Data Rate Limit	Shows the rate in packets-per-second for the number of IPv6 data packets trapped to CPU when the packet fails to be forwarded in the hardware due to unresolved hardware address of the destined IPv6 node.
IPv6 Neighbors Dynamic Renew	Shows the dynamic renewal mode for the periodic NUD (neighbor unreachability detection) run on the existing IPv6 neighbor entries based on the activity of the entries in the hardware.
IPv6 NUD Maximum Unicast Solicits	Shows the maximum number of unicast Neighbor Solicitations sent during NUD (neighbor unreachabililty detection) before switching to multicast Neighbor Solicitations.
IPv6 NUD Maximum Multicast Solicits	Shows the maximum number of multicast Neighbor Solicitations sent during NUD (neighbor unreachabililty detection) when in UNREACHABLE state.
IPv6 NUD Exponential Backoff Multiple	Shows the exponential backoff multiple to be used in the calculation of the next timeout value for Neighbor Solicitation transmission during NUD (neighbor unreachabililty detection) following the exponential backoff algorithm.

8-38 show ipv6 interface

Shows the usability status of the IPv6 interfaces and also whether the sending of ICMPv6 Destination Unreachable messages is allowed. The *slot /port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **vlan** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. Meanwhile, the keyword **loopback** directly specifies the loopback interface, whereas the keyword **tunnel** specifies the IPv6 tunnel interface.

show ipv6 interface {brief | *slot/port* **| vlan** *1-4093* **| loopback** *0-7* **| tunnel** *0-7***}**

Parameters

Brief	Display summary information about IPv6 configuration settings for all interfaces.
slot/port	Enter an interface in slot/port format.
vlan *1-4093*	Enter an interface in VLAN format.
loopback *0-7*	Display the configured Loopback interface information.
tunnel *0-7*	Display the configured Tunnel interface information.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 interface brief

Interface    Oper.Mode    IPv6 Address/Length
----------   ----------   ------------------------------
0/33         Enabled      FE80::211:88FF:FE2A:3E3C/128
                          2033::211:88FF:FE2A:3E3C/64
0/17         Enabled      FE80::211:88FF:FE2A:3E3C/128
                          2017::A42A:26DB:1049:43DD/128     [DHCP]
4/1          Enabled      FE80::211:88FF:FE2A:3E3C/128
                          2001::211:88FF:FE2A:3E3C/64       [AUTO]
4/2          Disabled     FE80::211:88FF:FE2A:3E3C/128      [TENT]
```

The following shows example CLI display output for the command.

```
(Switch)#show ipv6 interface 0/4/1

IPv6 is enabled
IPv6 Prefix is.................................. fe80::210:18ff:fe00:1105/128
.............................................. 2001::1/64
Routing Mode.................................... Enabled
IPv6 Enable Mode................................ Enabled
Administrative Mode............................. Enabled
IPv6 Operational Mode........................... Enabled
Bandwidth....................................... 10000 kbps
Interface Maximum Transmit Unit................. 1500
Router Duplicate Address Detection Transmits..... 1
Address DHCP Mode............................... Disabled
IPv6 Hop Limit Unspecified...................... Enabled
Router Advertisement NS Interval................ 0
Router Advertisement Lifetime................... 1800
Router Advertisement Reachable Time............. 0
Router Advertisement Interval................... 600
Router Advertisement Managed Config Flag........ Disabled
Router Advertisement Other Config Flag.......... Disabled
Router Advertisement Router Preference.......... medium
Router Advertisement Suppress Flag.............. Disabled
IPv6 Destination Unreachables................... Enabled
ICMPv6 Redirects................................ Enabled

Prefix 2001::1/64
Preferred Lifetime.............................. 604800
Valid Lifetime.................................. 2592600
Onlink Flag..................................... Enabled
```

```
Autonomous Flag.............................. Enabled
```

Display Parameters

If the **brief** parameter is used, then the following information is shown for all configured IPv6 interfaces:

Interface	The interface in *slot/port* format.
IPv6 Operational Mode	Shows whether the mode is enabled or disabled.
IPv6 Address/Length	Shows the IPv6 address and length on interfaces with IPv6 enabled.
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. Global addresses with no annotation are assumed to be manually configured.

lf an interface is specified, then the following information is also shown.

Routing Mode	Shows whether IPv6 routing is enabled or disabled.
IPv6 Enable Mode	Shows whether IPv6 is enabled on the interface.
Administrative Mode	Shows whether the interface administrative mode is enabled or disabled.
Bandwidth	Shows bandwidth of the interface.
Interface Maximum Transmission Unit	Indicates the MTU size in bytes.
Router Duplicate Address Detection Transmits	The number of consecutive duplicate address detection probes to transmit.
Address DHCP Mode	Shows whether the DHCPv6 client is enabled on the interface.
IPv6 Hop Limit Unspecified	Indicates if the router is configured on this interface to send Router Advertisements with unspecified (0) as the Current Hop Limit value.
Router Advertisement NS Interval	The interval, in milliseconds, between router advertisements for advertised neighbor solicitations.
Router Advertisement Lifetime	Shows the router lifetime value of the interface in router advertisements.
Router Advertisement Reachable Time	The amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	The frequency, in seconds, that router advertisements are sent.
Router Advertisement Managed Config Flag	Shows whether the managed configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Other Config Flag	Shows whether the other configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Router Preference	Shows the router preference.

Router Advertisement Suppress Flag	Shows whether router advertisements are suppressed (enabled) or sent (disabled).
IPv6 Destination Unreachables	Shows whether ICMPv6 Destination Unreachable messages may be sent (enabled) or not (disabled). For more information, see “ipv6 unreachables”.
ICMPv6 Redirect	Specifies if ICMPv6 redirect messages are sent back to the sender by the Router in the redirect scenario is enabled on this interface.

In the event that an IPv6 prefix is configured on the interface, the following information is also shown.

IPv6 Prefix is	The IPv6 prefix forthe specified interface.
Preferred Lifetime	The amount of time the advertised prefix is a preferred prefix.
Valid Lifetime	The amount of time the advertised prefix is valid.
Onlink Flag	Shows whether the onlink flag is set (enabled) in the prefix.
Autonomous Flag	Shows whether the autonomous address-configuration flag (autoconfig) is set (enabled) in the prefix.

8-39 show ipv6 dhcp interface

Displays a list of all the IPv6 addresses that are currently being leased from a DHCP server on a specific in-band interface. The *slot/port* argument corresponds to either a physical routing interface or a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ipv6 dhcp [interface *slot/port* **| vlan** *1-4093***]**

Parameters

slot/port	(Optional) Enter an interface in slot/port format.
vlan *1-4093*	(Optional) Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Mode	Displays whether the specified interface is in Client mode or not.
State	State of the DHCPv6 Client on this interface. The valid values are: INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND, RELEASE.

Server DUID	DHCPv6 Unique Identifier of the DHCPv6 Server on this interface.
T1 Time	The T1 time specified by the DHCPv6 server. After the client has held the address for this length of time, the client tries to renew the lease.
T2 Time	The T2 time specified by the DHCPv6 server. If the lease renewal fails, then when the client has held the lease for this length of time, the client sends a Rebind message to the server.
Interface IAID	An identifier for an identity association chosen by this client.
Leased Address	The IPv6 address leased by the DHCPv6 Server for this interface.
Preferred Lifetime	The preferred lifetime of the IPv6 address, as defined in RFC 2462.
Valid Lifetime	The valid lifetime of the IPv6 address, as defined by RFC 2462.
Renew Time	The time until the client tries to renew the lease.
Expiry Time	The time until the address expires.

8-40 show ipv6 nd raguard policy

Shows the status of the IPv6 RA GUARD feature on the switch. Using the command causes the ports/interfaces on which this feature is enabled, as well as the associated device role, to be listed.

show ipv6 nd raguard policy

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following constitutes an example of the command.

```
(Switching)#show ipv6 nd raguard policy

Configured Interfaces
Interface    Role
----------   ----------
Gi1/0/1      Host
```

Display Parameters

Interface	The port/interface on which this feature is enabled.

Role	The associated device role for the interface.

8-41 show ipv6 neighbors

Displays information regarding the IPv6 neighbors.

show ipv6 neighbor [interface {*slot/port* **| tunnel** *0-7* **| vlan** *1-4093***}]**

Parameters

slot/port	(Optional) Enter an interface in slot/port format.
tunnel *0-7*	(Optional) Indicates the configured Tunnel interface information (0-7).
vlan *1-4093*	(Optional) Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 neighbors

Count of Neighbors:............................. 3

IPv6 Address                MAC Address            State     Age       Intf.
--------------------------  -----------------      --------  --------  --------
FE80::222:BDFF:FED9:1D88    00:22:bd:d9:1d:88      Stale     194673    Vlan1
FE80::222:BDFF:FED9:1D89    00:22:bd:d9:1d:89      Stale     194721    Vlan1
FE80::222:BDFF:FED9:1D89    00:22:bd:d9:1d:89      Stale     194717    Vlan5
```

Display Parameters

Interface	The interface in slot/port format.
IPv6 Address	IPv6 address of neighbor or interface.
MAC Address	Link-layer Address.
IsRtr	Shows whether the neighbor is a router. If the value is TRUE, the neighbor is known to be a router, and FALSE otherwise. A value of FALSE might mean that routers are not always known to be routers.
Neighbor State	State of neighbor cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.

Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

8-42 clear ipv6 neighbors

Clears all entries in the IPv6 neighbor table or a specific entry on a specific interface. The *slot/port* parameter is used to specify an interface, while the *ipv6address* parameter is used to specify an IPV6 address or the **vlan** parameter is used to specify a VLAN.

clear ipv6 neighbors [{*slot/port* **|** *ipv6address* **| vlan** *id***}]**

Parameters

slot/port	(Optional) Indicates an interface in slot/port format.
ipv6address	(Optional) Indicates the IP address entry of a interface.
vlan *id*	(Optional) Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

8-43 show ipv6 protocols

Lists a summary of the configuration and status details for the active IPv6 routing protocols. Specifically, using the command causes the routing protocols that are configured and enabled to be listed. If a specific protocol is selected in the command line, then the information displayed is limited to that protocol.

show ipv6 protocols [bgp | ospf]

Parameters

bgp	Indicates BGP protocol only.
ospf	Indicates OSPFv3 protocol only.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Router)#show ipv6 protocols

Routing Protocol................................ BGP
BGP Router ID................................... 1.1.1.1
Local AS Number................................. 1
BGP Admin Mode.................................. Enable
Maximum Paths................................... Internal 1, External 1
Always compare MED.............................. FALSE
Maximum AS Path Length.......................... 75
Fast Internal Failover.......................... Enable
Fast External Failover.......................... Enable
Distance........................................ Ext 20, Int 200, Local 200

Prefixes Originated:
     2005::/64 (active)
     3012::/48

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

Routing Protocol................................ OSPFV3
Router ID....................................... 1.1.1.1
OSPF Admin Mode................................. Enable
Maximum Paths................................... 4
Distance........................................ Intra 110 Inter 110 Ext 110

Default Route Advertise......................... Disabled
Always.......................................... FALSE
Metric.......................................... Not configured
Metric Type..................................... External Type 2

Number of Active Areas.......................... 0 (0 normal, 0 stub, 0 nssa)
ABR Status...................................... Disable
ASBR Status..................................... Disable
```

Display Parameters

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, RIP, 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.
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.
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
OSPFV3 Section:	
Routing Protocol	OSPFv3.
Router ID	The router ID configured for OSPFv3.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.
Distance	The default administrative distance (or route preference) for intra-as, inter-as, and external OSPF 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.

8-44 show ipv6 route

Displays the IPv6 routing table The *ipv6-address* parameter is used to specify an IPv6 address for which the best-matching route will be displayed. The *ipv6-prefix/ipv6-prefix-length* parameter is used to specify an IPv6 network for which the matching route will be displayed. The *interface* parameter is used to specify that those routes with next-hops on the *interface* will be displayed. The *slot/port* argument corresponds to either a physical routing interface or a VLAN routing interface. The keyword **vlan** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. The optional *protocol* parameter is used to specify the protocol that installed the routes. The value for the *protocol* parameter must consist of one of the following keywords: **connected**, **ospf**, **static**. The optional **all** parameter is used to specify that all the routes, including the best and non-best routes, will be displayed. If it is not used, then only the best routes will be displayed.

Note: If the connected keyword is used for the protocol parameter, then the all option will not be available because there will be no best or non-best connected routes.

show ipv6 route [{*ipv6-address* **[***protocol***] | {{***ipv6-prefix/ipv6-prefix-length* **|** *slot/port* **| vlan** *1-4093***} [***protocol***] |** *protocol* **| summary} [all] | all}]**

Parameters

ipv6-address	Enter the IPv6 Address of the Route.
protocol	(Optional) Indicates the IPv6 routing protocol.
ipv6-prefix/ipv6-prefix-length	Enter the IPv6 prefix and prefix length.
slot/port	Enter an interface in slot/port format.
vlan *1-4093*	Enter an interface in VLAN format.
summary	Indicates the current state of the routing table.
all	(Optional) Indicates all (best and non-best) the routes.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 route

IPv6 Routing Table - 3 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
```

```
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
       P - Net Prototype
```

The following is an example of the CLI display output for the command indicating a truncated route.

```
(router)#show ipv6 route

IPv6 Routing Table - 2 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route
       O - OSPF Intra, OI — OSPF Inter, 0E1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, P - Net Prototype

C      2001:db9:1::/64 [0/0]
       via ::, 0/1
OI     3000::/64 [110/1]
       via fe80:: 200:e7ff:fe2e:ec3f,    00h:00m:11s, 0/1    T
```

The following is an example of the CLI display output for the command indicating kernel routes with the code K.

```
(router)#show ipv6 route

IPv6 Routing Table - 4 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
       P - Net Prototype

C      2009:1::/64 [0/0]
       via :: , 0/11
C      2044:1::/64 [0/0]
       via :: , 0/18
K      3001:33:3::/64 [1/0]
       via 2009:1::12,     00h:00m:25s, 0/11
K      5001:55:5::/64 [1/0]
       via 2044:1::14,     00h:00m:35s, 0/18
```

The following is an example of the CLI display output showing a hardware failure

```
(router)#
(router)#configure
(router)(ConFig)#interface 0/1
(router)(Interface 0/1)#routing
(router)(Interface 0/1)#ipv6 enable
(router)(Interface 0/1)#ipv6 address 2001::2/64
(router)(Interface 0/1)#exit
(router)(Config)#ipv6 route net-prototype 3601::/64 2001::4 1
```

```
(router)#show ipv6 route

IPV6 Routing Table - 1 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
       P - Net Prototype

C      2001::128 [0/0]
       Via ::, 0/1
P      3001::64 [0/1]
       via 2001::4,        00h:00m:04s, 0/1 hw-failure
```

Display Parameters

Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The show ipv6 route command is used to display the routing tables in the following format:

```
Codes: C - connected, S - static
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, Truncated, K - kernel
```

The columns for a given routing table show the following information:

Code	The code for the routing protocol that created this routing entry.
Default Gateway	The IPv6 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.
IPv6-Prefix/IPv6-Prefix-Length	The IPv6-Prefix and prefix-length of the destination IPv6 network corresponding to this route.
Preference/Metric	The administrative distance (preference) and cost (metric) associated with this route. An Example of this output is [1/0], where 1 is the preference and 0 is the metric.
Tag	The decimal value of the tag associated with a redistributed route, if it is not 0.
Next-Hop	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path 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.
T	A flag appended to an IPv6 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.

In order to control the traffic destined for a particular network administratively and prevent the traffic from being forwarded through a given router, a static reject route can be configured on the router. The traffic would then be discarded and an ICMP destination unreachable message would be sent back to the source. This approach is typically utilized to prevent routing loops. The reject route that is added in the recovery time object (RTO) will be **OSPF Inter-Area** types. Reject routes (REJECT route types installed by any protocol) are not redistributed by OSPF and are supported in both OSPFv2 and OSPFv3.

8-45 show ipv6 route ecmp groups

Reports all the current ECMP groups included in the IPv6 routing table, where an ECMP group consists of a set of two or more next hops that are used in one or more routes. Such groups are numbered in an arbitrary manner from 1 to n. The output for the command indicates both the number of next hops in the group as well as the number of routes that utilize the set of next hops. The output also includes the IPv6 address and the outgoing interface for each next hop in each group.

show ipv6 route ecmp-groups

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(router)#show ipv6 route ecmp-groups

ECMP Group 1 with 2 next hops (used by 1 route)
     2001:DB8:1::1 on interface 2/1
     2001:DB8:2::14 on interface 2/2

ECMP Group 2 with 3 next hops (used by 1 route)
     2001:DB8:4::15 on interface 2/32
     2001:DB8:7::12 on interface 2/33
     2001:DB8:9::45 on interface 2/34
```

8-46 show ipv6 route hw-failure

Displays the routes for which failure to be added to the hardware occurred due to hash errors or a table full condition.

show ipv6 route hw-failure

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the command output.

```
(Routing)#show ipv6 route connected

IPv6 Routing Table - 2 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
       P - Net Prototype

C      2001::/128 [0/0]
       via ::, 0/1
C      2005::/128 [0/0]
       via ::, 0/2

(Routing)#show ipv6 route hw-failure

IPv6 Routing Table - 4 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
       P - Net Prototype

P      3001:: /64 [0/1]
       via 2001::4,  00h:00m:04s, 0/1 hw-failure
P      3001:0:0:1::/64 [0/1]
       via 2001::4,  00h:00m:04s, 0/1 hw-failure
```

```
P      3001:0:0:2::/64 [0/1]
       via 2001::4,  00h:00m:04s, 0/1 hw-failure
P      3001:0:0:3::/64 [0/1]
       via 2001::4,  00h:00m:04s, 0/1 hw-failure
```

8-47 show ipv6 route net-prototype

Shows the net-prototype routes, which are displayed with a P.

show ipv6 route net-prototype

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following provides an example of the command.

```
(Routing)#show ipv6 route net-prototype

IPv6 Routing Table - 2 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
       P - Net Prototype

P      3001::/64 [0/1]
       via 2001::4,  00h:00m:04s, 0/1
P      3001:0:0:1::/64 [0/1]
       via 2001::4,  00h:00m:04s, 0/1
```

8-48 show ipv6 route preferences

Displays the preference value associated with the specified type of route, where lower numbers are given greater preference. Relatedly, a route with a preference value of 255 cannot be used to forward traffic.

show ipv6 route preferences

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following provides an example of the command.

```
(1b6m)#show route preferences

Local.......................................... 0
Static......................................... 1
OSPF Intra..................................... 110
OSPF Inter..................................... 110
OSPF External.................................. 110
BGP External................................... 20
BGP Internal................................... 200
BGP Local...................................... 200
```

Display Parameters

Local	Preference of directly-connected routes.
Static	Preference of static routes.
OSPF Intra	Preference of routes within the OSPF area.
OSPF Inter	Preference of routes to other OSPF routes that are outside of the area.
OSPF External	Preference of OSPF external routes.
BGP External	Preferepce of BGP external routes.
BGP Internal	Preference of routes to other BGP routes that are outside of the area.
BGP Local	Preference of routes within the BGP area.

8-49 show ipv6 route summary

Shows a summary of the routing table's current status. If the optional **all** keyword is used, then some statistics, such as the number of routes from each source, will also include counts for alternate routes. An alternate route consists of a route that is not the most preferred route to its own destination, such that it is not installed in the forwarding table. To be shown only the number of best routes, omit the optional keyword.

show ipv6 route summary [all]

Parameters

all	(Optional) Display all (best and non-best) routes.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 route summary

Connected Routes.............................. 4
Static Routes................................. 0
6To4 Routes................................... 0
BGP Routes.................................... 10
External...................................... 0
Internal...................................... 10
Local......................................... 0
OSPF Routes................................... 13
Intra Area Routes............................. 0
Inter Area Routes............................. 13
External Type-1 Routes........................ 0
External Type-2 Routes........................ 0
Reject Routes................................. 0
Net Prototype Routes.......................... 10004
Total routes.................................. 17

Best Routes (High............................. 17 (17)
Alternate Routes.............................. 0
Route Adds.................................... 44
Route Deletes................................. 27
Unresolved Route Adds......................... 0
Invalid Route Adds............................ 0
Failed Route Adds............................. 0
Hardware Failed Route Adds.................... 4
Reserved Locals............................... 0

Unique Next Hops (High)....................... 8 (8)
Next Hop Groups (High)........................ 8 (8)
ECMP Groups (High)............................ 3 (3)
ECMP Routes................................... 12
Truncated ECMP Routes......................... 0
ECMP Retries.................................. 0
Routes with 1 Next Hop........................ 5
Routes with 2 Next Hops....................... 1
```

```
Routes with 3 Next Hops..... 1
Routes with 4 Next Hops..... 10
Number of Prefixes:
     /64: 17
```

Display Parameters

Connected Routes	Total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
6To4	Total number of 6to4 routes in the routing table.
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 OSPFv3 protocol.
Intra Area Route	The type of route to a destination, intra-area route.
Inter Area Routes	The type of route to a destination, inter-area route.
External Type-1 Routes	The total number of external type-1 routes installed by OSPF protocol.
External Type-2 Routes	The 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 total number of net-prototype routes.
Number of Prefixes	Summarizes the number of routes with prefixes of different lengths.
Total Routes	The total number of routes in the routing table.
Best Routes	The number of best routes currently in the routing table. This number only counts the best route to each destination.
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 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 that failed to be inserted into the hardware due to a 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	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.
Unique Next Hops High	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.
ECMP Groups High	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.
Routes with n Next Hops	The current number of routes with each number of next hops.
Number of Prefixes	Summarizes the number of routes with prefixes of different lengths.

8-50 clear ipv6 route counters

Resets the IPv6 routing table counters that are reported in the command. More specifically, this command only resets those event counters that report the routing table's current state, while it does not reset counters such as the number of routes of each type.

clear ipv6 route counters

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

8-51 show ipv6 snooping counters

Shows the counters that are associated with IPv6 RA GUARD feature. The number of router redirect packets and router advertisements that are dropped by the switch globally due to RA GUARD feature are shown in the command output.

show ipv6 snooping counters

Parameters

None

Default

The default is None.

Command Mode

- Global Config
- Privileged EXEC

Example

The following provides an example of the command.

```
(Switching)#show ipv6 snooping counters

IPv6 Dropped Messages

RA(Router Advertisement ICMP type 134)

REDIR(Router Redirect - ICMP type 137)

RA      Redir
-----   --------
0       0
```

8-52 show ipv6 vlan

Shows the IPv6 VLAN routing interface addresses.

show ipv6 vlan

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ipv6 vlan

MAC Address used by Routing VLANs:   00:05:64:2F:0F:83

       Logical
VLAN ID      Interface       IPv6 Address/Prefix Length
----------   ----------      ------------------------------
1            Vlan1           fe80::205:64ff:fe2f:f83/64
                             2001:1::1/64
5            Vlan5           fe80::205:64ff:fe2f:f83/64
                             2001:5::1/64
10           Vlan10          fe80::205:64ff:fe2f:f83/64
                             2015:10::2/64
20           Vlan20          fe80::205:64ff:fe2f:f83/64
                             2015:20::2/64
30           Vlan30          fe80::205:64ff:fe2f:f83/64
                             2015:30::2/64
```

Display Parameters

MAC Address used by Routing VLANs	Shows the MAC address.

The remainder of the output for this command is shown in a table under the following column headings.

Column Headings	Definition
VLAN ID	The VLAN ID of a configured VLAN.
Logical Interface	The interface in slot/port format that is associated with the VLAN ID.
IPv6 Address/Prefix Length	The IPv6 prefix and prefix length associated with the VLAN ID.

8-53 show ipv6 traffic

Displays traffic and statistics for IPv6 and ICMPv6. A logical, loopback, or tunnel interface should be specified in the command. Doing so will allow the user to view information regarding the traffic on the specified interface. The *slot/port* argument corresponds to either a physical routing interface or a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. If an interface is not specified, the command will cause information about the traffic on all interfaces to be displayed.

show ipv6 traffic [{*slot/port* **| vlan** *1-4093* **| loopback** *loopback-id* **| tunnel** *tunnet-id***}]**

Parameters

slot/port	(Optional) Enter an interface in slot/port format.
vlan *1-4093*	(Optional) Enter an interface in VLAN format.
loopback *loopback-id*	(Optional) Display the configured Loopback interface information.
tunnel *tunnet-id*	(Optional) Configure IPv6 Tunnel.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Total Datagrams Received	Total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	Total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter increments at the interface to which these datagrams were addressed, which might not necessarily be the input interface for some of the datagrams.
Received Datagrams Discarded Due Header Errors	Number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.
Received Datagrams Discarded Due To MTU	Number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	Number of input datagrams discarded because no route could be found to transmit them to their destination.
Received Datagrams With Unknown Protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	Number of input datagrams discarded because the IPv6 address in their IPv6 Header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0) and unsupported addresses (for example, addresses with unallocated prefixes).
Received Datagrams Discarded Due To Truncated Data	Number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	Number of input IPv6 datagrams for which no problems were encountered to prevent their continue processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not

	include datagrams discarded while awaiting reassembly.
Received Datagrams Reassembly Required	Number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Successfully Reassembled	Number of IPv6 datagrams successfully reassembled. Note that this counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Failed To Reassemble	Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in by combining them as they are received. This counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Forwarded	Number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface increments.
Datagrams Locally Transmitted	Total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.
Datagrams Transmit Failed	Number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutFon/i/Datagrams if any such packets met this (discretionaiy) discard criterion.
Fragments Created	Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Datagrams Successfully Fragmented	Number of IPv6 datagrams that have been successfully fragmented at this output interface.
Datagrams Failed To Fragment	Number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
Multicast Datagrams Received	Number of multicast packets received by the interface.
Multicast Datagrams Transmitted	Number of multicast packets transmitted by the interface.
Total ICMPv6 messages received	Total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmplnErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
ICMPv6 Messages with errors	Number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
ICMPv6 Destination Unreachable Messages	Number of ICMP Destination Unreachable messages received by the interface.

lCMPv6 Messages Prohibited Administratively	Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
lCMPv6 Time Exceeded Messages	Number of ICMP Time Exceeded messages received by the interface.
lCMPv6 Parameter Problem Messages	Number of ICMP Parameter Problem messages received by the interface.
lCMPv6 messages with too big packets	Number of ICMP Packet Too Big messages received by the interface.
lCMPv6 Echo Request Messages Received	Number of ICMP Echo (request) messages received by the interface.
lCMPv6 Echo Reply Messages Received	Number of ICMP Echo Reply messages received by the interface.
lCMPv6 Router Solicit Messages Received	Number of ICMP Router Solicit messages received by the interface.
lCMPv6 Router Advertisement Messages Received	Number of lCMP Router Advertisement messages received by the interface.
lCMPv6 Neighbor Solicit Messages Received	Number of ICMP Neighbor Solicit messages received by the interface.
lCMPv6 Neighbor Advertisement Messages Received	Number of ICMP Neighbor Advertisement messages received by the interface.
lCMPv6 Redirect Messages Received	Number of Redirect messages received by the interface.
Transmitted	Number of lCMPv6 Group Membership Query messages received by the interface.
Total lCMPv6 Messages Transmitted	Total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
lCMPv6 Messages Not Transmitted Due To Error	Number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of lPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter‘s value.
lCMPv6 Destination Unreachable Messages Transmitted	Number of ICMP Destination Unreachable messages sent by the interface.
lCMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP destination unreachable/communication administratively prohibited messages sent.
lCMPv6 Time Exceeded Messages Transmitted	Number of ICMP Time Exceeded messages sent by the interface.
lCMPv6 Parameter Problem Messages Transmitted	Number of ICMP Parameter Problem messages sent by the interface.
lCMPv6 Packet Too Big Messages Transmitted	Number of ICMP Packet Too Big messages sent by the interface.

ICMPv6 Echo Request Messages Transmitted	Number of ICMP Echo (request) messages sent by the interface.lCMP echo messages sent.
ICMPv6 Echo Reply Messages Transmitted	Number of ICMP Echo Reply messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	Number of ICMP Router Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	Number of ICMP Router Advertisement messages sent by the interface.
ICMPv6 Neighbor Solicit Messages Transmitted	Number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	Number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Received	Number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
ICMPv6 Group Membership Query Messages Received	Number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Received	Number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Received	Number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	Number of duplicate addresses detected by the interface.

8-54 clear ipv6 snooping counters

Clears the counters that are associated with IPv6 RA GUARD feature.

clear ipv6 snooping counters

Parameters

None

Default

The default is None.

Command Mode

- Global Config
- Privileged EXEC

8-55 clear ipv6 statistics

Clears the IPv6 statistics for all the interfaces or for a specified interface, whether a loopback, tunnel, or VLAN interface. The IPv6 statistics are displayed in the output for the **show ipv6 traffic** command. If an interface is not specified, the counters for all the IPv6 traffic statistics will be reset to zero.

clear ipv6 statistics [{*slot/port* **| loopback** *loopback-id* **| tunnel** *tunnel-id* **| vlan** *id***}]**

Parameters

slot/port	(Optional) Enter an interface in slot/port format.
loopback *loopback-id*	(Optional) Clear the IPv6 statistics for the specified Loopback interface.
tunnel *tunnet-id*	(Optional) Clear the IPv6 statistics for the specified Tunnel interface.
vlan *id*	(Optional) Enter an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

OSPFv3 Commands

In this section, the commands used to configure OSPFv3, which is a link-state routing protocol that is used to route traffic within a network, are described. The following subsections are included in this section:

- "Global OSPFv3 Commands"
- "OSPFv3 Interface Commands"
- "OSPFV3 Graceful Restart Commands"

"OSPFv3 Stub Router Commands"

- OSPFv3 Show Commands"

Global OSPFv3 Commands

8-56 ipv6 router ospf

This command is used to enter the Router OSPFv3 Config mode.

Ipv6 router ospf

Parameters

None

Default

The default is None.

Command Mode

Global Config

8-57 area default-cost (OSPFv3)

Configures the monetary default cost for a stub area. The area ID and an integer value of from 1 to 16777215 must be specified.

area *areaid* **default-cost** *1-16777215*

Parameters

areaid	Indicates a valid area ID.

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-58 area nssa (OSPFv3)

Configures the area ID specified so that it will function as an NSSA.

The **no** command disables the NSSA function of the specified area ID.

area *areaid* **nssa**

no area *areaid* **nssa**

Parameters

areaid	Indicates a valid area ID.

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-59 area nssa default-info-originate (OSPFv3)

Configures the metric type and metric type for the default route advertised into the NSSA. The optional metric parameter is used to specify the metric value for the default route and must fall within the range of 1-16777214. If a metric value is not specified, the default value of 10 is used. The assigned metric type can either be comparable (nssa-external 1) or non-comparable (nssa-external 2).

The **no** command disables the default route advertised into the NSSA.

area *areaid* **nssa default-info-originate [***metric***] [{comparable | non-comparable}]**

no area *areaid* **nssa default-info-originate [***metric***] [{comparable | non-comparable}]**

Parameters

areaid	Indicates a valid area ID.
metric	(Optional) Indicates the metric value (1-16777214).
comparable	(Optional) Configure the Metric Type as comparable.
non-comparable	(Optional) Configure the Metric Type as non-comparable.

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-60 area nssa no-redistribute (OSPFv3)

Configures the NSSA ABR such that no redistribution of learned external routes to the NSSA will occur.

The **no** command disables the NSSAABR such that learned external routes are redistributed to the NSSA.

area *areaid* **nssa no-redistribute**

no area *areaid* **nssa no-redistribute**

Parameters

areaid	Indicates a valid area ID.

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-61 area nssa no-summary (OSPFv3)

Configures the NSSA such that summary LSAs will not be advertised into the NSSA.

The **no** command disables NSSA from the summary LSAs.

area *areaid* **nssa no-summary**

no area *areaid* **nssa no-summary**

Parameters

areaid	Indicates a valid area ID.

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-62 area nssa translator-role (OSPFv3)

Configures the translator role for the NSSA. Using a value of **always** will cause the router to assume the role of translator immediately if it becomes a border router, while using a value of **candidate** will cause the router to participate in the translator selection process if it becomes a border router.

The **no** command disables the NSSA translator role from the specified area ID.

area *areaid* **nssa translator-role {always | candidate}**

no area *areaid* **nssa translator-role {always | candidate}**

Parameters

areaid	Indicates a valid area ID.
always	Enter always for the translator role.
candidate	Enter candidate for the translator role.

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-63 area nssa translator-stab-intv (OSPFv3)

Configures the translator *stabilityinterval* parameter of the NSSA. The *stabilityinterval* parameter indicates the period of time for which a selected translator continues the performance of its duties after it has determined that its translator status has been taken over by another router.

The **no** command disables the NSSA translator's stabilityinterval from the specified area ID.

area *areaid* **nssa translator-stab-intv** *stabilityinterval*

no area *areaid* **nssa translator-stab-intv** *stabilityinterval*

Parameters

areaid	Indicates a valid area ID.
stabilityinterval	Indicates the integer for the Translator Stability interval. 0-3600

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-64 area range (OSPFv3)

Configures a summary prefix that an given area border router advertises for a specific area.

The **no** command deletes a summary prefix or removes a static cost.

area *area-id* **range** *prefix netmask* **{summarylink | nssaexternallink} [advertise | not-advertise] [cost** *cost***]**

no area *areaid* **range** *prefix netmask* **{summarylink | nssaexternallink} cost**

Parameters

area-id	The area identifier for the area whose networks are to be summarized.
prefix netmask	The summary prefix to be advertised when the ABR computes a route to one or more networks within this prefix in this area.
summarylink	When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.

nssaexternallink	When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	(Optional) When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.
not-advertise	(Optional) When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. When the not-advertise option is given, any static cost previously configured is removed from the system configuration.
cost *cost*	(Optional) If an optional cost is given, OSPF sets the metric field in the inter-area -prefix LSA to the configured value rather than setting the metric to the largest cost among the networks covered by the area range.

Default

The default is as follows: no area ranges or costs configured.

Command Mode

Router OSPFv3 Config

8-65 area stub (OSPFv3)

Creates a stub area for the area ID specified. The primary characteristic of a stub area is that AS External LSAs are not imported into the area. The removal of AS External LSAs and Summary LSAs can substantially reduce the link state database of the routers within the stub area.

The **no** command deletes a stub area for the area ID specified.

area *areaid* **stub**

no area *areaid* **stub**

Parameters

areaid	Indicates a valid area ID.

Default

The default is DHCP.

Command Mode

Router OSPFv3 Config

8-66 area stub no-summary (OSPFv3)

Disables the importation of Summary LSAs for the stub area specified by the *areaid*.

The **no** command sets the Summary LSA importation mode back to the default for the stub area specified by the *areaid*.

area *areaid* **stub no-summary**

no area *areaid* **stub no-summary**

Parameters

areaid	Indicates a valid area ID.

Default

The default is Enabled.

Command Mode

Router OSPFv3 Config

8-67 area virtual-link (OSPFv3)

Creates the OSPF virtual interface for the identified *areaid* and *neighbor* parameters. The *neighbor* parameter indicates the Router ID of the neighbor.

The **no** command deletes the OSPF virtual interface from the specified interface that is identified by the *areaid* and *neighbor* parameters.

area *areaid* **virtual-link** *neighbor*

no area *areaid* **virtual-link** *neighbor*

Parameters

areaid	Indicates a valid area ID.
neighbor	Indicates the router ID of the virtual neighbor.

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-68 area virtual-link dead-interval (OSPFv3)

Configures the dead interval for the OSPF virtual interface located on the virtual interface specified by the *areaid* and *neighbor* parameters. The *neighbor* parameter indicates the Router ID of the neighbor.

The **no** command configures the default dead interval for the OSPF virtual interface located on the virtual interface specified by the *areaid* and *neighbor* parameters.

area *areaid* **virtual-link** *neighbor* **dead-interval** *1-65535*

no area *areaid* **virtual-link** *neighbor* **dead-interval**

Parameters

areaid	Indicates a valid area ID.
neighbor	Indicates the router ID of the virtual neighbor.

Default

The default is 40.

Command Mode

Router OSPFv3 Config

8-69 area virtual-link hello-interval (OSPFv3)

Configures the hello interval for the OSPF virtual interface located on the virtual interface specified by the *areaid* and *neighbor* parameters. The *neighbor* parameter indicates the Router ID of the neighbor.

The **no** command configures the default hello interval for the OSPF virtual interface located on the virtual interface specified by the *areaid* and *neighbor* parameters.

area *areaid* **virtual-link** *neighbor* **hello-interval** *1-65535*

no area *areaid* **virtual-link** *neighbor* **hello-interval**

Parameters

areaid	Indicates a valid area ID.
neighbor	Indicates the router ID of the virtual neighbor.

Default

The default is 10.

Command Mode

Router OSPFv3 Config

8-70 area virtual-link retransmit-interval (OSPFv3)

Configures the retransmit interval for the OSPF virtual interface located on the virtual interface specified by the *areaid* and *neighbor* parameters. The *neighbor* parameter indicates the Router ID of the neighbor.

The **no** command configures the default retransmit interval for the OSPF virtual interface located on the virtual interface specified by the *areaid* and *neighbor* parameters.

area *areaid* **virtual-link** *neighbor* **retransmit-interval** *0-3600*

no area *areaid* **virtual-link** *neighbor* **retransmit-interval**

Parameters

areaid	Indicates a valid area ID.
neighbor	Indicates the router ID of the virtual neighbor.

Default

The default is 5.

Command Mode

Router OSPFv3 Config

8-71 area virtual-link transmit-delay (OSPFv3)

Configures the transmit delay for the OSPF virtual interface located on the virtual interface specified by the *areaid* and *neighbor* parameters. The *neighbor* parameter is the Router ID of the neighbor.

The **no** command configures the default transmit delay for the OSPF virtual interface located on the virtual interface specified by the *areaid* and *neighbor* parameters.

area *areaid* **virtual-link** *neighbor* **transmit-delay** *0-3600*

no area *areaid* **virtual-link** *neighbor* **transmit-delay**

Parameters

areaid	Indicates a valid area ID.
neighbor	Indicates the router ID of the virtual neighbor.

Default

The default is 1.

Command Mode

Router OSPFv3 Config

8-72 auto-cost reference-bandwidth (OSPFv3)

The OSPF computes, by default, the link cost of each interface from the interface bandwidth. Faster links will have lower metrics, which makes them better options in route selection. The configuration parameters for the **auto-cost reference bandwidth** and **bandwidth** commands give the user control over the default link cost. As such, the user can configure an interface bandwidth for the OSPF that is independent of the actual link speed. Another configuration parameter allows the user to control the ratio of the interface bandwidth to link cost. The link cost itself is calculated as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where the interface bandwidth is determined by the bandwidth command. Due to the default reference bandwidth being 100 Mbps, the OSPF uses the same default link cost for all of the interfaces with a bandwidth of 100 Mbps or greater. The **auto-cost** command can be used to change the reference bandwidth, with the reference bandwidth being specified in megabits per second (Mbps). The allowed range for the reference bandwidth is 1-4294967 Mbps.

The **no** command sets the reference bandwidth back to the default value.

auto-cost reference-bandwidth *1-4294967*

no auto-cost reference-bandwidth

Parameters

None

Default

The default is 100Mbps.

Command Mode

Router OSPFv3 Config

8-73 clear ipv6 ospf

The clear ipv6 OSPF command is used to clear routing, disables and enable OSPF.

clear ipv6 ospf

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

8-74 clear ipv6 ospf configuration

Resets the OSPF configuration back to the factory defaults.

clear ipv6 ospf configuration

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

8-75 clear ipv6 ospf counters

Resets the global and interface statistics.

clear ipv6 ospf counters

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

8-76 clear ipv6 ospf neighbor

Drops the adjacency with all OSPF neighbors. A one-way hello can be sent on each neighbor's interface. Once that is done, adjacencies can be reestablished. Specify the neighbor's Router ID using the optional parameter *neighbor-id* if you wish to drop all adjacencies with a specific router ID.

clear ipv6 ospf neighbor [*Ipaddr* **|** *neighbor-id***]**

Parameters

Ipaddr	Indicates the neighbor's Router ID.

neighbor-id	(Optional) Indicates the ID of the interface to restrict.

Default

The default is None.

Command Mode

Privileged EXEC

8-77 clear ipv6 ospf neighbor interface

Use the optional parameter [*slot/port*] to drop adjacency with all neighbors on a specific interface. The slot/port argument corresponds to either a physical routing interface or a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. The optional parameter [*neighbor-id*] is used to drop adjacency with a specific router ID on a specific interface.

clear ipv6 ospf neighbor interface [*slot/port* **| vlan** *1-4093***] [***neighbor-id***]**

Parameters

slot/port	(Optional) Indicates the interface in slot/port format.
vlan *1-4093*	(Optional) Indicates the interface in VLAN format.
neighbor-id	(Optional) Clears all OSPF counters for a specified neighbor.

Default

The default is None.

Command Mode

Privileged EXEC

8-78 clear ipv6 ospf redistribution

Flushes all self-originated external LSAs. The redistribution configuration can be reapplied and prefixes reoriginated as necessary.

clear ipv6 ospf redistribution

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

8-79 default-information originate (OSPFv3)

Controls the advertisement of default routes.

The **no** command resets the advertisement of default routes.

default-information originate [always] [metric *0-16777214***] [metric-type {1 | 2}]**

no default-information originate [metric] [metric-type]

Parameters

always	Indicates the default route is always advertised.
metric	Indicates the cost for reaching the rest of the world through this route (0-16777214).
metric-type {1 | 2}	Indicates how the cost of a neighbor metric is determined, default: type 2.

Default

The default is as follows:

- metric – unspecified
- type – 2

Command Mode

Router OSPFv3 Config

8-80 default-metric (OSPFv3)

Sets a default for the metric of distributed routes.

The **no** command resets a default for the metric of distributed routes.

default-metric *1-16777214*

no default-metric

Parameters

None

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-81 distance ospf (OSPFv3)

Sets the route preference value for the OSPF route types in the router. When determining the best route, lower route preference values are preferred. The OSPF route type can be intra, inter, or external. The external type routes are all given the same preference value. The allowed range of the *preference* value is 1 to 255.

The **no** command sets the default route preference value for the OSPF routes in the router. The OSPF route type can be intra, inter, or external. The external type routes are all given the same preference value.

distance ospf {intra-area *1-255* **| inter-area** *1-255* **| external** *1-255***}**

no distance ospf {intra-area | inter-area | external}

Parameters

intra-area	Indicates the distance for all routes within an area (1-255).
inter-area	Indicates the distance for all routes from one area to another area (1-255).
external	Indicates the distance for routes learned by redistribution from other routing domains (1-255).

Default

The default is 110.

Command Mode

Router OSPFv3 Config

8-82 enable (OSPFV3)

Resets the default administrative mode of the OSPF in the router to active.

The **no** command sets the administrative mode of the OSPF in the router to inactive.

enable

no enable

Parameters

None

Default

The default is Enabled.

Command Mode

Router OSPFv3 Config

8-83 exit-overflow-interval (OSPFV3)

Configures the exit overflow interval for the OSPF. Specifically, it indicates the number of seconds that a router will wait after entering the overflow state before attempting to exit the overflow state. This lets the router to originate non-defaultAS-external-LSAs again. When the value is set to 0, the router will not leave the overflow state until restarted.

The **no** command configures the default exit overflow interval for the OSPF.

exit-overflow-interval *0-2147483647*

no exit-overflow-interval

Parameters

None

Default

The default is 0 seconds.

Command Mode

Router OSPFv3 Config

8-84 external-lsdb-limit (OSPFv3)

Configures the external LSDB limit for the OSPF. If the value is set to -1, then there will be no limit. A router enters the overflow state when the number of non-default AS-external-LSAs in the router's link-state database reaches the external LSDB limit. The router will never hold more than the external LSDB limit of non-default AS-external-LSAs in its database. Please note that the external LSDB limit in all routers attached to the OSPF backbone and/or any regular OSPF area MUST be set identically.

The **no** command configures the default external LSDB limit for the OSPF.

external-lsdb limit *-1-2147483647*

no external-lsdb limit

Parameters

None

Default

The default is -1.

Command Mode

Router OSPFv3 Config

8-85 maximum-paths (OSPFv3)

Sets the number of paths that the OSPF can report for a specific destination where the *maxpaths* value is platform-dependent.

The **no** command resets the number of paths that the OSPF can report for a specific destination back to the default value.

maximum-paths *maxpaths*

no maximum-paths

Parameters

maxpaths	Indicates the maximum path value, 1 – 48.

Default

The default is 4.

Command Mode

Router OSPFv3 Config

8-86 passive-interface default (OSPFv3)

Enables the global passive mode by default for all interfaces. Using this command overrides any interface level passive mode. The OSPF will then not form adjacencies over a passive interface.

The **no** command disables the global passive mode by default for all interfaces. That is, any interface that was previously configured to be passive returns to the non-passive mode.

passive-interface default

no passive-interface default

Parameters

None

Default

The default is Disabled.

Command Mode

Router OSPFv3 Config

8-87 passive-interface (OSPFv3)

Sets the specified interface or tunnel to be passive. The slot/port argument corresponds to either a physical routing interface or a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. The command overrides the global passive mode that is currently in effect on the specified interface or tunnel.

The **no** command sets the specified interface or tunnel to be non-passive. The command overrides the global passive mode that is currently in effect on the specified interface or tunnel.

passive-interface {*slot/port* **| vlan** *1-4093* **| tunnel** *tunnel-id***}**

no enable password

Parameters

slot/port	Indicates the interface in slot/port format.
vlan *1-4093*	Indicates the VLAN number (1-4093).
tunnel *tunnel-id*	Indicates the tunnel interface.

Default

The default is Disabled.

Command Mode

Router OSPFv3 Config

8-88 redistribute (OSPFv3)

Configures the OSPFv3 protocol to allow for the redistribution of routes from the specified source protocol/routers. If the **bgp** keyword is used to redistribute BGP routes into the OSPFV3, then only the external BGP routes will be redistributed.

The **no** command configures the OSPF protocol to prohibit the redistribution of routes from the specified source protocol/routers.

redistribute {static | connected | bgp} [metric *0-16777214***] [metric-type {1 | 2}] [tag** *0-4294967295***]**

no no redistribute {static | connected | bgp} [metric] [metric-type] [tag]

Parameters

static	Indicates the redistribution of the static route.
connected	Indicates that connected routes will be redistributed.
bgp	Indicates that BGP4+ routes will be redistributed.
metric	(Optional) Indicates metric for redistributed routes (0-16777214).
metric-type {1 | 2}	(Optional) Indicates the type of metric used to meaure
tag *0-4294967295*	(Optional) Configures the OSPF route redistribution tag.

Default

The default is as follows:

- metric – unspecified
- type – 2
- tag – 0

Command Mode

Router OSPFv3 Config

8-89 router-id (OSPFv3)

Sets a 4-digit dotted-decimal number that uniquely identifies the router OSPF ID. The *ipaddress* parameter is a configured value.

router-id *ipaddress*

Parameters

ipaddress	Enter an IP Address.

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-90 timers pacing lsa-group

Adjusts how OSPFv3 groups LSAs for the purposes of a periodic refresh. OSPFv3 will refresh self-originated LSAs around once every 30 minutes. When OSPFv3 refreshes LSAs, it takes into consideration all self-originated LSAs with an age from 1800 to 1800 plus the pacing group size. Grouping the LSAs for a refresh allows OSPFv3 to combine the refreshed LSAs into a minimal number of LS Update packets, which makes LSA distribution more efficient.

When OSPFv3 originates a revised or new LSA, it will select a random refresh delay for that LSA. OSPFv3 then refreshes the LSA when the refresh delay expires. Through the selection of a random refresh delay, OSPFv3 avoids the need to refresh a large number of LSAs all at once, even in the event that a large number of LSAs are originated at one time.

The window in which LSAs are refreshed is measured in seconds, with the allowed range for the pacing group window being 10 to 1800 seconds.

The **no** command resets the LSA Group Pacing parameter back to the factory default value of 60 seconds.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameters

seconds	Set width of the window for grouping LSAs for refresh (10-1800).

Default

The default is 60 seconds.

Command Mode

Router OSPFv3 Config

8-91 timers throttle spf

The *spf-hold* value specifies the amount of delay for the initial “wait interval”. In the event that an SPF calculation is not scheduled within the current “wait interval”, then the next SPF calculation is scheduled at a delay defined by *spf-start*. If an SPF calculation has been scheduled within the current “wait interval”, then the “wait interval” is set to a value equal to two times the current “wait interval” until the “wait interval” hits the maximum time in milliseconds as specified by *spf-maximum*. Subsequent wait times will then remain at the maximum until such time as the values are reset or an LSA is received in between SPF calculations.

The **no** command resets the SPF throttling parameters back to the factory default values.

timers throttle spf *spf-start spf-hold spf-maximum*

no timers throttle spf

Parameters

spf-start	Indicates the SPF schedule delay in milliseconds when no SPF calculation has been scheduled during the current “wait interval”. Value range is 1 to 600000 milliseconds.

spf-hold	Indicates the initial SPF “wait interval” in milliseconds. Value range is 1 to 600000 milliseconds.
spf-maximum	Indicates the maximum SPF “wait interval" in milliseconds. Value range is 1 to 600000 milliseconds.

Default

The default is as follows:

- spf-start = 2000 ms
- spf-hold = 5000 ms
- spf-maximum = 5000 ms

Command Mode

Privileged EXEC

8-92 trapflags (OSPFv3)

Enables individual OSPF traps, enables a group of trap flags simultaneously, or enables all the trap flags simultaneously. The different groups of trapflags, and each one of a group’s specific trapflags that are to be enabled or disabled, are listed in Table 12.

Table 12: Trapflag Groups (OSPFv3)

Group	Flags
Errors	• authentication-failure • bad-packet • config-error • virt-authentication-failure • virt-bad-packet • virt-config-error
lsa	• lsa-maxage • lsa-originate
overflow	• lsdb-overflow • lsdb-approaching-overflow
retransmit	• packets • virt-packets
state-change	• if state-change • neighbor-state-change • virtif-state-change • virtneighbor-state-change

- To enable an individual flag, enter the group name followed by the name of that particular flag.
- To enable all of the flags in a group, enter the group name followed by **all**.
- To enable all of the flags, enter the command as **trapflags all**.

The **no** command resets to the default reference bandwidth.

- To disable an individual flag, enter the group name followed by the name of that particular flag.
- To disable all of the flags in a group, enter the group name followed by **all**.
- To disable all of the flags, enter the command as **trapflags all**.

trapflags {all I errors {all | authentication-failure | bad-packet | config-error | virt-authentication-failure | virt-bad-packet | virt-config-error} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-approaching-overflow | lsdb-overflow } | retransmit {all | packets | virt-packets} | state-change {all | if-state-change | neighbor-state-change | virtif-state-change | virtneighbor-state-change}}

no trapflags {all I errors [all | authentication-failure | bad-packet | config-error | virt-authentication-failure | virt-bad-packet | virt-config-error] | lsa [all | lsa-maxage | lsa-originate] | overflow [all | lsdb-approaching-overflow | lsdb-overflow]} | retransmit [all | packets | virt-packets] | state-change [all | if-state-change | neighbor-state-change | virtif-state-change | virtneighbor-state-change]}

Parameters

all	Enable/Disable all Traps.
errors	Enable/Disable OSPF Trap errors.
authentication-failure	Authentication failure on non virtual interfaces.
bad-packet	Packet parse failure on non virtual interfaces.
config-error	Config mismatch errors on non virtual interfaces.
virt-authentication-failure	Authentication failure on virtual interfaces.
virt-bad-packet	Packet parse failure on virtual interfaces.
virt-config-error	Config mismatch errors on virtual interfaces.
lsa	Enable/Disable LSA related traps.
lsa-maxage	This trap signifies that one of the LSA in the router's link-state database has aged to MaxAge. The factory default is disabled.
lsa-originate	This trap signifies that a new LSA has been originated by this device.
overflow	Enable/Disable Overflow traps.
lsdb-approaching-overflow	This trap signifies that the number of LSAs in the router's link-state database has exceeded ninety percent of OSPF External LSDB Limit.
lsdb-overflow	This trap signifies that the number of LSAs in the router's link-state database has exceeded OSPF External LSDB Limit. The factory default is disabled.
retransmit	Enable/Disable packet retransmit traps.
packets	This trap signifies that an OSPF packet has been retransmitted on a non-virtual interface. All packets that may be retransmitted are associated with an LSDB entry.
virt-packets	This trap signifies that an OSPF packet has been retransmitted on a virtual interface. All packets that may be retransmitted are associated with an LSDB entry
state-change	Enable/Disable state change traps.

if-state-change	This trap signifies that there has been a change in the state of a non-virtual OSPF interface.
neighbor-state-change	This trap signifies that there has been a change in the state of a nonvirtual OSPF neighbor.
virtif-state-change	This trap signifies that there has been a change in the state of an OSPF virtual interface.
virtneighbor-state-change	This trap signifies that there has been a change in the state of an OSPF virtual neighbor.

Default

The default is Disabled.

Command Mode

Router OSPFv3 Config

OSPFv3 Interface Commands

8-93 ipv6 ospf area

Sets the OSPF area that the specified router interface or range of interfaces belongs to. The command also enables the OSPF for the specified router interface or range of interfaces. The area must consist of a 32-bit integer that is formatted as a 4-digit dotted-decimal number or as a decimal value within the range of 0-4294967295. The area identifies uniquely the area to which the interface will connect. If an area ID is assigned for an area that does not exist yet, then the area will be created with default values.

ipv6 ospf area *0-4294967295*

Parameters

None

Default

The default is None.

Command Mode

Interface Config

8-94 ipv6 ospf cost

Configures the cost on a specific OSPF interface or range of interfaces.

The **no** command resets the cost on an OSPF interface to the default.

ipv6 ospf cost *1-65535*

no ipv6 ospf cost

Parameters

None

Default

The default is 10.

Command Mode

Interface Config

8-95 ipv6 ospf dead-interval

Sets the OSPF dead interval used for the specified interface or range of interfaces, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value of this interval must be a valid positive integer and must be the same for all the routers that are attached to a common network. The value should also be some multiple of the Hello interval (i.e., 4).

The **no** command resets the OSPF dead interval for the specified interface or range of interfaces back to the default value.

ipv6 ospf dead-interval *1-2147483647*

no ipv6 ospf dead-interval

Parameters

None

Default

The default is 40.

Command Mode

Interface Config

8-96 ipv6 ospf hello-interval

Sets the OSPF hello interval, which represents the length of time in seconds, for the given interface. The value must be a valid positive integer and must be the same for all the routers that are to a network.

The **no** command resets the OSPF hello interval for the specified interface back to the default value.

ipv6 ospf hello-interval *1-65535*

no ipv6 ospf hello-interval

Parameters

None

Default

The default is 10.

Command Mode

Interface Config

8-97 ipv6 ospf link-lsa-suppression

Enables Link LSA Suppression on a given interface. No Link LSA protocol packets are originated (transmitted) on a point-to-point (P2P) interface when Link LSA Suppression is enabled on the interface. This configuration does not apply, meanwhile, to non-P2P interfaces.

The **no** command resets the Link LSA Suppression for the interface to disabled. If the Link LSA Suppression is disabled, then Link LSA protocol packets will be originated (transmitted) on the P2P interface.

ipv6 ospf link-lsa- suppression

no ipv6 ospf link-lsa- suppression

Parameters

None

Default

The default is False.

Command Mode

Privileged EXEC

8-98 ipv6 ospf mtu-ignore

Disables OSPF maximum transmission unit (MTU) mismatch detection on a specified interface or a range of interfaces. OSPF Database Description packets are used to specify the size of the largest IP packet that is allowed to be sent without fragmentation on the interface. When a Database Description packet is received by a router, the router examines the MTU advertised by the neighbor. If the MTU is larger than the router is allowed to accept, then by default, the Database Description packet will be rejected and OSPF adjacency will not be established.

The **no** command enables OSPF MTU mismatch detection.

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Parameters

None

Default

The default is Enabled.

Command Mode

Interface Config

8-99 ipv6 ospf network

Changes the default OSPF network type for a specific interface or a range of interfaces. The network type is normally determined according to the physical IP network type, and all Ethernet networks are, by default, OSPF type broadcast. Similarly, the default type for tunnel interfaces is point-to-point. When an Ethernet port is utilized as a single large bandwidth IP network in between two routers, then the network type may be point-to-point since only two routers are invlovled. The use of point-to-point as the network type eliminates the overhead of the OSPF designated router selection. It is not useful under normal circumstances to set a tunnel to OSPF network type broadcast.

The **no** command resets the interface type back to the default value.

ipv6 ospf network {broadcast | point-to-point}

no ipv6 ospf network {broadcast | point-to-point}

Parameters

broadcast	Set OSPFv3 Interface Type to Broadcast.
point-to-point	Set OSPFv3 Interfcae Type to Point to Point.

Default

The default is Broadcast.

Command Mode

Interface Config

8-100 ipv6 ospf prefix-suppression

Suppresses the advertisement of those IPv6 prefixes that are associated with a given interface, with the exception of those associated with secondary IPv6 addresses. Use of this command takes precedence over the global configuration. If the configuration is not specified, however, then the global prefix-suppression configuration applies.

By using the disable option, prefix-suppression can be disabled at the interface level. This option is useful if the user wants to exclude specific interfaces from performing prefix-suppression in the event that the feature is enabled globally.

Please note that using the disable option is not the same as not configuring the interface specific prefix-suppression. In the event that prefix-suppression is not configured at the interface level, then the global prefix-suppression configuration will be applicable for the IPv6 prefixes associated with the interface.

The **no** command removes any prefix-suppression configurations at the interface level. In other words, if the no ipv6 ospf prefix-suppression command is utilized, then global prefix-suppression applies to the interface. Please note that not configuring the command is not the same as disabling interface level prefix-suppression.

ipv6 ospf prefix-suppression [disable]

no ipv6 ospf prefix-suppression

Parameters

disable	(Optional) Disable prefix-suppression on the interface.

Default

Not configured.

Command Mode

Interface Config

8-101 ipv6 ospf priority

Sets the OSPF priority for a specific router interface or a range of interfaces. The priority for the interface must be a priority integer from 0 to 255, where a value of 0 means that the router is not allowed to become the designated router for the network in question.

The **no** command resets the OSPF priority for the specified router interface to the default.

ipv6 ospf priority *0-255*

no ipv6 ospf priority

Parameters

None

Default

The default is 1 (highest router priority value).

Command Mode

Interface Config

8-102 ipv6 ospf retransmit-interval

Sets the OSPF retransmit interval, which is specified in seconds, for the given interface or a range of interfaces. The value indicates the number of seconds between retransmissions of link-state advertisement for adjacencies belonging to the given router interface. The value is likewise used when retransmitting database description and link-state request packets.

The **no** command resets the OSPF retransmit interval for the specified interface to the default value.

ipv6 ospf retransmit-interval *0-3600*

no ipv6 ospf retransmit-interval

Parameters

None

Default

The default is 5 seconds.

Command Mode

Interface Config

8-103 ipv6 ospf transmit-delay

Sets the OSPF Transit Delay, which is specified in seconds, for the specified interface or a range of interfaces. In addition, this command sets the estimated number of seconds that it takes to transmit a link state update packet over the given interface.

The **no** command resets the OSPF Transit Delay for the specified interface to the default value.

ipv6 ospf transmit-delay *0-3600*

no ipv6 ospf transmit-delay

Parameters

None

Default

The default is 1 second.

Command Mode

Interface Config

OSPFV3 Graceful Restart Commands

The OSPFv3 protocol can be configured so that it participates in the checkpointing service, such that the protocol can execute a “graceful restart” if the management unit fails. In a graceful restart, the hardware will continue forwarding IPv6 packets by using OSPFv3 routes at the same time that a backup switch takes over management unit responsibility.

A graceful restart utilizes the concept of “helpful neighbors“. When a fully adjacent router receives a link state announcement (LSA) from the restarting management unit that indicates its intention to perform a graceful restart, the adjacent router enters helper mode. When in helper mode, a switch continues to advertise to the rest of the network that those other network members still have full adjacencies with the router that is restarting, thus avoiding the announcement of a topology change and the possibility of a flood of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue the forwarding of packets through the restarting router as it restarts. The restarting router then relearns the network topology from those helpful neighbors.

Graceful restarts may be enabled either for planned starts, unplanned restarts, or both. The operator initiates a planned restart through the management command **initiate failover**. A failover may be intiated in order to take the management unit out of service (for example, in order to fix a partial hardware failure), to address faulty system behavior that cannot be corrected via less severe management actions, or for other reasons. An unplanned restart consists of an unexpected failover resulting from a fatal hardware failure of the management unit or from a software hang or crash on the management unit.

8-104 nsf (OSPFv3)

Enables the OSPF graceful restart functionality on a given interface.

The **no** command disables graceful restart for all restarts.

nsf {ietf [helper] | helper [disable | planned-only | strict-lsa-checking]

no nsf

Parameters

helper	Configure grafeul restart helpful neighbor.
ietf	(Optional) This keyword is accepted but not required.
disable	Disable helpful neighbor support.
planned-only	(Optional) This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).
strict-lsa-checking	Terminate graceful restart helper mode on topology change.

Default

The default is Disabled.

Command Mode

Router OSPFv3 Config

8-105 nsf helper (OSPFv3)

Enables helpful neighbor functionality for the OSPF protocol. This functionality can be enabled for planned restarts, unplanned restarts, or both.

The **no** command disables helpful neighbor functionality for OSPF.

nsf helper [planned-only]

no nsf helper

Parameters

planned-only	(Optional) This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

Default

The default is as follows: OSPF acts as a helpful neighbor in both planned and unplanned restarts.

Command Mode

Router OSPFv3 Config

8-106 nsf ietf helper disable (OSPFv3)

Disables the helpful neighbor functionality for the OSPF.

Note: The following commands are functionally equivalent: **no nsf helper** and **nsf ietf helper disable**. Meanwhile, the **nsf ietf helper disable** command is supported solely for compatibility with other network software CLI.

nsf ietf helper disable

Parameters

None

Default

The default is None.

Command Mode

Router OSPFv3 Config

8-107 nsf helper strict-lsa-checking (OSPFv3)

A restarting router is not able to react to any topology changes. In particular, a restarting router cannot immediately update its forwarding table; as such, a topology change may lead to forwarding loops or black holes that remain until the graceful restart is completed. By exiting a graceful restart when a topology change occurs, a router seeks to eliminate any loops or black holes as fast as possible by

routing around the restarting router. A helpful neighbor will consider a link down with the restarting router to constitute a topology change, regardless of the strict LSA checking configuration.

This command can be used to require that an OSPF helpful neighbor exit the helper mode whenever a topology change occurs.

The **no** command allows the OSPF to continue as a helpful neighbor regardless of any topology changes.

nsf [ietf] helper strict-lsa-checking

no nsf [ietf] helper strict-lsa-checking

Parameters

ietf	(Optional) This keyword is accepted but not required.

Default

The default is Enabled.

Command Mode

Router OSPFv3 Config

OSPFv3 Stub Router Commands

8-108 max-metric router-lsa

Use this command in the Router OSPFv3 Global Configuration mode to configure OSPFv3 to enter the stub router mode. When OSPFv3 is in the stub router mode, OSPFv3 sets the metric for the nonstub links in its router LSA to MaxLinkMetric, thus causing other routers to compute very lengthy paths through the stub router and to prefer any alternate path. Thus, when alternate routes are available, doing so eliminates all transit traffic through the stub router. The stub router mode is useful when a router is being added to or removed from a network or for avoiding transient routes when a router reloads.

OSPFv3 can be forced into the stub router mode administratively. OSPFv3 remains in the stub router mode until the user takes OSPFv3 out of the stub router mode. Alternatively, OSPF can be configured to start in the stub router mode for a configurable period of time after the router boots up.

lf the summary LSA metric is set to 16,777,215, then other routers will skip the summary LSA when those routers compute routes.

lf a router has been configured to enter the stub router mode on startup (max-metric router-lsa on-startup), and then to enter max-metric router lsa, there is no change. lf OSPFv3 is administratively placed in the stub router mode (i.e., if the max-metric router-lsa command has been given), and the user then configures OSPFv3 to enter the stub router mode on startup (max-metric router-lsa on-startup), then OSPFv3 exits the stub router mode (assuming that the startup period has expired), and the configuration is then updated. If no parameters are sspecified, then the stub router mode sends only maximum metric values for router LSAs.

The **no** command can be used in the OSPFv3 Router Configuration mode to disable the stub router mode. Using the command clears either type of stub router mode (that is, always or on-startup) and resets all LSA options. In the event that the OSPF is configured to enter the global configuration mode on startup, and if during normal operation the user would like to immediately place OSPF in the stub router mode, then the command **no max-metric router-lsa on-startup** should be issued. Using the command no max-

metric with the external-lsa, inter-area-lsas, or summary-lsa option router-lsa summary-lsa causes the OSPF to send summary LSAs with metrics calculated using normal procedures.

max-metric router-lsa [external-lsa *1-16777215***] [inter-area lsas** *1-16777215***] [on-startup** *5-86466***] [summary-lsa** *1-16777215***]**

no no max-metric router-lsa [external-lsa] [inter-area-lsas] [on-startup] [summary-lsa]

Parameters

external-lsa *1-16777215*	(Optional) Sends the maximum metric values for external LSAs. max-metric-value is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFF). The default value is 16711680 (0XFF0000).
inter-area lsas *1-16777215*	(Optional) Sends the maximum metric values for lnter-Area-Router LSAs.
on-startup *5-86466*	(Optional) Starts OSPF in stub router mode. seconds is the number of seconds that OSPF remains in stub router mode after a reboot. The range is 5 to 86,400 seconds. There is no default value.
summary-lsa *1-16777215*	(Optional) Sends the maximum metric values for Summary LSAs.

Default

The default is as follows: OSPF not in stub router mode.

Command Mode

OSPFv3 Router Config

8-109 clear ipv6 ospf stub-router

Forces the OSPF to exit the stub router mode in the event that it has automatically entered the stub router mode due to a resource limitation. The OSPF only exits the stub router mode in the event that it entered the stub router mode due to a resource limitation or if it is in the stub router mode at startup. If the OSPF is configured to be in the stub router mode permanently, then this command has no effect.

clear ipv6 ospf stub-router

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

OSPFv3 Show Commands

8-110 show ipv6 ospf

Shows information relevant to the OSPF router.

show ipv6 ospf

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ipv6 ospf

Router ID..................................... 0.0.0.0
OSPF Admin Mode............................... Enable
External LSDB Limit........................... No Limit
Exit Overflow Interval........................ 0
SPF Start Time................................ 2000 ms
SPF Hold Time................................. 5000 ms
SPF Maximum Hold Time......................... 5000 ms
LSA Refresh Group Pacing Time................. 60 sec
AutoCost Ref BW............................... 100 Mbps
Default Passive Setting....................... Disabled
Prefix Suppression............................ Disabled
Maximum Paths................................. 48
Default Metric................................ Not Configured
Maximum Routes................................ 2048
Stub Router Configuration..................... None
Bfd Mode...................................... Disabled

Default Route Advertise....................... Disabled
Always........................................ False
Metric........................................ Not Configured
Metric Type................................... External Type 2

NSF Helper Support............................ Always
```

```
NSF Helper Strict LSA Checking.................. Enabled
```

Display Parameters

Note: Some of the information below is only shown if the user enables OSPF and configures certain features.

Router ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled..
External LSDB Limit	The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
SPF Start Time	The number of milliseconds the SPF calculation is delayed if no SPF calculation has been scheduled during the current “wait interval”.
SPF Hold Time	The number of milliseconds of the initial “wait interval”.
SPF Maximum Hold Time	The maximum number of milliseconds of the “wait interval”.
LSA Refresh Group Pacing Time	The size of the LSA refresh group window, in seconds.
AutoCost Ref BW	Shows the value of the auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.
Prefix-suppression	Displays whether prefix-suppression is enabled or disabled on the given interface.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
Default Metric	Default value for redistributed routes.
Maximum Routes	Indicates the maximum number of routes an OSPF path can take for a given destination.
Stub Router Configuration	Indicates the configuration setting of the stub router: Configured, Startup, Resource Limitation, or None.
Bfd Mode	Indicates whether BFD is enabled or disabled.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not.
Always	Shows whether default routes are always advertised.
Metric	The metric for the advertised default routes. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
NSF Helper Support	Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).

NSF help Strict LSA checking	Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.

8-111 show ipv6 ospf abr

Shows the internal OSPFv3 routes used to reach Area Border Routers (ABR). This command allows no options.

show ipv6 ospf abr

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Type	The type of the route to the destination. It can be either: • intra – intra-area route • inter – Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

8-112 show ipv6 ospf area

Shows information regarding the area. The *areaid* parameter identifies the OSPF area that is shown.

show ipv6 ospf area *areaid*

Parameters

areaid	Indicates the area ID.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Area ID	The area ID of the requested OSPF area.
External Routing	A number representing the external routing capabilities for this area.
Spf Runs	The number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
Stub Mode	Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled.
Import Summary LSAs	Shows whether to import summary LSAs (enabled).
OSPF Stub Metric Value	The metric value of the stub area. This field displays only if the area is a configured as a stub area.
The following OSPF NSSA specific information displays only if the area is configured as an NSSA.	
Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.
Default Information Originate	Shows whether to advertise a default route into the NSSA.
Default Metric	The metric value for the default route advertised into the NSSA.
Default Metric Type	The metric type for the default route advertised into the NSSA.
Translator Role	The NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	The amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

8-113 show ipv6 ospf asbr

Shows the internal OSPFv3 routes used to reach Autonomous System Boundary Routers (ASBR).

show ipv6 ospf asbr

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Type	The type of the route to the destination. It can be either: • intra – intra-area route • inter – Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

8-114 show ipv6 ospf database

Displays information regarding the link state database when the OSPFv3 is enabled. If no parameters are entered, then the command shows the LSA headers for all areas. The optional *areaid* parameter can be used to display the database information regarding a specific area. The other optional parameters can be used to specify the type of link state advertisements to show. The term **external** is used to display the external LSAs. The term **inter-area** is used to display the inter-area LSAs. The term **link** is used to display the link LSAs. The term **network** is used to display the network LSAs. The term **nssa-external** is used to display NSSA external LSAs. The term **prefix** is used to display intra-area Prefix LSAs. The term **router** is used to display router LSAs. The terms **unknown area**, **unknown as**, and **unknown link** are used to display unknown area, AS, or link-scope LSAs, respectively. The term *lsid* is used to specify the link state ID (LSID). The term **adv-router** is used to show the LSAs that are restricted by the advertising router. The term **self-originate** is used to display the LSAs that are self-originated. The information below is only shown if OSPF is enabled.

show ipv6 ospf [*areaid*] database [{external | inter-area {prefix | router} | link | network | nssa-external | prefix | router | unknown {area | as | link}}] [*lsid*] [{adv-router [*rtrid*] | self-originate}]

Parameters

areaid	(Optional) Indicates the area ID.
external	(Optional) External LSAs.
inter-area	(Optional) Inter-area LSAs.
prefix	Inter-area Prefix LSAs.
router	Inter-area Router LSAs.
link	(Optional) Indicates a link LSAs.
network	(Optional) Indicates a network LSAs.
nssa-external	(Optional) Indicates NSSA external LSAs.
prefix	(Optional) Indicates intra-area Prefix LSAs.
router	(Optional) Indicates a router LSAs.
unknown {area | as | link}	(Optional) Indicates unknown LSAs.
lsid	(Optional) Indicates the link state ID (LSID).
adv-router	(Optional) Restrict by advertising router.
rtrid	(Optional) Indicates a enter an IP Address.
self-originate	(Optional) Indicates self originated LSAs.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

The following information is displayed for each link-type and area.

Link Id	A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Adv Router	The Advertising Router. Is a 32-bit dotted decimal number representing the LSDB interface.
Age	A number representing the age of the link state advertisement in seconds.
Sequence	A number that represents which LSA is more recent.
Checksum	The total number LSA checksum.
Prefix	The IPv6 prefix.

Interface	The interface for the link.
Rtr Count	The number of routers attached to the network.

8-115 show ipv6 ospf database database-summary

Shows the number of each type of LSA in the database, as well as the total number of LSAs in the database.

show ipv6 ospf database database-summary

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Router	Total number of router LSAs in the OSPFv3 link state database.
Network	Total number of network LSAs in the OSPFv3 link state database.
Inter-area Prefix	Total number of inter-area prefix LSAs in the OSPFv3 link state database.
Inter-area Router	Total number of inter-area router LSAs in the OSPFv3 link state database.
Type-7 Ext	Total number of NSSA external LSAs in the OSPFv3 link state database.
Link	Total number of link LSAs in the OSPFv3 link state database.
Intra-area Prefix	Total number of intra-area prefix LSAs in the OSPFv3 link state database.
Link Unknown	Total number of link-source unknown LSAs in the OSPFv3 link state database.
Area Unknown	Total number of area unknown LSAs in the OSPFv3 link state database.
AS Unknown	Total number of as unknown LSAs in the OSPFv3 link state database.
Type-5 Ext	Total number of AS external LSAs in the OSPFv3 link state database.
Self-Originated Type-5	Total number of self originated AS external LSAs in the OSPFv3 link state database.

Total	Total number of router LSAs in the OSPFv3 link state database.

8-116 show ipv6 ospf interface

Shows the information for an IFO object or for virtual interface tables. The slot/port argument corresponds to either a physical routing interface or a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ipv6 ospf interface {*slot/port* **| brief |vlan** *1-4093* **| loopback** *loopback-id* **| tunnel** *tunnel-id***}**

Parameters

slot/port	Enter an interface in slot/port format.
brief	Display snapshot of OSPF interfaces configured.
vlan *1-4093*	Enter an interface in VLAN format.
loopback *loopback-id*	Display the configured Loopback interface information.
tunnel *tunnel-id*	Display the configured Tunnel interface information.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

IP Address	The IPv6 address of the interface.
ifIndex	The interface index number associated with the interface.
OSPF Admin Mode	Shows whether the admin mode is enabled or disabled.
OSPF Area ID	The area ID associated with this interface.
Router Priority	The router priority. The router priority determines which router is the designated router.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time. in seconds, the interface waits before assuming a neighbor is down.
LSA Ack Interval	The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.

Interface Transmit Delay	The number of seconds the interface adds to the age of LSA packets before transmission.
Authentication Type	The type of authentication the interface performs on LSAs it receives.
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
Prefix-suppression	Displays whether prefix-suppression is enabled, disabled, or unconfigured on the given interface.
Passive Status	Shows whether the interface is passive or not.
OSPF MTU-ignore	Shows whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.
Link LSA Suppression	The configured state of Link LSA Suppression for the interface.

The following informatiognliy displays if OSPF is initialized on the interface:

OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value broadcast. The OSPF interface Type will be ‘broadcast’.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.
Metric Cost	The cost of the OSPF interface.

8-117 show ipv6 ospf interface brief

Shows a brief summary of information for an IFO object or for virtual interface tables.

show ipv6 ospf interface brief

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Interface	The routing interface associated with the rest of the data in the row.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area ID for the specified interface.
Router Priority	The router priority. The router priority determines which router is the designated router.
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time, in seconds, the interface waits before assuming a neighbor is down.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Retransmit Delay Interval	The number of seconds the interface adds to the age of LSA packets before transmission.
LSA Ack Interval	The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.

8-118 show ipv6 ospf interface stats

Shows the statistics for the specified interface. The command only displays information, however, if OSPF is enabled.

show ipv6 ospf interface stats {*slot/port* **| vlan** *id***}**

Parameters

slot/port	Enter an interface in slot/port format.
vlan *id*	Enter an interface in VLAN format.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

OSPFv3 Area ID	The area ID of this OSPF interface.

IP Address	The IP address associated with this OSPF interface.
OSPFv3 Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state. or an error has occurred.
Packets Received	The number of OSPFv3 packets received on the interface.
Packets Transmitted	The number of OSPFv3 packets sent on the interface.
LSAs Sent	The total number of LSAs flooded on the interface.
LSA Acks Received	The total number of LSAs acknowledged from this interface.
LSA Acks Sent	The total number of LSAs acknowledged to this interface.
Sent Packets	The number of OSPF packets transmitted on the interface.
Received Packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packets sender.
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packets destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. NOTE: Does not apply to Hellos.
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

The number of OSPF packets of each type that are sent and received on the interface are listed in Table 11.

8-119 show ipv6 ospf lsa-group

Shows the number of self-originated LSAs within each LSA group.

show ipv6 ospf lsa-group

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following provides an example of the command.

```
(Routing)#show ipv6 ospf lsa-group

Total self-originated LSAs: 3019
Average LSAs per group: 100
Pacing group limit: 400
Number of self-originated LSAs within each LSA group...

   Group Start Age   Group End Age      Count
                 0              59         96
                60             119         88
               120             179        102
               180             239         95
               240             299         95
               300             359         92
               360             419         48
               420             479         58
               480             539        103
               540             599         99
               600             659        119
               660             719        110
               720             779        106
               780             839        122
               840             899        110
               900             959         99
               960            1019        135
              1020            1079        101
              1080            1139         94
              1140            1199        115
              1200            1259        110
              1260            1319        111
              1320            1379        111
              1380            1439         99
              1440            1499        102
              1500            1559         96
```

```
          1560          1619          106
          1620          1679          111
          1680          1739          106
          1740          1799           80
          1800          1859            0
          1860          1919            0
```

Display Parameters

Total self-originated LSAs	The number of LSAs the router is currently originating.
Average LSAs per group	The number of self-originated LSAs divided by the number of LSA groups. The number of LSA groups is the refresh interval (1800 seconds) divided by the pacing interval (configured with timers pacing lsa-group) plus two.
Pacing group limit	The maximum number of self-originated LSAs in one LSA group. If the number of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout the refresh interval to achieve better balance.
Groups	For each LSA pacing group, the output shows the range of LSA ages in the group and the number of LSAs in the group.

8-120 show ipv6 ospf max-metric

Shows the configured maximum metrics for the stub-router mode.

show ipv6 ospf max-metric

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following provides an example of the command.

```
(Config)#show ipv6 ospf max-metric

OSPFv3 Router with ID (3.3.3.3)
  Start time: 00:00:00, Time elapsed: 00:01:05
  Originating router-LSAs with maximum metric
     Condition: on startup for 1000 seconds, State: inactive
```

```
    Advertise external-LSAs with metric 16711680
```

8-121 show ipv6 ospf neighbor

Shows information regarding OSPF neighbors. If a neighbor IP address is not specified, summary information is displayed in a table. If an interface or tunnel is specified, then only information about that interface or tunnel will be displayed. The slot/port argument corresponds to either a physical routing interface or a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. The *ip-address* parameter indicates the IP address of the neighbor, and when this is specifed, detailed information regarding the neighbor will be displayed. The information below is only displayed if OSPF is enabled and if the interface has a neighbor.

show ipv6 ospf neighbor [interface {*slot/port* **| vlan** *1-4093* **| tunnel** *tunnel_id***}] [***ip-address***]**

Parameters

interface	(Optional) Indicates the restrict interface.
slot/port	Enter an interface in slot/port format.
vlan	Enter an interface in VLAN format (1-4093).
tunnel *tunnel_id*	Display the configured Tunnel interface information.
ip-address	(Optional) Enter the IPv6 address for the indicated neighbor interface.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

If an IP address is not specified, a table with the following columns will be displayed for all neighbors or for the neighbor associated with the interface specified by the user:

Router ID	The 4-digit dotted-decimal number of the neighbor router.
Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
Intf ID	The interface ID of the neighbor.
Interface	The interface of the local router.
State	The state of the neighboring routers. Possible values are: • Down – initial state of the neighbor conversation - no recent information has been received from the neighbor.

	• Attempt – no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. • lnit – an Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. • 2 way – communication between the two routers is bidirectional. • Exchange start – the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial Database Description (DD) sequence number. • Exchange – the router is describing its entire link state database by sending DD packets to the neighbor. • Full – the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Restart Helper Status	Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: • Helping – This router is acting as a helpful neighbor to the specified router. • Not Helping – This router is not a helpful neighbor at this time.
Restart Reason	When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router.
Remaining Grace Time	The number of seconds remaining in current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command.
Restart Helper Exit Reason	Indicates the reason that the specified router last exited a graceful restart. • None – Graceful restart has not been attempted • in Progress – Restart is in progress • Completed – The previous graceful restart completed successfully • Timed Out – The previous graceful restart timed out • Topology Changed – The previous graceful restart terminated prematurely because of a topology change.

If you specify an IP address for the neighbor router, the following fields display:

Interface	The interface of the local router.
Area ID	The area ID associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. These are listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	The router priority for the specified interface.
Dead Timer Due	The amount of time, in seconds, to wait before the router assumes the

	neighbor is unreachable.
State	The state of the neighboring routers.
Events	Number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router ID of the specified interface.

8-122 show ipv6 ospf range

Shows the set of OSPFv3 area ranges that are configured for a given area.

show ipv6 ospf range *areaid*

Parameters

areaid	Indicates an area ID.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Area ID	The area whose prefixes are summarized.
IPv6 Prefix/Prefix Length	The summary prefix and prefix lengtn.
Type	**S** (Summary Link) or **E** (External Link).
Action	**Enabled** or **Disabled**.
Cost	Metric to be advertised when the range is active.

8-123 show ipv6 ospf statistics

Shows information regarding the 15 most recent Shortest Path First (SPF) calculations. SPF consists of the OSPF routing table calculation.

show ipv6 ospf statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 ospf statistics

Area 0.0.0.0: SPF algorithm executed 10 times

Delta T      Intra    Summ     Ext    SPF Total   RIB Update       Reason
23:32:46         0       0       0            0            0       R, IP
23:32:09         0       0       0            0            0       R, N, IP
23:32:04         0       0       0            0            0       R
23:31:44         0       0       0            0            0       R, N, IP
23:31:39         0       0       0            0            1       R
23:29:57         0       3       7           10          131       R
23:29:52         0      14      29           43          568       SN
04:07:23         0       9      23           33          117       SN
04:07:23         0       9      23           33          117       SN
04:07:18         0       0       0            1          485       SN
04:07:14         0       1       0            1            3       X
```

Display Parameters

The following information will be displayed, with the most recent statistics shown at the end of the table.

Delta T	The time since the routing table was computed. The time is in the format hours, minutes, and seconds (hh:mm:ss).
Intra	The time taken to compute intra-area routes, in milliseconds.
Summ	The time taken to compute inter-area routes, in milliseconds.
Ext	The time taken to compute external routes, in milliseconds.
SPF Total	The total time taken to compute routes, in milliseconds. The total may exceed the sum of Intra, Summ, and Ext times.
RIB Update	The time from the completion of the routing table calculation until all changes have been made in the common routing table [the Routing Information Base (RIB)], in milliseconds.

Reason	The event or events that triggered the SPF. The reason codes are as follows: • R: New router LSA • N: New network LSA • SN: New network (inter-area prefix) summary LSA • SA: New ASBR (inter-area router) summary LSA • X: New external LSA • IP: New intra-area prefix LSA • L: New Link LSA

8-124 show ipv6 ospf stub table

Shows the OSPF stub table. The information below will be shown only if OSPF is initialized on the switch in question.

show ipv6 ospf stub table

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Area ID	A 32-bit identifier for the created stub area.
Type of Service	Type of service associated with the stub metric. For this release, Normal TOS is the only supported type.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

8-125 show ipv6 ospf virtual-link

Shows the OSPF Virtual Interface information for a specific area and neighbor. The *areaid* parameter specifies the area, while the *neighbor* parameter specifies the neighbor's Router ID.

show ipv6 ospf virtual-link *areaid neighbor*

Parameters

areaid	Indicates the area ID of the requested OSPF area.
neighbor	Indicates the input neighbor Router ID.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Area ID	The area ID of the requested OSPF area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Interface Transmit Delay	The configured transmit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	The type of authentication the interface performs on LSAs it receives.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

8-126 show ipv6 ospf virtual-link brief

Shows the OSPFv3 Virtual interface information for all the areas in the system.

show ipv6 ospf virtual-link brief

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ipv6 ospf virtual-link brief

                                    Hello        Dead     Retransmit  Transmit
   Area ID         Neighbor        Interval    Interval    Interval    Delay
---------------  ---------------  ----------  ----------  ----------  --------
```

Display Parameters

Area ID	The area ID of the requested OSPFv3 area.
Neighbor	The neighbor interface of the OSPFv3 virtual interface.
Hello Interval	The configured hello interval for the OSPFv3 virtual interface.
Dead Interval	The configured dead interval for the OSPFv3 virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPFv3 virtual interface.
Transmit Delay	The configured transmit delay for the OSPFv3 virtual interface.

DHCPv6 Commands

In this section, the commands used to configure the DHCPv6 server on the system and to view DHCPv6 information are described.

8-127 ipv6 dhcp client pd

Enables the Dynamic Host Configuration Protocol (DHCP) for an IPv6 client process (that is, if the process is not currently running) and enables requests for prefix delegation (PD) through a specified interface. A prefix is stored in the IPv6 general prefix pool with an internal name that is defined by the automatic argument when prefix delegation is enabled and the prefix in question is successfully acquired.

Note: Only one IP interface provides support for the Prefix Delegation client.

The optional **rapid-commit** parameter enables the utilization of a two-message exchange method for prefix delegation and for other configurations. If the parameter is enabled, the client will include the rapid commit option in a solicit message.

On a given interface, the DHCP for IPv6 client, server, and relay functions are mutually exclusive. In the event that one of these functions is already enabled and the user attempts to configure a different function on the given interface, a message will be displayed.

The **no** command disables requests for prefix delegation.

ipv6 dhcp client pd [rapid-commit]

no ipv6 dhcp client pd

Parameters

rapid-commit	(Optional) Indicates the IPv6 DHCP Client Preference.

Default

The default is Disabled on an interface.

Command Mode

Interface Config

Example

The following examples of the command enable prefix delegation on interface 0/1.

```
(Switch)#configure
(Switch)(Config)#interface 0/1
(Switch)(Interface 0/1)#ipv6 dhcp client pd
```

```
(Switch)#configure
(Switch)(Config)#interface 0/1
(Switch)(Interface 0/1)#ipv6 dhcp client pd rapid-commit
```

8-128 ipv6 dhcp server

Configures DHCPv6 server functionality for a single interface or a range of interfaces. The *pool-name* parameter indicates the DHCPv6 pool that contains stateless and/or prefix delegation parameters; the **automatic** parameter enables the server to determine automatically which pool to use when addresses for a client are allocated; the **rapid-commit** parameter is an optional parameter that allows for an abbreviated exchange between the server and client; and the **preference** *pref-value* parameter is a value used by clients to determine their preference among multiple DHCPv6 servers. DHCPv6 server and DHCPv6 relay functions are mutually exclusive for a given interface.

ipv6 dhcp server {*pool-name* **| automatic} [rapid-commit] [preference** *pref-value***]**

Parameters

pool-name	Sets the IPv6 DHCP Server Pool Name.
automatic	Enables the server to automatically configure the pool.
rapid-commit	(Optional) Sets the IPv6 DHCP Server to Rapid Commit.
preference *pref-value*	(Optional) Sets the IPv6 DHCP Server Preference.

Default

The default is None.

Command Mode

Interface Config

8-129 ipv6 dhcp relay destination

Configures DHCPv6 relay functionality for a single interface or a range of interfaces. The **destination** keyword can be used to set the relay server IPv6 address. The *relay-address* parameter consists of the IPv6 address for a DHCPv6 relay server. The **interface** keyword can be used to set the relay server interface. The *relay-interface* parameter consists of an interface (*slot/port*) used to reach a relay server. The optional **remote-id** indicates the Relay Agent Information Option “remote ID” suboption that is to be added to relayed messages. This can consist of either the special keyword *duid-ifid*, which results in the “remote ID” being derived from both the DHCPv6 server DUID and the relay interface number, or it can consist of a user-defined string.

Note: If the *relay-address* parameter consists of an IPv6 global address, then the *relay-interface* parameter is not required. If the *relay-address* parameter consists of a link-local or multicast address, then the *relay-interface* parameter is required. Finally, if a value for the *relay-address* is not specified, then a value for the *relay-interface* parameter must be specified and the DHCPV6-ALL-AGENTS multicast address (i.e., **FF02::1:2**) will be used to relay DHCPv6 messages to the relay server.

ipv6 dhcp relay {destination [*relay-address***] interface [***relay-interface***] | interface [***relay-interface***]} [remote-id {***duid-ifid* **| user-defined-string}]**

Parameters

destination	Sets the IPv6 DHCP Relay Address.
relay-address	(Optional) Indicates the IPv6 address of the relay server.
interface	Set the IPv6 DHCP Relay Interface.
relay-interface	(Optional) Indicates the IPv6 DHCP relay interface of the relay server.
remote-id	(Optional) Set the IPv6 DHCP Relay Remote ID.
duid-ifid	Sets the IPv6 DHCP Relay Remote ID.
user-defined-string	Sets IPv6 DHCP relay user defined remote ID.

Default

The default is None.

Command Mode

Interface Config

8-130 ipv6 dhcp pool

This command is used in the Global Config mode in order to enter the IPv6 DHCP Pool Config mode. The **exit** command can then be used to return to the Global Config mode. Also, enter CTRL+Z to return to the User EXEC mode. The *pool-name* parameter should be less than 31 alpha-numeric characters in length. DHCPv6 pools are used in order to specify information that a DHCPv6 server distributes to DHCPv6 clients. Such pools are shared among multiple interfaces over which DHCPv6 server capabilities are configured.

Once the creation of the DHCP for an IPv6 configuration information pool has been completed, the **ipv6 dhcp server** command can be used to associate the pool with a given server on a given interface. If an information pool is not configured, the **ipv6 dhcp server** interface configuration command can be used to enable the DHCPv6 server function on a given interface.

When a DHCPv6 pool is associated with an interface, only that pool will service any requests on the associated interface. The pool will also service other interfaces. If a DHCPv6 pool is not associated with an interface by the user, the pool can service requests on any interface. If no IPv6 address prefix is used, then the pool will return only configured options.

The **no** command removes the specified DHCPv6 pool.

ipv6 dhcp pool *pool-name*

no ipv6 dhcp pool *pool-name*

Parameters

pool-name	Enter Pool Name. Range 1-31 characters.

Default

The default is None.

Command Mode

Global Config

8-131 address prefix (IPv6)

Sets an address prefix for address assignment, where the address must be in hexadecimal form and use 16-bit values between colons.

If the optional **lifetime** parameter values are not configured, then the default lifetime values for the *valid-lifetime* and *preferred-lifetime* parameters are considered to be infinite.

address prefix *ipv6-prefix* **[lifetime {***valid-lifetime preferred-lifetime* **| infinite}]**

Parameters

ipv6-prefix	Indicates an IPv6 address prefix in hexadecimal format using 16-bit values between colons.

lifetime	(Optional) Sets a length of time for the hosts to remember router advertisements. If configured, both valid and preferred lifetimes must be configured.
valid-lifetime	The amount of time, in seconds, the prefix remains valid for the requesting router to use. The range is from 60 through 4294967294. The preferred-lifetime value cannot exceed the valid-lifetime value.
preferred-lifetime	The amount of time, in seconds, that the prefix remains preferred for the requesting router to use. The range is from 60 through 4294967294. The preferred-lifetime value cannot exceed the valid-lifetime value.
infinite	An unlimited lifetime.

Default

The default is None.

Command Mode

IPv6 DHCP Pool Config

Example

The following example of the command shows how a user can configure an IPv6 address prefix for the IPv6 configuration pool pool1.

```
(Switch)#configure
(Switch)(Config)#ipv6 dhcp pool pool1
(Switch)(Config-dhcp6s-pool)#address prefix 2001::/64
(Switch)(Config-dhcp6s-pool)#exit
```

8-132 domain-name (IPv6)

Sets the DNS domain name that is provided to a DHCPv6 client by a DHCPv6 server. The DNS domain name is configured to provide stateless server support. The domain name can be no more than 31 alpha-numeric characters in length. A DHCPv6 pool can include multiple domain names, up to a maximum of 8.

The **no** command removes a DHCPv6 domain name from a DHCPv6 pool.

domain-name *domain*

no domain-name *domain*

Parameters

domain	Indicates the DNS domain name as provided by a DHCPv6 server.

Default

The default is None.

Command Mode

IPv6 DHCP Pool Config

8-133 dns-server (IPv6)

Sets the IPv6 DNS server address that is provided to a DHCPv6 client by a DHCPv6 server. A DNS server address is configured to provide stateless server support. A DHCPv6 pool can include multiple domain names, up to a maximum of 8.

The **no** command removes a DHCPv6 server address from a DHCPv6 server.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Parameters

ipv6-address	Indicates an IPv6 address in hexadecimal format using 16-bit values between colons.

Default

The default is None.

Command Mode

IPv6 DHCP Pool Config

8-134 prefix-delegation (IPv6)

It is possible to define multiple IPv6 prefixes within a pool for distribution to specific DHCPv6 Prefix delegation clients. The prefix parameter indicates the delegated IPv6 prefix, and the DUID parameter indicates the client's unique DUID value (Example: 00:01:00:09:f8:79:4e:00:04:76:73:43:76). The name parameter consists of a 31-character textual client's name that is useful for logging or tracing purposes only. The valid lifetime parameter indicates, in seconds, the valid lifetime for the delegated prefix, and the preferred lifetime parameter indicates, in seconds, the preferred lifetime for the delegated prefix.

The **no** command deletes a specific prefix-delegation client.

prefix-delegation *prefix/prefixlength* **client-***DUID* **[name** *client-name***] [prefer-lifetime** *0-4294967295* **| infinite] [valid-lifetime** *0-4294967295* **| infinite]**

no prefix-delegation *prefix/prefix-delegation DUID*

Parameters

prefix/prefixlength	Inidcates the IPv6 prefix and prefix length.
client-*DUID*	Enter generated IPv6 DHCP unique identifier string.
name *client-name*	(Optional) Indicates the Prefix Delegation Host Name.
prefer-lifetime	(Optional) Indicates the preferred lifetime (*0-4294967295*).

infinite	(Optional) Sets Preferred Lifetime to be infinite.
valid-lifetime	(Optional) Indicates a valid lifetime value (*0-4294967295*).
prefix/prefix-delegation DUID	Enter Preferred Lifetime in the range of 0 to 4294967295 seconds (configuring 0 equates to selecting 4294967295).

Default

The default is as follows:

- valid-lifetime – 2592000
- preferred-lifetime – 604800

Command Mode

IPv6 DHCP Pool Config

8-135 show ipv6 dhcp statistics

Shows the IPv6 DHCP statistics for all interfaces.

show ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show ipv6 dhcp statistics

DHCPv6 Interface Global Statistics
-------------------------------------------------
DHCPv6 Solicit Packets Received.................. 0
DHCPv6 Request Packets Received.................. 0
DHCPv6 Confirm Packets Received.................. 0
DHCPv6 Renew Packets Received.................... 0
DHCPv6 Rebind Packets Received................... 0
DHCPv6 Release Packets Received.................. 0
DHCPv6 Decline Packets Received.................. 0
DHCPv6 Inform Packets Received................... 0
```

```
DHCPv6 Relay-forward Packets Received..... 0
DHCPv6 Relay-reply Packets Received..... 0
DHCPv6 Malformed Packets Received..... 0
Received DHCPv6 Packets Discarded..... 0
Total DHCPv6 Packets Received..... 0
DHCPv6 Advertisement Packets Transmitted..... 0
DHCPv6 Reply Packets Transmitted..... 0
DHCPv6 Relay-reply Packets Transmitted..... 0
DHCPv6 Relay-forward Packets Transmitted..... 0
Total DHCPv6 Packets Transmitted..... 0
```

Display Parameters

DHCPv6 Solicit Packets Received	Number of solicit received statistics.
DHCPv6 Request Packets Received	Number of request received statistics.
DHCPv6 Confirm Packets Received	Number of confirm received statistics.
DHCPv6 Renew Packets Received	Number of renew received statistics.
DHCPv6 Rebind Packets Received	Number of rebind received statistics.
DHCPv6 Release Packets Received	Number of release received statistics.
DHCPv6 Decline Packets Received	Number of decline received statistics.
DHCPv6 Inform Packets Received	Number of inform received statistics.
DHCPv6 Relay-forward Packets Received	Number of relay forward received statistics.
DHCPv6 Relay-reply Packets Received	Number of relay-reply received statistics.
DHCPv6 Malformed Packets Received	Number of malformed packets statistics.
Received DHCPv6 Packets Discarded	Number of DHCP discarded statistics.
Total DHCPv6 Packets Received	Total number of DHCPv6 received statistics.
DHCPv6 Advertisement Packets Transmitted	Number of advertise sent statistics.
DHCPv6 Reply Packets Transmitted	Number of reply sent statistics.
DHCPv6 Reconfig Packets Transmitted	Number of reconfigure sent statistics.

DHCPv6 Relay-reply Packets Transmitted	Number of relay-reply sent statistics.
DHCPv6 Relay-forward Packets Transmitted	Number of relay-forward sent statistics.
Total DHCPv6 Packets Transmitted	Total number of DHCPv6 sent statistics.

8-136 show ipv6 dhcp interface

Shows the DHCPv6 information for all the relevant interfaces or for a specified interface. The slot/port argument corresponds to either a physical routing interface or a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. If an interface is specified, the user can utilize the optional **statistics** parameter in order to view statistics for the specified interface.

show ipv6 dhcp interface {*slot/port* **| vlan** *1-4093***} [statistics]**

Parameters

slot/port	Enters an interface in slot/port format.
vlan *1-4093*	Enters an interface in VLAN format.
statistics	(Optional) Displays IPv6 Interface Statistics.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

IPv6 Interface	The interface name in slot/port format.
Mode	Shows whether the interface is an IPv6 DHCP relay or server.

lf the server interface mode is used, the following information will be displayed.

Pool Name	The pool name specifying information for DHCPv6 server distribution to DHCPv6 clients.
Server Preference	The preference of the server.
Option Flags	Shows whether rapid commit is enabled.

lf the relay interface mode is used, the following information will be displayed.

Relay Address	The IPv6 address of the relay server.
Relay Interface Number	The relay server interface in slot/port format.
Relay Remote ID	If configured, shows the name of the relay remote.
Option Flags	Shows whether rapid commit is configured.

If the statistics parameter is used, the command will cause the IPv6 DHCP statistics for the specified interface to be displayed. For detailed information about the output, please see “show ipv6 dhcp statistics”.

8-137 show ipv6 dhcp binding

Shows the configured DHCP pool.

show ipv6 dhcp binding [*ipv6-address***]**

Parameters

ipv6-address	(Optional) Indicates the display client IPv6 Address

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

DHCP Client Address	Address of DHCP Client.
DUID	String that represents the Client DUID.
IAID	Identity Association ID.
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Prefix Type	IPv6 Prefix type (IAPD, IANA, or IATA).
Client Address	Address of DHCP Client.
Client Interface	IPv6 Address of DHCP Client.
Expiration	Address of DNS server address.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.

8-138 show ipv6 dhcp pool

Shows the configured DHCP pool.

show ipv6 dhcp pool *pool-name*

Parameters

pool-name	Enter a Pool Name up to 32 alphanumeric characters in length.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

DHCP Pool Name	Unique Pool name configuration.
Client DUID	Client's DHCP unique identifier (DUID). DUID is generated using the combination of the local system burned-in MAC address and a timestamp value.
Host	Name of the client.
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
DNS Server Address	Address of DNS server address.
Domain Nane	DNS domain name.

8-139 show network ipv6 dhcp statistics

Shows the statistics for the DHCPv6 client that is running on the network management interface.

show network ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC

- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Switching)#show network ipv6 dhcp statistics

DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received.....................0
DHCPv6 Reply Packets Received.............................0
Received DHCPv6 Advertisement Packets Discarded...........0
Received DHCPv6 Reply Packets Discarded...................0
DHCPv6 Malformed Packets Received.........................0
Total DHCPv6 Packets Received.............................0

DHCPv6 Solicit Packets Transmitted........................0
DHCPv6 Request Packets Transmitted........................0
DHCPv6 Renew Packets Transmitted..........................0
DHCPv6 Rebind Packets Transmitted.........................0
DHCPv6 Release Packets Transmitted........................0
Total DHCPv6 Packets Transmitted..........................0
```

Display Parameters

DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the network interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the network interface.

DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the network interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the network interface.

8-140 show serviceport ipv6 dhcp statistics

Shows the statistics for the DHCPv6 client that is running on the serviceport management interface.

show serviceport ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Switching)#show serviceport ipv6 dhcp statistics

DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received.....................0
DHCPv6 Reply Packets Received.............................0
Received DHCPv6 Advertisement Packets Discarded...........0
Received DHCPv6 Reply Packets Discarded...................0
DHCPv6 Malformed Packets Received.........................0
Total DHCPv6 Packets Received.............................0

DHCPv6 Solicit Packets Transmitted........................0
DHCPv6 Request Packets Transmitted........................0
DHCPv6 Renew Packets Transmitted..........................0
DHCPv6 Rebind Packets Transmitted.........................0
DHCPv6 Release Packets Transmitted........................0
Total DHCPv6 Packets Transmitted..........................0
```

Display Parameters

DHCPV6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the service port interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the service port interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the service port interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the service port interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the service port interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the service port interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the service port interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the service port interface.
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the service port interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the service port interface.
DHCPv6 Release Packets Transmitted	The number of DHCPV6 Release packets transmitted on the service port interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the service port interface.

8-141 clear ipv6 dhcp

Clears the DHCPv6 statistics for all interfaces or for the specified interface. The slot/port parameter can be used to specify an interface and the VLAN parameter can be used to specify a VLAN.

clear ipv6 dhcp {statistics | interface {*slot/port* **| vlan** *id***} }**

Parameters

statistics	Clears the IPv6 DHCP Statistics.
slot/port	Indicates an interface in slot/port format.
vlan *id*	Indicates an interface in VLAN format.

Default

The default is None.

Command Mode

Privileged EXEC

8-142 clear ipv6 dhcp binding

Deletes a given automatic address binding from the DHCP server database. The address parameter must be a valid IPv6 address.

On the DHCP for the lPv6 server, a binding table entry is automatically:

- Created whenever the delegation of a prefix to a client from the configuration pool occurs.
- Updated when the prefix delegation is renewed, rebinded, or confirmed by the client.
- Deleted when all the prefixes in the binding are voluntarily released by the client, all the prefixes' valid lifetimes have expired, or the clear IPv6 DHCP binding command is run by an administrator.

In the event that the **clear ipv6 dhcp binding** command is utilized with the optional *ipv6-address* argument specified, then only the binding for the client that is specified is deleted. When the **clear ipv6 dhcp binding** command is utilized without the ipv6-address argument, then all of the automatic client bindings are cleared from the DHCP for IPv6 binding table.

clear ipv6 dhcp binding [*ipv6-address***]**

Parameters

ipv6-address	(Optional) Clears IPv6 DHCP binding for given address.

Default

The default is None.

Command Mode

Privileged EXEC

8-143 clear network ipv6 dhcp statistics

Clears the DHCPv6 statistics from the *network management* interface.

clear network ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

8-144 clear serviceport ipv6 dhcp statistics

Clears the DHCPv6 client statistics from the *service port* interface.

clear serviceport ipv6 dhcp statistics

Parameters

None

Default

The default is None.

Command Mode

Privileged EXEC

DHCPv6 Snooping Configuration Commands

In this section, the commands used to configure IPv6 DHCP Snooping are described.

8-145 ipv6 dhcp snooping

Globally enables IPv6 DHCP Snooping.

The **no** command globally disables IPv6 DHCP Snooping.

ipv6 dhcp snooping

no ipv6 dhcp snooping

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

8-146 ipv6 dhcp snooping vlan

Enables DHCP Snooping on a list of VLAN ranges separated by commas.

The **no** command disables DHCP Snooping on VLANs.

ipv6 dhcp snooping vlan *vlan-list*

no ipv6 dhcp snooping vlan *vlan-list*

Parameters

vlan-list	Enter VLAN IDs in range <1-4093>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Default

The default is Disabled.

Command Mode

Global Config

8-147 ipv6 dhcp snooping verify mac-address

Enables the source MAC address to be verified with the client hardware address in a received DCHP message.

The **no** command disables the ability to verify the source MAC address with the client hardware address.

ipv6 dhcp snooping verify mac-address

no ipv6 dhcp snooping verify mac-address

Parameters

None

Default

The default is Enabled.

Command Mode

Global Config

8-148 ipv6 dhcp snooping database

Configures the persistent location for the DHCP Snooping database. This location can consist of a local or a remote file on a specific IP machine.

ipv6 dhcp snooping database {local | tftp://hostIP/filename | write delay *interval***}**

Parameters

local	Configure DHCP snooping binding url in the form local.
tftp://hostIP/filename	Configure DHCP snooping binding url in the form tftp://host/filename.
Write delay *interval*	Configure DHCP snooping bindings store interval in seconds (15-86400).

Default

The default is Local.

Command Mode

Global Config

8-149 ipv6 dhcp snooping database write-delay

Configures the interval at which the DHCP Snooping database is persisted in seconds.

The **no** command resets the write delay value back to the default value.

ipv6 dhcp snooping database write-delay *15-86400*

no ipv6 dhcp snooping database write-delay 15-86400

Parameters

None

Default

The default is 300 seconds.

Command Mode

Global Config

8-150 ipv6 dhcp snooping binding

Configures static DHCP Snooping binding.

The **no** command removes the existing DHCP static entry from the DHCP Snooping database.

ipv6 dhcp snooping binding *macaddr* **vlan** *1-4093 ipv6-address* **interface** *interface id*

no ipv6 dhcp snooping binding *macaddr*

Parameters

macaddr	Indicates the MAC address.
vlan	Indicates a VLAN ID (1-4093).
ipv6-address	Indicates an IPv6 Address.
interface *interface id*	Indicates an interface ID to bind.

Default

The default is None.

Command Mode

Global Config

8-151 ipv6 dhcp snooping trust

Configures a single interface or a range of interfaces as trusted.

The **no** command configures a port as untrusted.

ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

8-152 ipv6 dhcp snooping log-invalid

Controls the filtration of logging DHCP messages by the DHCP Snooping application. The command can be utilized to configure either a specific interface or a range of interfaces.

The **no** command disables the filtration of logging DHCP messages by the DHCP Snooping application.

ipv6 dhcp snooping log-invalid

no ipv6 dhcp snooping log-invalid

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

8-153 ipv6 dhcp snooping limit

Controls the rate at which the DHCP Snooping messages arrive at a specific interface or a range of interfaces. Rate limiting is disabled by default. When rate limiting is enabled, the allowable rate can range from 0 to as high as 300 packets per second. The allowed range for the burst level is 1 to 15 seconds. The configuration of rate limiting occurs on a physical port, and it may be applied to both trusted and untrusted ports.

The **no** command resets the rate at which the DHCP Snooping messages arrive, as well as the burst level, to the default values.

ipv6 dhcp snooping limit {rate *0-300* **[***burst interval seconds***]}**

no ipv6 dhcp snooping limit

Parameters

rate	Configure rate limit in pps (0-300).
burst interval seconds	(Optional) Indicates the burst interval in seconds.

Default

The default is Disabled (no limit).

Command Mode

Interface Config

8-154 ipv6 verify source

Configures the lPv6SG source ID attribute so that it filters the data traffic in the hardware. The source ID consists of a combination of the IP address and MAC address. Normal command makes data traffic filtration based on the IP address possible. With the “port-security” option, meanwhile, the filtering of data traffic is conducted based on the IP and MAC addresses.

Please note that this command can be used to configure either a specific interface or a range of interfaces.

The **no** command disables the IPv6SG configuration in the hardware. The port-security cannot be disabled alone if it is configured.

ipv6 verify source {port-security}

no ipv6 verify source

Parameters

port-security	Filter incoming packets by source MAC address.

Default

The default is as follows:the IP address indicates the source ID.

Command Mode

Interface Config

8-155 ipv6 verify binding

Configures entries regarding the static IPv6 source guard (lPv6SG).

The **no** command removes an IPv6SG static entry from the IPv6SG database.

ipv6 verify binding *mac-address* **vlan** *vlan id ip IPv6 address* **interface** *interface id*

no ipv6 verify binding *mac-address* **vlan** *vlan id IPv6 address* **interface** *interface id*

Parameters

mac-address	Indicates a MAC address.
vlan *vlan id*	Indicates a VLAN ID.
ip address	Indicates an IPv6 Address.
interface *interface id*	Indicates an interface ID to bind.

Default

The default is None.

Command Mode

Global Config

8-156 show ipv6 dhcp snooping

Shows the DHCP Snooping global configurations and the configurations for each port.

show ipv6 dhcp snooping

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch)#show ipv6 dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40

Interface    Trusted         Log Invalid Pkts
----------   ----------      --------------------
0/1          Yes             No
0/2          No              Yes
0/3          No              Yes
0/4          No              No
0/6          No              No
```

Display Parameters

Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

8-157 show ipv6 DHCP snooping binding

Shows the DHCP Snooping binding entries. The following options can be used to restrict the output:

- Dynamic: Restricts the output according to DCHP snooping.
- Interface: Restricts the output according to a specific interface.
- Static: Restricts the output according to static entries.
- VLAN: Restricts the output according to VLAN.

show ipv6 dhcp snooping binding [{static | dynamic}] [interface *slot/port***] [vlan** *1-4093***]**

Parameters

static	(Optional) Restricts the output according to static entries.
dynamic	(Optional) Restricts the output according to DCHP snooping.
interface *slot/port*	(Optional) Restricts the output according to a specific interface.
vlan *1-4093*	(Optional) Restricts the output according to VLAN (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch)#show ipv6 dhcp snooping binding

Total number of bindings: 2

MAC Address             IPv6 Address     VLAN    Interface   Type    Lease time (Secs)
--------------------    ---------------  -----   ----------  -----   -----------------
00:02:B3:06:60:80       2000::1/64       10      0/1                 86400
00:0F:FE:00:13:04       3000::1/64       10      0/1                 86400
```

Display Parameters

MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IPv6 Address	Displays the valid IPv6 address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease time (Secs)	The remaining lease time for the entry.

8-158 show ipv6 dhcp snooping database

Shows the DHCP Snooping configuration that is related to the database persistency.

show ipv6 dhcp snooping database

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch)#show ipv6 dhcp snooping database

agent url: /10.131.13.79:/sai1.txt
write-delay: 5000
```

Display Parameters

Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

8-159 show ipv6 dhcp snooping interfaces

Shows the DHCP Snooping status for all the interfaces or for a specified interface.

show ipv6 dhcp snooping interfaces [interface *slot/port***]**

Parameters

interface *slot/port*	Indicates an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch)#show ipv6 dhcp snooping interfaces
```

```
Interface    Trust State     Rate Limit(pps)    Burst Interval(seconds)
----------   ------------    ---------------    -------------------------
1/g1         No              15                 1
1/g2         No              15                 1
1/g3         No              15                 1
```

```
(switch)#show ip dhcp snooping interfaces ethernet 0/1

Interface    Trust State     Rate Limit(pps)    Burst Interval(seconds)
----------   ------------    ---------------    -------------------------
0/1          Yes             15                 1
```

8-160 show ipv6 dhcp snooping statistics

Lists the statistics regarding IPv6 DHCP Snooping security violations on untrusted ports.

show ipv6 dhcp snooping statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch)#show ipv6 dhcp snooping statistics

Interface    MAC Verify Failures  Client Ifc Mismatch  DHCP Server Msgs Rec'd
----------   -------------------- -------------------- -------------------------
0/2          0                    0                    0
0/3          0                    0                    0
0/4          0                    0                    0
0/5          0                    0                    0
0/6          0                    0                    0
0/7          0                    0                    0
0/8          0                    0                    0
0/9          0                    0                    0
0/10         0                    0                    0
0/11         0                    0                    0
```

0/12	0	0	0
0/13	0	0	0
0/14	0	0	0
0/15	0	0	0
0/16	0	0	0
0/17	0	0	0
0/18	0	0	0
0/19	0	0	0
0/20	0	0	0

Display Parameters

Interface	The IPv6 address of the interface in slot/port format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client hardware address mismatch.
Client lfc Mismatch	Represents the number of link-level flow control (LFC) mismatches between client identifiers.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

8-161 clear ipv6 dhcp snooping binding

Clears all DHCPv6 Snooping bindings on a specific interface or on all the interfaces.

clear ipv6 dhcp snooping binding [interface *slot/port***]**

Parameters

interface *slot/port*	(Optional) Indicates an interface in slot/port format.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

8-162 clear ipv6 dhcp snooping statistics

Clears all DHCPv6 Snooping statistics.

clear ipv6 dhcp snooping statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

8-163 show ipv6 verify

Shows the IPv6 configuration for a specified slot/port

show ipv6 verify *interface*

Parameters

interface	Indicates an interface in slot/port format.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch)#show ipv6 verify 0/1

Interface    Filter Type     IP Address      MAC Address          Vlan
----------   ------------    -------------   ------------------   -----
0/1          ipv6-mac        2000::1/64      00:02:B3:06:60:80    10
0/1          ipv6-mac        3000::1/64      00:0F:FE:00:13:04    10
```

Display Parameters

Interface	Interface address in slot/port format.
Filter Type	ls one of two values:

	• IPv6-mac: User has configured MAC address filtering on this interface. • IPv6: Only IPv6 address filtering on this interface.
IPv6 Address	IPv6 address of the interface.
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays “permit-all.”
VLAN	The VLAN for the binding rule.

8-164 show ipv6 verify source

Shows the IPv6SG configurations for all ports. If the user specifies the interface option, then the output is restricted to the slot/port that was specified.

show ipv6 verify source {*interface***}**

Parameters

interface	Indicates an interface in slot/port format.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch)#show ipv6 verify source

Interface    Filter Type     IP Address      MAC Address          Vlan
----------   ------------    -------------   -----------------    -----
0/1          ipv6-mac        2000::1/64      00:02:B3:06:60:80    10
0/1          ipv6-mac        3000::1/64      00:0F:FE:00:13:04    10
```

Display Parameters

Interface	Interface address in slot/port format.
Filter Type	ls one of two values: • IPv6-mac: User has configured MAC address filtering on this interface.

	• IPv6: Only IPv6 address filtering on this interface.
IPv6 Address	IPv6 address of the interface.
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. if port security is disabled on the interface, then the MAC Address field displays “permit-all.”
VLAN	The VLAN for the binding rule.

8-165 show ipv6 source binding

Shows the IPv6SG bindings.

show ipv6 source binding [{dhcp-snooping | static}] [Interface *slot/port***] [vlan** *Id***]**

Parameters

dhcp-snooping	(Optional) Restrict the output based on DHCP snooping.
static	(Optional) Restrict the output based on static entries.
Interface *slot/port*	(Optional) Restrict the output based on a specific interface.
vlan *Id*	(Optional) Restricts the output based on VLAN.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(switch) #show ipv6 source binding

MAC Address             IP Address   Type              Vlan      Interface
--------------------    ----------   ---------------   -----     ----------
00:00:00:00:00:08       2000::1      dhcp-snooping     2         0/1
00:00:00:00:00:09       3000::1      dhcp-snooping     3         0/1
00:00:00:00:00:0A       4000::1      dhcp-snooping     4         0/1
```

Display Parameters

MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.

Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in slot/port format.

9. IP Multicast Commands

In this chapter, the IP Multicast commands made available in the D-LINK OS CLI are described.

The following sections are contained in this IP Multicast Commands chapter:

CAUTION: The commands described in this chapter belong to one of the two following functional groups:

- Show commands, which are used to display switch settings, statistics, and other information.
- Configuration commands, which are used to configure the features and options of the given switch. For every configuration command, there is a corresponding show command that can be used to display the configuration setting.

Multicast Commands

In this section, the commands used to configure IP Multicast and view IP Multicast settings and statistics are described.

9-1 ip mcast boundary

Adds an administrative scope multicast boundary that is specified by the *groupipaddr* and *mask* parameters, which indicate the group IP address and group IP mask for which the multicast administrative boundary is applicable. A single interface or a range of interfaces can be configured using this command.

The **no** command deletes an administrative scope multicast boundary that is specified by the *groupipaddr* and *mask* parameters, which indicate the group IP address and group IP mask for which the multicast administrative boundary is applicable.

ip mcast boundary *groupipaddr mask*

no ip mcast boundary *groupipaddr mask*

Parameters

groupipaddr	Indicates the group IP address.
mask	Indicates an IP address mask

Default

The default is None.

Command Mode

Interface Config

9-2 ip mroute

Configures an IPv4 Multicast Static Route for a specific source

The **no** command removes the configured IPv4 Multicast Static Route.

ip mroute *src-ip-addr src-mask rpf-ip-addr preference*

no ip mroute *src-ip-addr*

Parameters

src-ip-addr	The IP address of the multicast source network.
src-mask	The IP mask of the multicast data source.
rpf-ip-addr	The IP address of the Reverse port forwarding (RPF) next-hop router toward the source.
preference	The administrative distance for this Static MRoute, that is, the preference value The range is 1 to 255

Default

The default is not configured with any MRoute.

Command Mode

Global Config

9-3 ip multicast

Sets the administrative mode for the IP multicast forwarder in a router to active. This command is also used to enable the administrative mode of IPv6 multicast routing.

The **no** command sets the administrative mode for the IP multicast forwarder in a router to inactive.

ip multicast

no ip multicast

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

9-4 ip multicast ttl-threshold

This command is exclusive to IPv4 and is used to apply a given Time-to-Live threshold value to a specific routing interface or a range of interfaces. The **ttl-threshold** indicates the TTL threshold that is to be applied to those multicast Data packets that are forwarded from the interface or interfaces in question. Use of the command sets the Time-to-Live threshold value so that any data packets that are forwarded over the interface that have a TTL value above the configured value will be dropped.

The **no** command is used to apply the default ttl-threshold to a given routing interface. The ttl-threshold indicates the TTL threshold that is to be applied to those multicast Data packets that are forwarded from the interface in question.

ip multicast ttl-threshold *0-255*

no ip multicast ttl-threshold

Parameters

None

Default

The default is 1.

Command Mode

Interface Config

9-5 show ip mcast

Shows the multicast information for the whole system.

show ip mcast

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip mcast

Admin Mode..................................... Disabled
Protocol State................................. Non-Operational
Table Max Size ................................ 2048
Protocol....................................... No protocol enabled.
Multicast forwarding cache entry count ........ 0
```

Display Parameters

Admin Mode	The administrative status of multicast. Possible values are enabled or disabled.
Protocol State	The current state of the multicast protocol. Possible values are Operational or Non-Operational.
Table Max Size	The maximum number of entries allowed in the multicast table.
Protocol	The multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.
Multicast Forwarding Cache Entry Count	The number of entries in the multicast forwarding cache.

9-6 show ip mcast boundary

Shows all the administrative scoped multicast boundaries that are configured. The *slot /port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ip mcast boundary {*slot/port* **| vlan** *1-4093* **| all}**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan	Indicates an interface in VLAN format (1-4093).
all	Indicates all for all interfaces.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip mcast boundary 0/1

          MULTICAST BOUNDARY
Interface    Group IP          Mask
Ethernet1- -192.50.10.10----255.255.255.0—
```

Display Parameters

Interface	*slot/port*
Group Ip	Indicates the group IP address.
Mask	Indicates the group IP mask.

9-7 show ip mcast interface

Shows the multicast information for a specific interface. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ip mcast interface {*slot/port* **| vlan** *1-4093***}**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan *1-4093*	Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip mcast interface 4/10

Interface TTL
--------- -----
4/10      1
```

Display Parameters

Interface	*slot/port*
TTL	The time-to-live value for this interface.

9-8 show ip mroute

Shows a summary of or all of the details of the multicast table.

Note: This command supersedes any previous show ip mcast mroute command.

show ip mroute { detail | summary | group *group-address* **| source** *source address* **| static}**

Parameters

detail	Display the multicast routing table details.
group *group-address*	Display multicast routing table entries for specified group IP address.
source *source address*	Display multicast routing table entries for specified source IP address.
static	Display the static multicast routing table entries.
detail	Display the multicast routing table details.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the output for the summary parameter in the PIM Sparse mode.

```
(Routing)#show ip mroute summary

                            Multicast route table summary
Source IP        Group IP    Protocol     Incoming Interface   Outgoing Interface List
---------------  ----------  ----------   -------------------  -----------------------
192.168.10.1     225.1.1.1   PIMSM        V110                 V120, V130
```

The following is an example of the output for the detail parameter in the PIM Sparse mode.

```
IP Multicast Routing Table
Flags: C - Connected, J - Received Pim (*,G) Join,
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires Protocol: PIMSM
```

```
(*,22S.6.6.6)
00:00:41/000        RP: 1.1.1.1
Joins/Prunes: 0/0
Incoming interface:        RPF nbr: 0.0.0.0
Outgoing interface list:
4/1    00:00:00/218 Joins:        0      Flags: C

(*,22S.7.7.7)
00:00:36/000        RP: 1.1.1.1
Joins/Prunes: 0/0
Incoming interface:        RPF nbr: 0.0.0.0
Outgoing interface list:
4/1    00:00:36/224 Joins:        0      Flags: C

(3.3.3.11,225.6.6.6)
00:00:51/158        Flags: T
Joins/Prunes: 0/0          Reg/Reg-stop: 0/0
Incoming interface: 4/2    RPF nbr:3.3.3.11
Outgoing interface list:
4/1    00:00:41/000 Joins:        0

(3.3.3.11,225.7.7.7)
00:17:42/201        Flags: T
Joins/Prunes: 0/0          Reg/Reg-stop: 0/0
Incoming interface: 4/2    RPF nbr:3.3.3.11
Outgoing interface list:
4/1    00:00:36/000 Joins:        0
```

The following is an example of the output for the detail parameter in the PIM Dense mode in the event that a multicast routing protocol other than PIMSM is enabled.

```
(Routing)(Config)#show ip mroute detail

                              IP Multicast Routing Table
Source IP          Group IP     Expiry Time  Up Time      RPF Neighbor    Flags
                                 (hh:mm:ss)   (hh:mm:ss)
---------------    ----------   ----------   ----------   ----------      -----
192.168.10.1       225.1.1.1    00:02:45     05:37:09     192.168.20.5    SPT
```

The following is an example of the IPv6 output for the detail parameter in the PIM Sparse mode.

```
#show ipv6 mroute detail

IP Multicast Routing Table
Flags: C - Connected, J - Received Pim (*,G) Join,
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires Protocol: PIMSM

( *,ff43::3)
00:00:41/000        RP: 2001::1
Joins/Prunes: 0/0
```

```
Incoming interface:        RPF nbr:::
Outgoing interface list:
4/1    00:00:41/219 Joins:        0      Flags: C

( *,ff24::6)
00:00:22/000        RP: 2001::1
Joins/Prunes: 0/0
Incoming interface:        RPF nbr:::
Outgoing interface list:
4/1    00:00:41/219 Joins:        0      Flags: C

(3001::10,ff43::3)
00:00:07/203        Flags: T
Joins/Prunes: 0/0          Reg/Reg-stop: 0/0
Incoming interface: 4/2    RPF nbr: 3001::10
Outgoing interface list:
4/1    00:00:07/000 Joins:        0

(4001::33,ff22::3)
00:00:55/108        Flags: T
Joins/Prunes: 0/0          Reg/Reg-stop: 0/0
Incoming interface: 4/1    RPF nbr: 3001::10
Outgoing interface list:
4/2    00:00:66/000 Joins:        0

(3001::10,ff43::3)
00:00:07/203        Flags: T
Joins/Prunes: 0/0          Reg/Reg-stop: 0/0
Incoming interface: 4/1    RPF nbr: 3001::10
Outgoing interface list:
4/2    00:00:77/000 Joins:        0
```

The following is an example of the output for the group parameter in the PIM Sparse mode.

```
(U16)#show ip mroute group 229.10.0.1

IP Multicast Routing Table

Flags: C - Connected,J - Received PIM (*,G) Join,
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime(HH:MM:SS)/Expiry(SSS)
Protocol: PIMSM

(*, 229.10.0.1), 00:04;35/179, RP: 192.0.2.20
Joins/Prunes: 20/1
Incoming interface: Null, RPF Address: 0.0.0.0
Outgoing interface list:
       VLAN 6       00:00:30/150 Joins:15     Flags: C
       VLAN 5       00:04:35/150 Joins:10     Flags: C
       VLAN 2       00:01:28/0   Joins:20     Flags: J
```

```
(192.0.2.20, 229.10.0.1), 00:04:35/177, Flags: T
Joins/Prunes:20/1, Reg/Reg-Stop:100/0
Incoming interface: VLAN 2, RPF Address: 0.0.0.0
Outgoing interface list:
       VLAN 5        00:03:25/0    Joins:20
       VLAN 6        00:00:10/0    Joins:5
```

The following is an example of the output for the source parameter in the PIM Sparse mode.

```
(U16)#show ip mroute source 192:0.2.20

IP Multicast Routing Table

Flags: C - Connected,J - Received PIM (*,G) Join,
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime(HH:MM:SS)/Expiry(SSS)
Protocol: PIMSM

(192.0.2.20, 229.10.0.1), 00:04;35/177, Flags: T
Joins/Prunes:20/1, Reg/Reg-Stop:100/0
Incoming interface: VLAN 2, RPF Address: 0.0.0.0
Outgoing interface list:
       VLAN 5        00:03:25/0    Joins:20
       VLAN 6        00:00:10/0    Joins:5
```

Display Parameters

If the **detail**, **group**, or **source** parameters are used in the PIM Sparse mode, then the command will display the following fields:

Flags	• F: Register flag. Indicates that the source connected router is sending registers to RP. This flag can be seen only on Designated Router connected to source. • T: SPT-bit set. Indicates that packets have been received on the shortest path source tree. • R: RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This flag typically indicates a prune state along the shared tree for a particular source.
Outgoing interface flags	• C: Connected. A member of the multicast group is directly connected to the interface. • J: Received PIM (*,G) Join on this interface.
Timers:Uptime/Expiry	• Uptime: Indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. • Expires: Indicates per interface how long (in seconds) until the entry will be removed from the IP multicast routing table
Counters	• Joins: Indicates the number of (*,G) or (S,G) joins received for the given entry. • Prunes: Indicates the number of (*,G) or (S,G) prunes received for the given entry.

	• Registers: indicates the number of register messages received for the given (S,G) entry. • Register Stops: Indicates the number of register stop messages received for the given (S,G) entry.
RPF Address	Reverse path forwarding (RPF) IP address of the upstream router to the source.
Outgoing Interface List	List of outgoing interfaces.
Protocol	The current operating multicast routing protocol.
RP	Address of the Rendezvous Point (RP) router.
Incoming Interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.

If the **detail** parameter is used in any mode other than the PIM sparse mode, then the command will display the following fields:

Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If the **summary** parameter is used in the PIM Sparse mode, then the command will display the following fields:

Source IP	Source address of the multicast route entry.
Group IP	Group address of the multicast route entry.
Protocol	The current operating multicast routing protocol.
Incoming Interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
Outgoing Interface List	List of outgoing Interfaces.

If the **summary** parameter is used, then the command will display the following fields:

Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which the entry was created.
Incoming Interface	The interface on which the packet for the source/group arrives.
Outgoing Interface List	The list of outgoing interfaces on which the packet is forwarded

9-9 show ip mroute group

Shows the multicast configuration settings – including the flags, timer settings, RPF neighboring routers, incoming and outgoing interfaces, and expiration times – for all of the entries included in the multicast mroute table that contains the given groupipaddr.

show ip mroute group *groupipaddr* **{detail | summary}**

Parameters

groupipaddr	Indicates the given group IP address.
detail	Displays the multicast routing table details.
summary	Displays the multicast routing table summary.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this group arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

9-10 show ip mroute source

Shows the multicast configuration settings – including the flags, timer settings, RPF neighboring routers, incoming and outgoing interfaces, and expiration times – for all of the entries included in the multicast mroute table that contains the indicated source IP address or the source IP address and group IP address pair.

show ip mcast mroute source sourceipaddr {summary | *detail***}**

Parameters

summary	Display the multicast routing table summary.

groupipaddr	Indicates the source IP address.
detail	Display the multicast routing table details.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

If the groupipaddr parameter is used, then the following column headings will be displayed in the output table:

Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If the summary parameter is used, then the following column headings will be displayed in the output table:

Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this source arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

9-11 show ip mroute static

The show ip mcast mroute static command is used in the Privileged EXEC or User EXEC mode in order to show all the static routes that are configured in the static mcast table, in the event that it is specified, or to show the static route associated with the given sourceipaddr.

show ip mroute static [*sourceipaddr***]**

Parameters

sourceipaddr	(Optional) Indicates the source IP address.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip mroute static

                    MULTICAST STATIC ROUTES
Source IP          Source Mask     RPF Address     Preference
---------------    ----------      ----------      ----------
1.1.1.1            255.255.255.0   2 2 2.2         23
```

Display Parameters

Source IP	IP address of the multicast source network.
Source Mask	The subnetwork mask pertaining to the source IP.
RPF Address	The IP address of the RPF next-hop router toward the source.
Preference	The administrative distance for this Static MRoute.

9-12 clear ip mroute

Deletes all of the multicast route entries or specified IP multicast route entries.

Note: It should be noted that this command clears only dynamic mroute entries; static mroute entries will not be cleared by it.

clear ip mroute {* | *group-address* **[***source-address***]}**

Parameters

*****	Deletes all IPv4 entries from the IP multicast routing table.
group-address	IP address of the multicast group.
source-address	(Optional) The IP address of a multicast source that is sending multicast traffic to the group.

Default

The default is None.

Command Mode

Privileged EXEC

Example

Issuing the following command will delete all of the entries from the IP multicast routing table.

```
(Routing)#clear ip mroute *
```

Issuing the following command will delete all of the entries from the IP multicast routing table that match with the multicast group address provided (that is, 224.1 .2.1), regardless of which source is responsible for sending for this group.

```
(Routing)#clear ip mroute 224.1.2.1
```

Issuing the following command will delete all of the entries from the IP multicast routing table that match with the multicast group address provided (that is, 224.1.2.1) and the multicast source address provided (that is, 192.168.10.10).

```
(Routing)#clear ip mroute 224.1.2.1 192.168.10.10
```

DVMRP Commands

In this section, the Distance Vector Multicast Routing Protocol (DVMRP) commands are described.

9-13 ip dvmrp

Sets the administrative mode of the DVMRP in the router to the active mode.

The **no** command sets administrative mode of the DVMRP in the router the to inactive mode.

ip dvmrp

no ip dvmrp

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

9-14 ip dvmrp metric

Configures the metric for a specific interface or a range of interfaces. The value of the metric is used in the DVMRP messages to indicate the cost to reach this network.

The **no** command resets the metric for a specific interface back to the default value.

ip dvmrp metric *1-31*

no ip dvmrp metric

Parameters

None

Default

The default is 1.

Command Mode

lnterface Config

9-15 ip dvmrp trapflags

Enables the DVMRP trap mode.

The **no** command disables the DVMRP trap mode.

ip dvmrp trapflags

no ip dvmrp trapflags

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

9-16 ip dvmrp

Sets the administrative mode of the DVMRP on a single interface or a range of interfaces to the active mode.

The **no** command sets the administrative mode of the DVMRP on a single interface to the inactive mode.

ip dvmrp

no ip dvmrp

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

9-17 show ip dvmrp

Shows the system-wide information for the DVMRP.

show ip dvmrp

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show ip dvmrp

Admin Mode..................................... Disabled
Version........................................ 3
Total Number of Routes......................... 0
Reachable Routes .............................. 0

       DVMRP  INTERFACE STATUS

Interface    Interface Mode    Operational Status
----------   ---------------   --------------------
4/1          Disabled          Non-Operational
4/2          Disabled          Non-Operational
4/3          Disabled          Non-Operational
```

```
4/4           Disabled          Non-Operational
4/5           Disabled          Non-Operational
```

Display Parameters

Admin Mode	Indicates whether DVMRP is enabled or disabled.
Version String	The version of DVMRP being used.
Number of Routes	The number of routes in the DVMRP routing table.
Reachable Routes	The number of entries in the routing table with non-infinite metrics.

For each interface, the following fields are shown.

Interface	*slot/port*
Interface Mode	The mode of this interface. Possible values are Enabled and Disabled.
State	The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.

9-18 show ip dvmrp interface

Shows the interface information for the DVMRP on a specific interface. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ip dvmrp interface {*slot/port* **| vlan** *1-4093***}**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan	Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ip dvmrp interface 4/10

Interface Mode................................ Disabled
```

```
Interface Metric ............................. 1
Local Address ................................ 192.150.2.2
```

Display Parameters

Interface Mode	Indicates whether DVMRP is enabled or disabled on the specified interface.
Metric	Displays the specified value for the interface metric. The value range is between 1 to 32.
Local Address	The IP address of the interface.

The following field will be shown only when the DVMRP is operational on the interface in question.

Generation ID	The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

```
(Routing) )#show ip dvmrp interface 4/10

Interface Mode................................ Enabled
Interface Metric ............................. 1
Local Address ................................ 192.150.2.2
Received Bad Packets ......................... 0
Received Bad Routes .......................... 0
Sent Routes .................................. 0
```

The following fields will be shown only if the DVMRP is enabled on the interface in question.

Received Bad Packets	The number of invalid packets received.
Received Bad Routes	The number of invalid routes received.
Sent Routes	The number of routes that have been sent on this interface.

9-19 show ip dvmrp neighbor

Shows the neighbor information for the DVMRP.

show ip dvmrp neighbor

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

IfIndex	The value of the interface used to reach the neighbor.
Nbr IP Addr	The IP address of the DVMRP neighbor for which this entry contains information.
State	The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.
Up Time	The time since this neighboring router was learned.
Expiry Time	The time remaining for the neighbor to age out This field is not applicable if the State is DOWN.
Generation ID	The Generation ID value for the neighbor.
Major Version	The major version of DVMRP protocol of neighbor.
Minor Version	The minor version of DVMRP protocol of neighbor.
Capabilities	The capabilities of neighbor.
Received Routes	The number of routes received from the neighbor.
Rcvd Bad Pkts	The number of invalid packets received from this neighbor.
Rcvd Bad Routes	The number of correct packets received with invalid routes.

9-20 show ip dvmrp nexthop

Shows the next hop information for routing multicast datagrams on outgoing interfaces.

show ip dvmrp nexthop

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Source IP	The sources for which this entry specifies a next hop on an outgoing interface.
Source Mask	The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.
Next Hop Interface	The interface in slot/port format for the outgoing interface for this next hop.
Type	The network is a LEKF or a BRANCH.

9-21 show ip dvmrp prune

Shows a table in which the router's upstream prune information is listed.

show ip dvmrp prune

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Group IP	The multicast Address that is pruned.
Source IP	The IP address of the source that has pruned.
Source Mask	The network Mask for the prune source. Mask is defined by 1s or a of prune source and mask matching.
Expiry Time (secs)	The expiry time in seconds. This is the time remaining for this prune to age out.

9-22 show ip dvmrp route

Shows the multicast routing information for the DVMRP.

show ip dvmrp route

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Source Address	The multicast address of the source group.
Source Mask	The IP Mask for the source group.
Upstream Neighbor	The IP address of the neighbor which is the source for the packets for a specified multicast address.
Interface	The interface used to receive the packets sent by the sources.
Metric	The distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.
Expiry Time (secs)	The expiry time in seconds, which is the time left for this route to age out.
Up Time (secs)	The time when a specified route was learnt, in seconds.

PIM Commands

In this section, the commands used to configure the Protocol Independent Multicast -Dense Mode (PIM-DM) and the Protocol Independent Multicast - Sparse Mode (PIM-SM) are described. The PIM-DM and PIM-SM consist of multicast routing protocols that provide scalable inter-domain multicast routing via the Internet, that is, independent of any mechanisms utilized by a particular unicast routing protocol. Only one PIM mode may be in operation at a given time.

9-23 ip pim dense

Enables the PIM Dense mode across the router administratively.

The **no** command administratively disables the PIM Dense mode across the router.

ip pim dense

no ip pim dense

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

Example

The following provides an example of the command.

```
(Routing)(Config)#ip pim dense
```

9-24 ip pim sparse

Enables the PIM Sparse mode across the router administratively.

The **no** command administratively disables the PIM Sparse mode across the router.

ip pim sparse

no ip pim sparse

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

Example

The following provides an example of the command.

```
(Routing)(Config)#ip pim sparse
```

9-25 ip pim

Enables PIM on a specific interface administratively.

The **no** command administratively disables PIM on the interface in question.

ip pim

no ip pim

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

Example

The following is an example of the CLI display output for the command.

```
(Routing)(Interface 9/1)#ip pim
```

9-26 ip pim hello-interval

Configures the transmission frequency of PIM hello messages on a specific interface.

The **no** command resets the transmission frequency of hello messages between neighbors enabled for PIM back to the default value.

ip pim hello-interval *0-18000*

no ip pim hello-interval

Parameters

None

Default

The default is 30 seconds.

Command Mode

Interface Config

Example

The following provides an example of the command.

```
(Routing)(Interface 0/1)#ip pim hello-interval 50
```

9-27 ip pim bsr-border

Prevents bootstrap router (BSR) messages from being transmitted or received on a specific interface.

The **no** command disables a specific interface from acting as the BSR border.

Note: Only when the Sparse mode is enabled in the Global mode will this command take effect.

ip pim bsr-border

no ip pim bsr-border

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

Example

The following provides an example of the command.

```
(Routing)(Interface 0/1)#ip pim bsr-border
```

9-28 ip pim bsr-candidate

Configures the router so that it will announce its candidacy to serve as a bootstrap router (BSR). The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

The **no** command removes the configured PIM Candidate BSR router.

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ip pim bsr-candidate interface {*slot/port* **| vlan** *1-4093***}** *hash-mask-length* **[***bsr-priority***] [interval** *interval***]**

no ip pim bsr-candidate interface {*slot/port* **| vlan** *1-4093***}**

Parameters

slot/port	Interface number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with PIM.
vlan *1-4093*	Indicates an interface in VLAN format (1-4093).
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
bsr-priority	(Optional) Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

interval *interval*	(Optional) Indicates the BSR candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Default

The default is Disabled.

Command Mode

Global Config

Example

The following are examples of the command.

```
(Routing)(Config)#ip pim bsr-candidate interface 0/1 32 5

(Routing)(Config)#ip pim bsr-candidate interface 0/1 32 5 interval 100
```

9-29 ip pim dr-priority

Sets the priority value determining when a given router is selected as the designated router (DR).

The **no** command resets the DR Priority of the specified interface back to its default value.

Note: Only when the Sparse mode is enabled in the Global mode will this command take effect.

ip pim dr-priority *0-2147483647*

no ip pim dr-priority

Parameters

None

Default

The default is 1.

Command Mode

Interface Config

Example

The following is an example of the CLI display output for the command.

```
(Routing)(Interface 0/1)#ip pim dr-priority 10
```

9-30 ip pim join-prune-interval

Configures the frequency with which PIM Join/Prune messages are sent on a specific interface. The length of the join/prune interval is specified in seconds.

The **no** command resets the length of the join/prune interval on the given interface back to the default value.

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ip pim join-prune-interval *0-18000*

no ip pim join-prune-interval

Parameters

None

Default

The default is 60.

Command Mode

Interface Config

Example

The following provides an example of the command.

```
(Routing)(Interface 0/1)#ip pim join-prune-interval 90
```

9-31 ip pim rp-address

Defines the address, for a specific multicast group range, of a PIM Rendezvous point (RP).

The **no** command removes the address, for the specified multicast group range, of the configured PIM Rendezvous point (RP).

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ip pim rp-address *rp-address group-address group-mask* **[override]**

no ip pim rp-address *rp-address group-address group-mask* **[override]**

Parameters

rp-address	The IP address of the RP.
group-address	The group address supported by the RP.
group-mask	The group mask for the group address.
override	(Optional) Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Default

The default is 0.

Command Mode

Global Config

Example

The following provides an example of the command.

```
(Routing)(Config)#ip pim rp-address 192.168.10.1

  224.1.2.0 255.255.255.0
```

9-32 ip pim rp-candidate

Configures a router to advertise itself to the bootstrap router (BSR) as a PIM candidate rendezvous point (RP) for a specified multicast group range. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

The **no** command removes the configured PIM candidate Rendezvous point (RP) for the given multicast group range.

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ip pim rp-candidate interface {*slot/port* **| vlan** *1-4093***}** *group-address group-mask* **[interval** *interval***]**

no ip pim rp-candidate interface {*slot/port* **| vlan** *1-4093***}** *group-address group-mask*

Parameters

slot/port	The IP address associated with this interface type and number is advertised as a candidate RP address. This interface must be enabled with PM.
vlan *1-4093*	Indicates an interface in VLAN format (1-4093).
group-address	The multicast group address that is advertised in association with the RP address.
group-mask	The multicast group prefix that is advertised in association with the RP address.
interval *interval*	(Optional) Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Default

The default is Disabled.

Command Mode

Global Config

Example

The following are examples of the command.

```
(Routing)(Config)#ip pim rp-candidate interface 0/1 224.1.2.0 255.255.255.0
```

```
(Routing)(Config)#ip pim rp-candidate interface 0/1 224.1.2.0 Z55.255.255.0 interval
200
```

9-33 ip pim ssm

Defines the range of Source Specific Multicast (SSM) IP multicast addresses for the router.

The **no** command removes the range of Source Specific Multicast (SSM) IP multicast addresses for the router.

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ip pim ssm {default | *group-address group-mask***}**

no ip pim ssm {default | *group-address group-mask***}**

Parameters

default	Defines the SSM range access list to 232/8.
group-address	Defining the SSM Range.
group-mask	Indicates the defined SSM Range.

Default

The default is Disabled.

Command Mode

Global Config

Example

The following are examples of the command.

```
(Routing)(Config)#ip pim ssm default
```

```
(Routing)(Config)#ip pim ssm 232.1.2.0 255.255.255.0
```

9-34 ip pim-trapflags

Enables the PIM trap mode for both the Dense Mode (DM) and the Sparse Mode (SM).

The **no** command resets the PIM trap mode back to the default.

ip pim-trapflags

no ip pim-trapflags

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

9-35 show ip mfc

Shows mroute entries in the multicast forwarding (MFC) database.

show ip mfc

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

```
(Routing)(Config)#show ip mfc

MFC IPv4 Mode..................................... Enabled
MFC IPv6 Mode..................................... Disabled
MFC Entry Count................................... 1
Current multicast IPv4 protocol.................. PIMSM
Current multicast IPv6 protocol.................. No protocol enabled.
Total software forwarded packets................. 0

Source address: 192.168.10.5
Group address: 225.1.1.1
Packets forwarded in software for this entry: 0      Protocol: PIM-SM
Expiry Time (secs): 206          Up Time (secs): 4
Incoming interface: 1/0/10       Outgoing interface list: None
```

Display Parameters

MFC IPv4 Mode	Enabled when IPv4 Multicast routing is operational.

MFC IPv6 Mode	Enabled when IPv6 Multicast routing is operational.
MFC Entry Count	The number of entries present in MFC.
Current multicast IPv4 Protocol	The current operating IPv4 multicast routing protocol.
Current multicast IPv6 Protocol	The current operating multicast IPv6 routing protocol.
Total Software Forwarded packets	Total Number of multicast packets forwarded in software.
Source Address	Source address of the multicast route entry.
Group Address	Group address of the multicast route entry.
Packets Forwarded in Software for this entry	Number of multicast packets that are forwarded in software for a specific multicast route entry,
Protocol	Multicast Routing Protocol that has added a specific entry.
Expiry Time (secs)	Expiry time for a specific Multicast Route entry in seconds.
Up Time (secs)	Up Time in seconds for a specific Multicast Routing entry.
Incoming interface	Incoming interface for a specific Multicast Route entry.
Outgoing interface list	Outgoing interface list for a specific Multicast Route entry.

9-36 show ip pim

Shows the system-wide information for the PIM-DM or the PIM-SM.

show ip pim

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

PIM Mode - Dense

```
(Routing)#show ip pim

PIM Mode      Dense
```

```
Interface    Interface Mode       Operational Status
----------   ---------------      --------------------
0/1          Enabled              Operational
0/3          Disabled             Non-Operational
```

PIM Mode - Sparse

```
(Routing)#show ip pim

PIM Mode      Sparse

Interface    Interface Mode       Operational Status
----------   ---------------      --------------------
0/1          Enabled              Operational
0/3          Disabled             Non-Operational
```

PIM Mode - None

```
(Routing)#show ip pim

PIM Mode      None

None of the routing interfaces are enabled for PIM.
```

Display Parameters

Note: Some of the fields in the following table will not be displayed in the command output if the PIM mode is the PIM-DM (dense) because they are applicable only to the PIM-SM.

PIM Mode	Indicates the configured mode of the PIM protocol as dense (PIM-DM) or sparse (PIM-SM).
Interface	*slot/port*
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

9-37 show ip pim ssm

Shows the configured source specific IP multicast addresses. The ouput of the command will read **No SSM address range is configured** if no SSM Group range has been configured.

show ip pim ssm

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip pim ssm

Group Address/Prefix Length
------------------------------
232.0.0.0/8
```

If an SSM Group range is not configured, the following message will be displayed:

```
No SSM address range is configured.
```

Display Parameters

Group Address	The IP multicast address of the SSM group.
Prefix Length	The network prefix length.

9-38 show ip pim interface

Shows the status parameters of the PIM interface. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. If an interface is not specified, then the command shows the status parameters for all PIM-enabled interfaces.

show ip pim interface [{*slot/port* **| vlan** *1-4093***}]**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan *1-4093*	Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip pim interface

Interface.....................................0/1
       Mode.....................................Sparse
       Hello Interval (secs).....................30
       Join Prune Interval (secs).................60
       DR Priority...............................1
       BSR Border................................Disabled
       Neighbor Count............................1
       Designated Router.........................192.168.10.1

Interface.....................................0/2
       Mode.....................................Sparse
       Hello Interval (secs).....................30
       Join Prune Interval (secs).................60
       DR Priority...............................1
       BSR Border................................Disabled
       Neighbor Count............................1
       Designated Router.........................192.168.10.1
```

The following message will be displayed if no interfaces are enabled for PIM:

```
None of the routing interfaces are enabled for PIM.
```

Display Parameters

Interface	*slot/port*. The interface number.
Mode	Indicates the active PIM mode enabled on the interface is dense or sparse.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. The default is 30 seconds.
Join Prune Interval	The join/prune interval value for the PIM router. The interval is in seconds.
DR Priority	The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense.
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface.
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense.

9-39 show ip pim neighbor

Shows the PIM neighbors discovered by PIMv2 Hello messages. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. If an interface is not specified, then the command shows the status parameters for all PIM-enabled interfaces.

show ip pim neighbor [{*slot/port* **| vlan** *1-4093***}]**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan *1-4093*	Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip pim neighbor 0/1

Neighbor Addr   Interface    Uptime (hh:mm:ss)  Expiry Time (hh:mm:ss)    DR Priority
-------------   ----------   -----------------  ----------------------    ------------
192.168.10.2    0/1          00:02:55           00:01:15                  NA
```

```
(Routing)#show ip pim neighbor

Neighbor Addr   Interface    Uptime (hh:mm:ss)  Expiry Time (hh:mm:ss)    DR Priority
-------------   ----------   -----------------  ----------------------    ------------
192.168.10.2    0/1          00:02:55           00:01:15                  1
192.168.20.2    0/2          00:03:50           00:02:10                  1
```

The following message will be displayed if no neighbors have been learned by any of the interfaces:

```
No neighbors exist on the router.
```

Display Parameters

Neighbor Addr	The IP address of the PIM neighbor on an interface.
Interface	*slot/port*
Up Time (hh:mm:ss)	The time since this neighbor has become active on this interface.

Expiry Time (hh:mm:ss)	Time remaining for the neighbor to expire.
DR Priority	The DR Priority configured on this Interface (PIM-SM only). **Note:** DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

9-40 show ip pim bsr-router

Shows the bootstrap router (BSR) information.

show ip pim bsr-router {candidate | elected}

Parameters

candidate	Indicates a PIM BSR Candidate table information.
elected	Indicates a PIM BSR Elected table information.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip pim bsr-router elected

BSR Address..................................... 192.168.10.1
     BSR Priority ............................. 0
     BSR Hash Mask Length ..................... 30
     Next Bootstrap message (hh:mm:ss ......... 00:00:24
```

```
(Routing)#show ip pim bsr-router candidate

BSR Address..................................... 192.168.10.1
     BSR Priority ............................. 0
     BSR Hash Mask Length ..................... 30
     C-BSR Advertisement Interval (secs) ..... 60
     Next Bootstrap message (hh:mm:ss) ........ NA
```

The following message will be displayed if no selected or configured BSRs exist on the router:

```
No BSR's exist/learned on this router.
```

Display Parameters

BSR Address	IP address of the BSR.
BSR Priority	Priority as configured in the ip pim bsr-candidate command.
BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the ip pim bsr-candidate command.
C-BSR Advertisement Interval	Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

9-41 show ip pim rp-hash

Shows the rendezvous point (RP) that has been selected for the group address specified.

show ip pim rp-hash *group-address*

Parameters

group-address	Indicates a group address.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip pim rp-hash 224.1.2.0

RP Address192.168.10.1
     Type Static
```

The following message will be displayed if no RP Group mapping exists on the router:

```
No RP-Group mappings exist/learned on this router.
```

Display Parameters

RP Address	The IP address of the RP for the group specified.
Type	Indicates the mechanism (BSR or static) by which the RP was selected.

9-42 show ip pim rp mapping

For the PIM group, shows the mapping to the active Rendezvous points (RP) that the router is aware of (whether they were configured or learned from the bootstrap router (BSR)). The optional parameters can be used to limit the information displayed to a specific RP address or in order to view group-to-candidate RP or group-to-Static RP mapping information.

show ip pim rp mapping [{*rp-address* **| candidate | static}]**

Parameters

rp-address	(Optional) Indicates an RP Address.
candidate	(Optional) Indicates a group to Candidate RP mapping info.
static	(Optional) Indicates a group to Static RP mapping info.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following are examples of the CLI display output for the command.

```
(Routing)#show ip pim rp mapping 192.168.10.1

RP Address                    192.168.10.1
     Group Address            224.1.2.1
     Group Mask               255.255.255.0
     Origin                   Static
```

```
(Routing)#show ip pim rp mapping

RP Address                    192.168.10.1
     Group Address            224.1.2.1
     Group Mask               255.255.255.0
     Origin                   Static

RP Address                    192.168.20.1
```

```
     Group Address           229.2.0.0
     Group Mask              255.255.0.0
     Origin                  Static
```

```
(Routing)#show ip pim rp mapping candidate

RP Address..................................... 192.168.10.1
     Group Address ............................ 224.1.2.1
     Group Mask ............................... 255.255.0.0
     Origin ................................... BSR
     C-RP Advertisement Interval (secs) ....... 60
     Next Candidate RP Advertisement(hh:mm:ss) .. 00:00:15
```

The following message will be displayed if no RP Group mapping exists on the router:

```
No RP-Group mappings exist on this router.
```

Display Parameters

RP Address	The IP address of the RP for the group specified.
Group Address	The IP address of the multicast group.
Group Mask	The subnet mask associated with the group.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.
C-RP Advertisement Interval	Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.
Next Candidate RP Advertisement (hh:mm:ss)	Indicates the time (hours, minutes, and seconds) in which the next C-RP Advertisement is due from this device.

9-43 show ip pim statistics

Shows statistics regarding the PIM control packets received per interface, but only if the PIM sparse mode is enabled.

show ip pim statistics

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

```
(Routing)#show ip pim statistics

================================================================================================
Interface    Stat    Hello   Register   Reg-Stop   Join/Pru   BSR     Assert     CRP
================================================================================================
Vl10         Rx      0       0          0          0          0       0          0
             Tx      2       0          0          0          0       0          0

       Invalid Packets Received - 0
------------------------------------------------------------------------------------------------
Vl20         Rx      0       0          0          5          0       0          0
             Tx      8       7          0          0          0       0          0

       Invalid Packets Received - 0
------------------------------------------------------------------------------------------------
1/0/5        Rx      0       0          6          5          0       0          0
             Tx      10      9          0          0          0       0          0

Invalid Packets Received - 0
------------------------------------------------------------------------------------------------
```

```
(Routing)#show ip pim statistics vlan 10

================================================================================================
Interface    Stat    Hello   Register   Reg-Stop   Join/Pru   BSR     Assert     CRP
================================================================================================
Vl10         Rx      0       0          0          0          0       0          0
             Tx      2       0          0          0          0       0          0

       Invalid Packets Received - 0
------------------------------------------------------------------------------------------------
```

```
(Routing)#show ip pim statistics 1/0/5

================================================================================================
Interface    Stat    Hello   Register   Reg-Stop   Join/Pru   BSR     Assert     CRP
================================================================================================
1/0/5        Rx      0       0          6          5          0       0          0
             Tx      10      9          0          0          0       0          0

Invalid Packets Received - 0
------------------------------------------------------------------------------------------------
```

Note: Use the key word IPv6 for IPv6 statistics.

Display Parameters

Stat	• Rx: Packets received • Tx: Packets transmitted
Interface	The PIM-enabled routing interface.
Hello	The number of PIM Hello messages.
Register	The number of PIM Register messages.
Reg-Stop	The number of PIM Register-stop messages.
Join/Pru	The number of PIM Join/Prune messages.
BSR	The number of PIM Boot Strap messages.
Assert	The number of PIM Assert messages.
CRP	The number of PIM Candidate RP Advertisement messages.

Internet Group Message Protocol Commands

In this section, the commands use to view and configure Internet Group Message Protocol (IGMP) settings are described.

9-44 ip igmp

Sets the administrative mode for IGMP on a single interface, range of interfaces, or all interfaces in the system to active.

The **no** command sets the administrative mode for IGMP in the system to inactive.

ip igmp

no ip igmp

Parameters

None

Default

The default is Disabled.

Command Mode

- Global Config
- Interface Config

9-45 ip igmp version

Configures the version of IGMP used for a single interface or a range of interfaces. The value for the *version* parameter must be 1, 2, or 3.

The **no** command resets the version of IGMP used to the default value.

ip igmp version *version*

no ip igmp version

Parameters

version	Indicates the IGMP or IGMP proxy version (1-3).

Default

The default is 3.

Command Mode

Interface Config

9-46 ip igmp last-member-query-count

Sets the number of Group-Specific Queries sent out by a given interface or a range of interfaces before the router assumes that no local members are present on the interface.

The **no** command resets the number of Group-Specific Queries back to the default value.

ip igmp last-member-query-count *1-20*

no ip igmp last-member-query-count

Parameters

None

Default

The default is None.

Command Mode

Interface Config

9-47 ip igmp last-member-query-interval

Configures the Maximum Response Time for Group-Specific Queries that are sent in response to Leave Group messages. The Maximum Response Time value can be configured for a single interface or a range of interfaces.

The **no** command resets the Maximum Response Time back to the default value.

ip igmp last-member-query-interval *0-255*

no ip igmp last-member-query-interval

Parameters

None

Default

The default is 1 second.

Command Mode

Interface Config

9-48 ip igmp query-interval

Configures the query interval for a single interface or a range of interfaces. The query interval defines the frequency with which IGMP Host-Query packets are transmitted on the given interface.

The **no** command resets the query interval for the given interface back to the default value.

ip igmp query-interval *1-3600*

no ip igmp query-interval

Parameters

None

Default

The default is 125 seconds.

Command Mode

Interface Config

9-49 ip igmp query-max-response-time

Configures the length of the maximum response time interval, which is the maximum query response time advertised in IGMPv2 queries, for a single interface or a range of interfaces. The length of the interval is specified in tenths of a second.

The **no** command resets the maximum response time interval for the specified interface back to the default value.

ip igmp query-max-response-time *0-255*

no ip igmp query-max-response-time

Parameters

None

Default

The default is 100 tenths of a second.

Command Mode

Interface Config

9-50 ip igmp robustness

Configures the robustness, which is the tuning for the expected packet loss on a subnet, for an interface or a range of interfaces. The Robustness variable for an interface may be increased if a subnet is expected to have a lot of loss.

The **no** command resets the robustness value back to the default value.

ip igmp robustness *2-255*

no ip igmp robustness

Parameters

None

Default

The default is 2.

Command Mode

Interface Config

9-51 ip igmp startup-query-count

Sets the number of Queries that are sent out upon startup, with the time between individual queries determined by the Startup Query Interval on the given interface or range of interfaces.

The **no** command resets the number of Queries that are sent out upon startup back to the default value.

ip igmp startup-query-count *1-20*

no ip igmp startup-query-count

Parameters

None

Default

The default is 2.

Command Mode

Interface Config

9-52 ip igmp startup-query-interval

Sets the interval between General Queries that are sent upon startup of a single interface or a range of interfaces. The value of the time interval value is given in seconds.

The **no** command resets the interval between General Queries that are sent upon startup of the interface back to the default value.

ip igmp startup-query-interval *1-300*

no ip igmp startup-query-interval

Parameters

None

Default

The default is 31.7.

Command Mode

Interface Config

9-53 show ip igmp

Shows the system-wide IGMP information.

show ip igmp

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ip igmp

IGMP admin mode................................ Disabled
IGMP header validation......................... Disabled

    IGMP INTERFACE STATUS

Interface      Interface Mode      Operational Status
----------     ---------------     --------------------
0/2            Disabled            Non-Operational
Vlan10         Disabled            Non-Operational
Vlan20         Disabled            Non-Operational
Vlan30         Disabled            Non-Operational
```

Display Parameters

IGMP Admin Mode	Displays the status of the IGMP admin mode: enabled or disabled.
IGMP Header Validation	Indicates if the function is enabled/disabled for header validation for all IGMP messages.
Interface	*slot/port*
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface.
Operational-Status	The current state of IGMP on this interface Possible values are Operational or Non-Operational.

9-54 show ip igmp groups

Shows the multicast groups registered on the interface. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. If the **[detail]** parameter is specified, then the command displays the multicast groups registered on the interface in detail.

show ip igmp groups {*slot/port* **| vlan** *1-4093* **[detail]}**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan	Indicates an interface in VLAN format (1-4093).
detail	(Optional) Indicates details of subscribed multicast groups.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip igmp groups

IP Address..................................... 225.1.1.1
Subnet Mask.................................... 255.255.255.255
Interface Mode................................. Enabled
Querier Status................................. Non-Querier
```

Display Parameters

If the detail keyword is not used, then the following fields are shown.

IP Address	The IP address of the interface participating in the multicast group.
Subnet Mask	The subnet mask of the interface participating in the multicast group.
Interface Mode	This displays whether IGMP is enabled or disabled on this interface.

If the interface is not enabled, then the following fields are not shown.

Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	The list of multicast groups that are registered on this interface.

If the detail keyword is used, then the following fields are shown.

Multicast IP Address	The IP address of the registered multicast group on this interface.
Last Reporter	The IP address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	The time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	The amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or “-----” if there is no Version 1 host present.
Version2 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or “-----” if there is no Version 2 host present.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

9-55 show ip igmp interface

Shows the IGMP information for the given interface. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ip igmp interface {*slot/port* **| vlan** *1-4093***}**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan *1-4093*	Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show ip igmp interface 4/10

Interface..................................... Vlan10
IP address.................................... 192.150.2.2
Subnet mask................................... 255.255.255.0
IGMP admin mode............................... Disabled
Interface Mode................................ Disabled
IGMP Version.................................. 3
Query Interval (secs)......................... 125
Query Max Response Time(1/10 th of a sec) ..... 100
Robustness.................................... 2
Startup Query Interval (secs) ................. 31
Startup Query Count........................... 2
Last Member Query Interval (1/10 of a second).. 10
Last Member Query Count....................... 2
```

Display Parameters

Interface	*slot/port*
IGMP Admin Mode	The administrative status of IGMP.
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface.

IGMP Version	The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.
Query Interval	The frequency at which IGMP Host-Query packets are transmitted on this interface.
Query Max Response Time	The maximum query response time advertised in lGMPv2 queries on this interface.
Robustness	The tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface.
Startup Query Interval	The interval between General Queries sent by a Querier on startup.
Startup Query Count	The number of Queries sent out on startup, separated by the Startup Query lnterval.
Last Member Query Interval	The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	The number of Group-Specific Queries sent before the router assumes that there are no local members.

9-56 show ip igmp interface membership

Shows the list of interfaces that have been registered in the multicast group.

show ip igmp interface membership *multiipaddr* **[detail]**

Parameters

multiipaddr	Indicates a multicast IP address.
detail	(Optional) Indicates details of subscribed multicast groups.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Interface	Valid slot and port number separated by forward slashes.
Interface IP	The IP address of the interface participating in the multicast group.
State	The interface that has IGMP in Querier mode or Non-Querier mode.

Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

If the detail keyword is used, then the following fields are shown:

Interface	Valid slot and port number separated by forward slashes.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Source Hosts	The list of unicast source IP addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP address. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Expiry Time	The amount of time remaining to remove this entry before it is aged out. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

9-57 show ip igmp interface stats

Shows the IGMP statistical information for the given interface. The statistics are shown only if the interface is enabled for IGMP. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ip igmp interface stats [*slot/port* **| vlan** *1-4093***]**

Parameters

slot/port	(Optional) Indicates an interface in slot/port format.
vlan	(Optional) Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Querier Status	The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.

Querier IP Address	The IP address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	The time since the interface Querier was last changed.
Querier Expiry Time	The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.
Wrong Version Queries	The number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Groups	The current number of membership entries for this interface.

IGMP Proxy Commands

The IGMP Proxy is utilized by the IGMP Router (i.e., the IPv4 system) to enable the system to send out IGMP host messages on behalf of those hosts that the system has discovered via standard IGMP router interfaces. When the IGMP Proxy is enabled, the system will behave as a proxy for all of the hosts residing on its router interfaces.

9-58 ip igmp-proxy

Enables the IGMP Proxy on a single interface or a range of interfaces. Multicast forwarding must be enabled in order to enable the IGMP Proxy on an interface. Also, the user must ensure that no multicast routing protocols are enabled on the router.

The **no** command is used to disable the IGMP Proxy on the router.

ip igmp-proxy

no ip igmp-proxy

Parameters

None

Default

The default is None.

Command Mode

Interface Config

9-59 ip igmp-proxy unsolicit-rprt-interval

Sets the length of the unsolicited report interval for the given IGMP Proxy interface or a range of interfaces. The command is only valid when the user has enabled the IGMP Proxy on the given interface or range of interfaces.

The **no** command resets the length of the unsolicited report interval for the IGMP Proxy router back to the default value.

ip igmp-proxy unsolicit-rprt-interval *1-260*

no ip igmp-proxy unsolicit-rprt-interval

Parameters

None

Default

The default is 1.

Command Mode

Interface Config

9-60 ip igmp-proxy reset-status

Resets the host interface status parameters for the given IGMP Proxy interface (or for a range of interfaces). The command is only valid when the user has enabled the IGMP Proxy on the interface.

ip igmp-proxy reset-status

Parameters

None

Default

The default is None.

Command Mode

Interface Config

9-61 show ip igmp-proxy

Shows a summary of the host interface status parameters. The command will cause the following parameters to be displayed only when the user has enabled the IGMP Proxy.

show ip igmp-proxy

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show igmp-proxy

Interface Index.................................. 0/1
Admin Mode....................................... Enable
Operational Mode................................. Enable
Version.......................................... 3
Num of Multicast Groups.......................... 0
Unsolicited Report Interval...................... 1
Querier IP Address on Proxy Interface............ 5.5.5.50
Older Version 1 Querier Timeout.................. 0
Older Version 2 Querier Timeout.................. 00::00:00
Proxy Start Frequency............................ 1
```

Display Parameters

Interface Index	The interface number of the IGMP Proxy.
Admin Mode	States whether the IGMP Proxy is enabled or disabled.
Operational Mode	States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.
Version	The present IGMP host version that is operational on the proxy interface.
Num of Multicast Groups	The number of multicast groups that are associated with the IGMP Proxy interface.
Unsolicited Report Interval	The time interval at which the IGMP Proxy interface sends unsolicited group membership report.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Older Version 2 Querier Timeout	The interval used to timeout the older version 2 queriers.
Proxy Start Frequency	The number of times the IGMP Proxy has been stopped and started.

9-62 show ip igmp-proxy interface

Shows a detailed list of information regarding the host interface status parameters. The command will cause the following parameters to be displayed only when the user has enabled the IGMP Proxy.

show ip igmp-proxy interface

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip igmp-proxy interface

Interface Index................................. 0/1


Ver     Query Rcvd      Report Rcvd     Report Sent     Leave Rcvd      Leave Sent
-----   ------------    ------------    ------------    ------------    -------------
1       0               0               0               -----           -----
2       0               0               0               0               0
3       0               0               0               -----           -----
```

Display Parameters

Interface Index	The *slot/port* of the IGMP proxy.

The column headings within the table providing information about the interface are the following:

Ver	The IGMP version.
Query Rcvd	Number of IGMP queries received.
Report Rcvd	Number of IGMP reports received.
Report Sent	Number of IGMP reports sent.
Leaves Rcvd	Number of IGMP leaves received. Vallid for version 2 only.
Leaves Sent	Number of IGMP leaves sent on the Proxy interface. Valid for version 2 only.

9-63 show ip igmp-proxy groups

Shows information regarding the subscribed multicast groups that the IGMP Proxy has reported. The command will cause a table of entries with the following parameters given as the fields of each column to be displayed.

show ip igmp-proxy groups

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip igmp-proxy groups

Interface Index................................. 0/1

Group Address   Last Reporter   Up Time      Member State    Filter Mode     Sources
-------------   -------------   ----------   -------------   ------------    ----------
225.4.4.4       5.5.5.48        00:02:21     DELAY_MEMBER    Include         3
226.4.4.4       5.5.5.48        00:02:21     DELAY_MEMBER    Include         3
227.4.4.4       5.5.5.48        00:02:21     DELAY_MEMBER    Exclude         0
228.4.4.4       5.5.5.48        00:02:21     DELAY_MEMBER    Include         3
```

Display Parameters

Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group on the network attached to the IGMP Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER • IDLE_MEMBER – interface has responded to the latest group membership query for this group. • DELAY_MEMBER – interface is going to send a group membership report to respond to a group membership query for this group.

Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.

9-64 show ip igmp-proxy groups detail

Shows complete information regarding the multicast groups that the IGMP Proxy has reported. The command will cause a table of entries with the following parameters given as the fields of each column to be displayed.

show ip igmp-proxy groups detail

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ip igmp-proxy groups

Interface Index................................ 0/1

Group Address   Last Reporter   Up Time      Member State    Filter Mode     Sources
-------------   -------------   ----------   -------------   ------------    ----------
225.4.4.4       5.5.5.48        00:02:21     DELAY_MEMBER    Include         3

Group Source List       Expiry Time
--------------------    ---------------
5.1.2.3                 00:02:21
6.1.2.3                 00:02:21
7.1.2.3                 00:02:21

Group Address   Last Reporter   Up Time      Member State    Filter Mode     Sources
-------------   -------------   ----------   -------------   ------------    ----------
226.4.4.4       5.5.5.48        00:02:21     DELAY_MEMBER    Include         3

Group Source List       Expiry Time
--------------------    ---------------
2.1.2.3                 00:02:21
6.1.2.3                 00:01:44
```

```
8.1.2.3                 00:01:44

Group Address   Last Reporter   Up Time      Member State    Filter Mode     Sources
-------------   -------------   ----------   -------------   ------------    ----------
227.4.4.4       5.5.5.48        00:02:21     DELAY_MEMBER    Exclude         0
228.4.4.4       5.5.5.48        00:03:21     DELAY_MEMBER    Include         3

Group Source List       Expiry Time
--------------------    ---------------
9.1.2.3                 00:03:21
6.1.2.3                 00:03:21
7.1.2.3                 00:03:21
```

Display Parameters

Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group, on the network attached to the IGMP-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. • IDLE_MEMBER – interface has responded to the latest group membership query for this group. • DELAY_MEMBER – interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	Time left before a source is deleted.

10. IPv6 Multicast Commands

In this chapter, the IPv6 Multicast commands available in the D-LINK OS CLI are described.

The commands described in this chapter belong to one of the three following functional groups:

- Show commands, which are commands that cause switch settings, statistics, and other information to be displayed
- Configuration commands, which are commands that cause the features and options of the given switch to be configured. For every configuration command, there is a corresponding show command that can be used to display the configuration setting.
- Clear commands, which are commands that cause some or all of the settings to be reset to factory defaults.

IPv6 Multicast Forwarder

10-1 ipv6 mroute

Configures an IPv6 Multicast Static Route for a source.

The **no** command removes the configured IPv6 Multicast Static Route.

ipv6 mroute *src-ip-addr src-mask rpf-addr* **[interface]** *preference*

no ipv6 mroute *src-ip-addr*

Parameters

src-ip-addr	The IP address of the multicast source network.
src-mask	The IP mask of the multicast data source.
rpf-addr	The IP address of the RPF next-hop router toward the source.
interface	(Optional) Specify the interface if the RPF Address is a link-local address.
preference	The administrative distance for this Static MRoute, that is, the preference value. The range is 1 to 255.

Default

The default is not configured with any MRoute.

Command Mode

Global Config

10-2 show ipv6 mroute

Note: No specific IP multicast is enabled for IPv6. However, enabling of multicast at the global config for both IPv4 and IPv6 is common.

This command is used to show the mroute entries that are specific for IPv6. (The command is essentially the IPv6 counterpart to the IPv4 **show ip mcast mroute** command.)

show ipv6 mroute {[detail] | [summary] | [group {*group-address***} [detail | summary]] | [source {***source-address***} [***grpaddr* **| summary]]}**

Parameters

detail	(Optional) the IPv6 multicast routing table details.
summary	(Optional) multicast routing table entries for specified group IPv6 address.
group	(Optional) Indicates the multicast routing table entries for specified group IPv6 address.
group-address	Indicates the group IPv6 address.
source	(Optional) Indicates the multicast routing table entries for specified source IPv6 address.
source-address	Indicates the source IPv6 address.
grpaddr	(Optional) Indicates the group source IPv6 address.
summary	(Optional) the IPv6 multicast routing table summary.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

If the **detail** parameter is used, then the command will cause the following Multicast Route Table fields to be displayed.

Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If the **summary** parameter is used, then the command will cause the following fields to be displayed.

Source IP Addr	The IP address of the multicast data source.

Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which the entry was created.
Incoming Interface	The interface on which the packet for the source/group arrives.
Outgoing Interface List	The list of outgoing interfaces on which the packet is forwarded.

10-3 show ipv6 mroute group

Shows the multicast configuration settings that are specific to IPv6, such as the flags, timer settings, RPF neighboring routers, incoming and outgoing interfaces, and expiration times for all of the entries included in the multicast mroute table that contain the given group IPv6 address group-address.

show ipv6 mroute group group-address {detail | summary}

Parameters

detail	Indicates the IPv6 multicast routing table details.
summary	Indicates the IPv6 multicast routing table summary.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Source IP Addr	Indicates the IP address of the multicast data source.
Group IP Addr	Indicates the IP address of the destination of the multicast packet.
Protocol	Indicates the multicast routing protocol by which this entry was created.
Incoming Interface	Indicates the interface on which the packet for this group arrives.
Outgoing Interface List	Indicates the list of outgoing interfaces on which this packet is forwarded.

10-4 show ipv6 mroute source

Shows the multicast configuration settings that are specific to IPv6, such as the flags, timer settings, RPF neighboring routers, incoming and outgoing interfaces, and expiration times for all of the entries included in the multicast mroute table that contain the given source IP address or both the source IP address and the group IP address pair.

show ipv6 mroute source source-address {*grpaddr* **| summary}**

Parameters

grpaddr	Indicates the group source IPv6 address.
summary	Indicates the IPv6 multicast routing table summary.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

If the *grpaddr* parameter is used, then the command will cause the following column headings to be displayed in the output table.

Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If the **summary** parameter is used, then the command will cause the following column headings to be displayed in the output table.

Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this source arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

10-5 show ipv6 mroute static

The **show ipvs mroute static** command is used in the Privileged EXEC or the User EXEC mode to show all of the configured IPv6 multicast static routes.

show ipv6 mroute static [*source-address***]**

Parameters

source-address	Indicates the source IPv6 address.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

Source Address	IP address of the multicast source network.
Source Mask	The subnetwork mask pertaining to the source IP.
RPF Address	The IP address of the RPF next-hop router toward the source.
Interface	The interface that is used to reach the RPF next-hop. This is valid if the RPF address is a link-local address.
Preference	The administrative distance for this Static MRoute.

10-6 clear ipv6 mroute

Deletes all of the IPv6 multicast route entries or the specified IPv6 multicast route entries.

Note: Only dynamic mroute entries are cleared by this command. Static mroute entries will not be cleared by it.

clear ipv6 mroute {* | group-address [source-address]}

Parameters

*****	Deletes all IPv6 entries from the IPv6 multicast routing table.
group-address	IPv6 address of the multicast group.
source-address	The IPv6 address of a multicast source that is sending multicast traffic to the group.

Default

The default is None.

Command Mode

Privileged EXEC

Example

Issuing the following command will delete all entries from the IPv6 multicast routing table.

```
(Routing)#clear ipv6 mroute *
```

Issuing the following command will delete all entries from the IPv6 multicast routing table that matches the multicast group address provided (that is, FF4E::1), regardless of which source is sending for this group.

```
(Routing)#clear ipv6 mroute FF4E::1
```

Issuing the following command will delete all entries from the IPv6 multicast routing table that matches both the multicast group address provided (that is, FF4E::1) and the multicast source address provided (that is, 2001::2):

```
(Routing)#clear ip mroute FF4E::1 2001::2
```

IPv6 PIM Commands

In this section, the commands used to configure the Protocol Independent Multicast - Dense Mode (PIM-DM) and the Protocol Independent Multicast - Sparse Mode (PIM-SM) for IPv6 multicast routing are described. The PIM-DM and PIM-SM consist of multicast routing protocols that provide scalable inter-domain multicast routing via the Internet, that is, independent of any mechanisms utilized by a particular unicast routing protocol. Only one PIM mode may be in operation at a given time.

10-7 ipv6 pim dense

Enables the administrative mode of the PIM-DM in the router.

The **no** command disables the administrative mode of the PIM-DM in the router.

ipv6 pim dense

no ipv6 pim dense

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

Example

The following provides an example of the command.

```
(Routing)(Config)#ipv6 pim dense
```

10-8 ipv6 pim sparse

Enables the administrative mode of the PIM-SM in the router.

The **no** command disables the administrative mode of the PIM-SM in the router.

ipv6 pim sparse

no ipv6 pim sparse

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

Example

The following provides an example of the command.

```
(Routing)(Config)#ipv6 pim sparse
```

10-9 ipv6 pim

Enables PIM on a specific interface or range of interfaces administratively.

The **no** command sets the administrative mode of the PIM on an interface to disabled.

ipv6 pim

no ipv6 pim

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

Example

The following is an example of the CLI display output for the command.

```
(Routing)(Interface 0/1)#ipv6 pim
```

10-10 ipv6 pim hello-interval

Configures the PIM hello interval for a specific router interface or a range of interfaces.

The **no** command resets the PIM hello interval back to the default value.

ipv6 pim hello-interval *0-18000*

no ipv6 pim hello-interval

Parameters

None

Default

The default is 30.

Command Mode

Interface Config

Example

The following provides an example of the command.

```
(Routing)(Interface 0/1)#ipv6 pim hello-interval 50
```

10-11 ipv6 pim bsr-border

Prevents bootstrap router (BSR) messages from being transmitted or received on a specific interface.

The **no** command disables the setting of a BSR border on the given interface.

Note: Only when the PIM-SM is enabled in the Global mode will this command take effect.

ipv6 pim bsr-border

no ipv6 pim bsr-border

Parameters

None

Default

The default is Disabled.

Command Mode

Interface Config

Example

The following provides an example of the command.

```
(Routing)(Interface 0/1)#ipv6 pim bsr-border
```

10-12 ipv6 pim bsr-candidate

Configures the router so that it will announce its candidacy to serve as a bootstrap router (BSR). The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

The **no** command to removes the configured PIM Candidate BSR router.

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ipv6 pim bsr-candidate interface {*slot/port* **| vlan** *1-4093***}** *hash-mask-length* **[***bsr-priority***] [interval** *interval***]**

no ipv6 pim bsr-candidate interface {*slot/port* **| vlan** *1-4093***}** *hash-mask-length* **[***bsr-priority***]**

Parameters

slot/port	Interface number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with PIM.
vlan	Indicates an interface in VLAN format (1-4093).
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
bsr-priority	(Optional) Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR. The default value is 0.
interval *interval*	(Optional) Indicates the BSR candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Default

The default is Disabled.

Command Mode

Global Config

Example

The following are examples of the command.

```
(Routing)(Config)#ipv6 pim bsr-candidate interface 0/1 32 5
```

```
(Routing)(Config)#ipv6 pim bsr-candidate interface 0/1 32 5 interval 100
```

10-13 ipv6 pim dr-priority

Sets the priority value determining when a given router is selected as the designated router (DR).

The **no** command resets the DR Priority of the specified interface back to its default value.

Note: Only when the PIM-SM is enabled in the Global mode will this command take effect.

ipv6 pim dr-priority *0-2147483647*

no ipv6 pim dr-priority

Parameters

None

Default

The default is 1.

Command Mode

Interface Config

Example

The following is an example of the CLI display output for the command.

```
(Routing)(Interface 0/1)#ipv6 pim dr-priority 10
```

10-14 ipv6 pim join-prune-interval

Configures the frequency with which PIM Join/Prune messages are sent on a specific interface. The length of the join/prune interval is specified in seconds.

The **no** command resets the length of the join/prune interval on the given interface back to the default value.

Note: Only when the PIM-SM is enabled in the Global mode will this command take effect.

ipv6 pim join-prune-interval *0-18000*

no ipv6 pim join-prune-interval

Parameters

None

Default

The default is 60.

Command Mode

Interface Config

Example

The following provides an example of the command.

```
(Routing)(Interface 0/1)#ipv6 pim join-prune-interval 90
```

10-15 ipv6 pim rp-address

Defines the address, for a specific multicast group range, of a PIM Rendezvous point (RP).

The **no** command removes the address, for the specified multicast group range, of the configured PIM Rendezvous point (RP).

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ipv6 pim rp-address {*rp-address* **|** *group-address/group-mask***} [override]**

no ipv6 pim rp-address {*rp-address* **|** *group-address/group-mask***} [override]**

Parameters

rp-address	The IPv6 address of the RP.
group-address	The group address supported by the RP.
group-mask	The group mask for the group address.
override	(Optional) Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Default

The default is 0.

Command Mode

Global Config

Example

The following provides an example of the command.

```
(Routing)(Config)#ipv6 pim rp-address 2001::1 ffle::0/64
```

10-16 ipv6 pim rp-candidate

Configures a router to advertise itself to the bootstrap router (BSR) as a PIM candidate rendezvous point (RP) for a specified multicast group range. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

The **no** command is used to disable the ability of the router to advertise itself to the bootstrap router (BSR) as a PIM candidate rendezvous point (RP).

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ipv6 pim rp-candidate interface {*slot/port* **| vlan** *1-4093***}** *group-address group-mask* **[interval** *interval***]**

no ipv6 pim rp-candidate interface {*slot/port* **| vlan** *1-4093***}** *group-address group-mask*

Parameters

slot/port	The IP address associated with this interface type and number is advertised as a candidate RP address. This interface must be enabled with PIM.
vlan	Indicates an interface in VLAN format (1-4093).
group-address	The multicast group address that is advertised in association with the RP address.
group-mask	The multicast group prefix that is advertised in association with the RP address.
interval *interval*	(Optional) Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Default

The default is Disabled.

Command Mode

Global Config

Example

The following are examples of the command.

```
(Routing)(Config)#ipv6 pim rp-candidate interface 0/1 ff1e::0/64
```

```
(Routing)(Config)#ipv6 pim rp-candidate interface 0/1 ff1e::0/64 interval 200
```

10-17 ipv6 pim ssm

Defines the range of Source Specific Multicast (SSM) IPv6 multicast addresses for the router.

The **no** command removes the range of Source Specific Multicast (SSM) IPv6 multicast addresses for the router.

Note: Only when the PIM-SM is configured as the PIM mode will this command take effect.

ipv6 pim ssm {default | *group-address group-mask***}**

no ipv6 pim ssm {default | *group-address group-mask***}**

Parameters

default	Indicates the SSM range access list to 232/8.
group-address	Indicates the defined SSM Range.
group-mask	Indicates the defined SSM Range.
default-range	Defines the SSM range access list FF3x::/32.

Default

The default is Disabled.

Command Mode

Global Config

Example

The following are example of the command.

```
(Routing)(Config)#ipv6 pim ssm default
```

```
(Routing)(Config)#ipv6 pim ssm ff32::/32
```

10-18 show ipv6 pim

Shows the system-wide information for the PIM-DM or the PIM-SM.

show ipv6 pim

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

PIM Mode – Dense

```
(Routing)#show ipv6 pim

PIM Mode..................................... Dense
```

```
Interface    Interface-Mode       Operational-Status
----------   ---------------      --------------------
0/1          Enabled              Non-Operational
0/3          Disabled             Non-Operational
0/21         Enabled              Operational
```

PIM Mode – Sparse

```
(Routing) #show ipv6 pim

PIM Mode..................................... Sparse

Interface    Interface-Mode       Operat onal-Status
----------   ---------------      --------------------
0/1          Enabled              Non-Operational
0/3          Disabled             Non-Operational
0/21         Enabled              Operational
```

PIM Mode – None

```
(Routing) #show ipv6 pim

PIM Mode..................................... None

None of the routing interfaces are enabled for PIM.
```

Display Parameters

Note: Some of the fields in the following table will not be displayed in the command output if the PIM mode is the PIM-DM (dense) because they are applicable only to the PIM-SM.

PIM Mode	Indicates whether the PIM mode is dense (PIM-DM) or sparse (PIM-SM).
Interface	*slot/port*
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

10-19 show ipv6 pim ssm

Shows the configured source specific IPv6 multicast addresses. The output of the command will read **No SSM address range is configured** if no SSM address range has been configured.

show ipv6 pim ssm

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 pim ssm

Group Address/Prefix Length
------------------------------
ff32::/32
```

If an SSM Group range is not configured, the following message will be displayed.

```
No SSM address range is configured.
```

Display Parameters

Group Address	The IPv6 multicast address of the SSM group.
Prefix Length	The network prefix length.

10-20 show ipv6 pim interface

Shows the interface information for PIM on a specific interface. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. If an interface is not specified, then the command shows the status parameters for all PIM-enabled interfaces.

show ipv6 pim interface [{*slot/port* **| vlan** *1-4093***}]**

Parameters

slot/port	(Optional) Indicates an interface in slot/port format.
vlan	(Optional) Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 pim interface

Interface..................................... 0/1
Mode.......................................... Sparse
Hello Interval (secs)......................... 30
Join Prune Interval (secs).................... 60
DR Priority................................... 1
BSR Border.................................... Disabled

Interface..................................... 0/21
Mode.......................................... Sparse
Hello Interval (secs)......................... 30
Join Prune Interval (secs).................... 60
DR Priority................................... 1
BSR Border.................................... Disabled
Neighbor Count................................ 1
Designated Router............................. fe80::20a:f7ff:fe81:8ad9
```

The following message will be displayed if no interfaces are enabled for PIM.

```
None of the routing interfaces are enabled for PIM.
```

Display Parameters

Interface	*slot/port*
Mode	Indicates whether the PIM mode enabled on the interface is dense or sparse.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. The default is 30 seconds.
Join Prune Interval	The join/prune interval for the PIM router. The interval is in seconds.
DR Priority	The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense.
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface.
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense.

10-21 show ipv6 pim neighbor

Shows the PIM neighbors discovered by PIMv2 Hello messages. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN. If the interface number is not specified, then the command shows the neighbors discovered for all the PIM-enabled interfaces.

show ipv6 pim neighbor [{*slot/port* **| vlan** *1-4093***}]**

Parameters

slot/port	(Optional) Indicates an interface in slot/port format.
vlan	(Optional) Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 pim neighbor

Neighbor Addr               Interface    Up Time      Expiry Time     DR Priority
                                         hh:mm:ss     hh:mm:ss
--------------------------  ----------   -----------  ------------    ------------
fe80::200:52ff:feb7:58ac    0/21         00:00:03     00:01:43        0 (DR)
```

The following message will be displayed if no neighbors have been learned by any of the interfaces.

```
No neighbors are learnt on any interface.
```

Display Parameters

Neighbor Addr	The IPv6 address of the PIM neighbor on an interface.
Interface	*slot/port*
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	Time remaining for the neighbor to expire.
DR Priority	The DR Priority configured on this Interface (PIM-SM only). **Note:** DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

10-22 show ipv6 pim bsr-router

Shows the bootstrap router (BSR) information.

show ipv6 pim bsr-router {candidate | elected}

Parameters

candidate	Indicates the PIM BSR candidate table information.
elected	Indicates the PIM BSR elected table information.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 pim bsr-router elected

BSR Address..................................... 3001::1
  BSR Priority ................................. 150
  BSR Hash Mask Length ......................... 120
  Next Bootstrap message (hh:mm:ss) ............ 00:00:15
```

```
(Routing)#show ipv6 pim bsr-router candidate

BSR Address..................................... 3001::1
  BSR Priority ................................. 150
  BSR Hash Mask Length ......................... 120
  C-BSR Advertisement Interval (secs) ........... 60
  Next Bootstrap message (hh:mm:ss) ............ NA
```

The following message will be displayed if no selected or configured BSRs exist on the router:

```
No BSR's exist/learned on this router.
```

Display Parameters

BSR Address	IPv6 address of the BSR.
BSR Priority	Priority as configured in the ipv6 pim bsr-candidate command.

BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the ipv6 pim bsr-candidate command.
C-BSR Advertisement Interval	Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

10-23 show ipv6 pim rp-hash

Shows the rendezvous point (RP) that is being used for a specified group.

show ipv6 pim rp-hash *group-address*

Parameters

group-address	The IPv6 multicast address of the SSM group.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing)#show ipv6 pim rp-hash ff1e::

RP Address..................................... 2001::1
  Type ........................................ Static
```

The following message will be displayed if no RP Group mapping exists on the router:

```
No RP-Group mappings exist/learned on this router.
```

Display Parameters

RP Address	The IPv6 address of the RP for the group specified.
Type	Indicates the mechanism (BSR or static) by which the RP was selected.

10-24 show ipv6 pim rp mapping

For the PIM group, shows the mapping to the active Rendezvous points (RP) that the router is aware of (whether they were configured or learned from the bootstrap router [BSR]). The optional parameters can be used to limit the information displayed to a specific RP address or in order to view group-to-candidate RP or group-to-Static RP mapping information.

show ipv6 pim rp mapping [{*rp-address* **| candidate | static}]**

Parameters

rp-address	(Optional) Indicates the RP Address of the active rendezvous point.
candidate	(Optional) Indicates the group to the candidate RP mapping info.
static	(Optional) Indicates the group to static RP mapping info.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following are examples of the CLI display output for the command.

```
(Routing)#show ipv6 pim rp mapping 2001::1

RP Address..................................... 2001::1
  Group Address ............................... ff1e::/64
  Origin ...................................... Static
  Expiry Time (hh:mm:ss) ...................... NA
  Next Candidate RP Advertisement (hh:mm:ss) .... NA
```

```
(Routing)#show ipv6 pim rp mapping

RP Address..................................... 2001::1
  Group Address ............................... ff1e::/64
  Origin ...................................... Static
  Expiry Time (hh:mm:ss) ...................... NA
  Next Candidate RP Advertisement (hh:mm:ss) .... NA
```

```
(Routing)#show ipv6 pim rp mapping candidate

RPAddress..................................... 2001::1
  Group Address ............................... ff1e::/64
  Origin ...................................... BSR
```

```
  C-RP Advertisement Interval (secs) ..... 200
```

The following message will be displayed if no RP Group mapping exists on the router.

```
No RP-Group mappings exist on this router.
```

Display Parameters

RP Address	The IPv6 address of the RP for the group specified.
Group Address	The IPv6 address and prefix length of the multicast group.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.
C-RP Advertisement Interval	Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.
Next Candidate RP Advertisement (hh:mm:ss)	Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP sends the C-RP advertisement messages to the elected BSR based on a scheduled interval.

IPv6 MLD Commands

IGMP/MLD Snooping is a type of Layer 2 functionality, but IGMP/MLD consist of Layer 3 multicast protocols. Their use requires that a network setup should have a multicast router (which can serve as a querier) present in order to solicit the multicast group registrations. However, some types of network setups do not require a multicast router because any multicast traffic is intended for hosts within the same network. In such a situation, D-LINK OS has an IGMP/MLD Snooping Querier that runs on one of the switches, while Snooping will be enabled on all of the switches. Please see “IGMP Snooping Configuration Commands” for more information on this topic.

10-25 ipv6 mld router

When used in administrative mode, the command enables MLD.

When used in the administrative mode, the **no** command disables MLD.

ipv6 mld router

no ipv6 mld router

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

10-26 ipv6 mld query-interval

Sets the query interval of the MLD router for a single interface or a range of interfaces. The query-interval stipulates the amount of time that passes between the sending of general queries when the router acts as the querier on that interface.

The **no** command resets the MLD query interval for that interface back to the default value.

ipv6 mld query-interval *1-3600*

no ipv6 mld query-interval

Parameters

None

Default

The default is 125 seconds.

Command Mode

Interface Config

10-27 ipv6 mld query-max-response-time

Sets the maximum response time of the MLD querier for a single interface or a range of interfaces, with this value being used to assign the maximum response time for the query messages sent on the interface or interfaces in question.

The **no** command resets the maximum response time of the MLD querier for the interface back to the default value.

ipv6 mld query-max-response-time *0-65535*

no ipv6 mld query-max-response-time

Parameters

None

Default

The default is 10,000 milliseconds.

Command Mode

Interface Config

10-28 ipv6 mld last-member-query-interval

Sets the length of the last member query interval of an MLD interface or a range of interfaces, where the value indicates the maximum response time for the group specific queries sent out by the interface or interfaces in question.

The **no** command resets the last-member-query-interval parameter for the given interface back to the default value.

ipv6 mld last-member-query-interval *0-65535*

no ipv6 mld last-member-query-interval

Parameters

None

Default

The default is 1,000 milliseconds.

Command Mode

Interface Config

10-29 ipv6 mld last-member-query-count

Sets the number of listener-specific queries that will be sent out before the router assumes that no local members are present on a single interface or a range of interfaces.

The **no** command resets the last-member-query-count parameter for the given interface back to the default value.

ipv6 mld last-member-query-count *1-20*

no ipv6 mld last-member-query-count

Parameters

None

Default

The default is 2.

Command Mode

lnterface Config

10-30 ipv6 mld version

Configures the MLD version that the interface in question uses.

The **no** command resets the MLD version used by the given interface back to the default value.

ipv6 mld version {1 | 2}

no ipv6 mld version

Parameters

None

Default

The default is 2.

Command Mode

Interface Config

10-31 show ipv6 mld groups

Shows information regarding the multicast groups that the MLD has reported. The information in question will only be displayed if MLD has been enabled on at least one interface. Otherwise,, there will be no group information available to display. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ipv6 mld groups {*slot/port* **| vlan** *1-4093* **|** *group-address***}**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan	Indicates an interface in VLAN format (1-4093).
group-address	Indicates the IPv6 address designated for the multicast group.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following are examples of the CLI display output for the commands.

```
(Routing)#show ipv6 mld groups ?
```

```
group-address      Enter Group Address Info.
<slot/port>        Enter interface in slot/port format.
```

```
(Routing)#show ipv6 mld groups 0/1

Group Address..................................... FF43::3
Interface......................................... 0/1
Up Time (hh:mm:ss)................................ 00:03:04
Expiry Time (hh:mm:ss)............................ ------
```

```
(Routing)#show ipv6 mld g ff43::3

Interface......................................... 0/1
Group Address..................................... FF43::3
Last Reporter..................................... FE80::200:FF:FE00:3
Up Time (hh:mm:ss)................................ 00:02:53
Expiry Time (hh:mm:ss)............................ ------
Filter Mode....................................... Include
Versionl Host Timer............................... ------
Group compat mode................................. v2

Source Address    Expiry Time
---------------   -------------
2003::10          00:04:17
2003::20          00:04:17
```

Display Parameters

When the *slot/port* is specified, the following fields will be displayed as a table.

Group Address	The address of the multicast group.
Interface	Interface through which the multicast group is reachable.
Up Time	Time elapsed in hours, minutes, and seconds since the multicast group has been known.
Expiry Time	Time left in hours. minutes. and seconds before the entry is removed from the MLD membership table.

When the *group-address* is specified, the following fields will be displayed for each multicast group and for each interface.

Interface	Interface through which the multicast group is reachable.
Group Address	The address of the multicast group.
Last Reporter	The IP Address of the source of the last membership report received for this multicast group address on that interface.
Filter Mode	The filter mode of the multicast group on this interface. The values it can take are include and exclude.
Version1 Host Timer	The time remaining until the router assumes there are no longer any

	MLD version-1 Hosts on the specified interface.
Group compat mode	The compatibility mode of the multicast group on this interface. The values it can take are MLDv1 and MLDv2.

The following table will also be displayed in order to specify all the sources that are associated with this group.

Source Address	The IP address of the source.
Uptime	Time elapsed in hours, minutes, and seconds since the source has been known.
Expiry Time	Time left in hours, minutes, and seconds before the entry is removed.

10-32 show ipv6 mld interface

Shows the MLD-related information for the interface in question. The *slot/port* argument corresponds to either a physical routing interface or to a VLAN routing interface. The keyword **VLAN** is utilized, instead of the *slot/port* format, to directly specify the VLAN ID of the routing VLAN.

show ipv6 mld interface {*slot/port* **| vlan** *1-4093***}**

Parameters

slot/port	Indicates an interface in slot/port format.
vlan	Indicates an interface in VLAN format (1-4093).

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show ipv6 mld interface all

Interface..................................... 0/1
MLD Global Admin Mode......................... Enabled
MLD Interface Admin Mode...................... Disabled
MLD Operational Mode.......................... Disabled
MLD Version................................... 2
Query Interval (secs)......................... 125
Query Max Response Time(milli-secs) ..... 10000
Robustness.................................... 2
```

```
Startup Query Interval (secs) ................. 31
Startup Query Count............................ 2
Last Member Query Interval (milli-secs)........ 1000
Last Member Query Count........................ 2

Interface...................................... 0/2
MLD Global Admin Mode.......................... Enabled
MLD Interface Admin Mode....................... Disabled
MLD Operational Mode........................... Disabled
MLD Version.................................... 2
Query Interval (secs).......................... 125
Query Max Response Time(milli-secs) ........... 10000
Robustness..................................... 2
Startup Query Interval (secs) ................. 31
Startup Query Count............................ 2
Last Member Query Interval (milli-secs)........ 000
Last Member Query Count........................ 2
```

Display Parameters

The following information will be displayed for all of the interfaces or for the specified interface only.

Interface	The interface number in slot/port format.
MLD Mode	Displays the configured administrative status of MLD.
Operational Mode	The operational status of MLD on the interface.
MLD Version	Indicates the version of MLD configured on the interface.
Query Interval	Indicates the configured query interval for the interface.
Query Max Response Time	Indicates the configured maximum query response time (in seconds) advertised in MLD queries on this interface.
Robustness	Displays the configured value for the tuning of the expected packet loss on a subnet attached to the interface.
Startup Query Interval	This valued indicates the configured interval between General Queries sent by a Querier on startup.
Startup Query Count	This value indicates the configured.number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	Value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.

If the operational mode of the MLD interface is enabled, then the following information will be displayed.

Querier Status	This value indicates whether the interface is an MLD querier or non-querier on the subnet it is associated with.
Querier Address	The IP address of the MLD querier on the subnet the interface is associated with.
Querier Up Time	Time elapsed in seconds since the querier state has been updated.

Querier Expiry Time	Time left in seconds before the Querier loses its title as querier.
Wrong Version Queries	Indicates the number of queries received whose MLD version does not match the MLD version of the interface.
Number of joins	Number of times a group membership has been added on this interface.
Number of Leaves	The number of times a group membership has been removed on this interface.
Number of Groups	The current number of membership entries for this interface.

10-33 show ipv6 mld traffic

Shows the MLD statistical information for the router.

show ipv6 mld traffic

Parameters

None

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows an example of the command.

```
(Routing)#show ipv6 mld traffic

Valid MLD Packets Received..................... 0
Valid MLD Packets Sent......................... 0
Queries Received............................... 0
Queries Sent................................... 0
Reports Received............................... 0
Reports Sent................................... 0
Leaves Received................................ 0
Leaves Sent.................................... 0
Bad Checksum MLD Packets....................... 0
Malformed MLD Packets.......................... 0
```

Display Parameters

Valid MLD Packets	The number of valid MLD packets received by the router.

Received	
Valid MLD Packets Sent	The number of valid MLD packets sent by the router.
Queries Received	The number of valid MLD queries received by the router.
Queries Sent	The number of valid MLD queries sent by the router.
Reports Received	The number of valid MLD reports received by the router.
Reports Sent	The number of valid MLD reports sent by the router.
Leaves Received	The number of valid MLD leaves received by the router.
Leaves Sent	The number of valid MLD leaves sent by the router.
Bad Checksum MLD Packets	The number of bad checksum MLD packets received by the router.
Malformed MLD Packets	The number of malformed MLD packets received by the router.

10-34 clear ipv6 mld counters

Resets the MLD counters for the specified interface to zero.

clear ipv6 mld *slot/port*

Parameters

slot/port	Indicates an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

10-35 clear ipv6 mld traffic

Clears all the existing entries in the MLD traffic database.

clear ipv6 mld *slot/port*

Parameters

slot/port	Indicates an interface in slot/port format.

Default

The default is None.

Command Mode

Privileged EXEC

IPv6 MLD-Proxy Commands

MLD-Proxy is the IPv6 equivalent of IGMP-Proxy. MLD-Proxy commands allow you to configure the network device as well as to view device settings and statistics using either serial interface or telnet session. The operation of MLD-Proxy commands is the same as for IGMP-Proxy: MLD is for IPv6 and IGMP is for IPv4.MGMD is a term used to refer to both IGMP and MLD.

10-36 ipv6 mld-proxy

Use this command to enable MLD-Proxy on the interface or range of interfaces. To enable MLD-Proxy on the interface, you must enable multicast forwarding. Also, make sure that there are no other multicast routing protocols enabled n the router.

Use the **no** command to disable MLD-Proxy on the router.

ipv6 mld-proxy

no ipv6 mld-proxy

Parameters

None.

Default

The default is None.

Command Mode

Interface Config

10-37 ipv6 mld-proxy unsolicit-rprt-interval

Use this command to set the unsolicited report interval for the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface.

Use the **no** command to reset the MLD-Proxy router's unsolicited report interval to the default value.

ipv6 mld-proxy unsolicit-rprt-interval *1-260*

no ipv6 mld-proxy unsolicit-rprt-interval

Parameters

None.

Default

The default is 1 second.

Command Mode

Interface Config

10-38 ipv6 mld-proxy reset-status

Use this command to reset the host interface status parameters of the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface.

ipv6 mld-proxy reset-status

Parameters

None.

Default

The default is None.

Command Mode

Interface Config

10-39 show ipv6 mld-proxy

Use this command to display a summary of the host interface status parameters.

show ipv6 mld-proxy

Parameters

None.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The foilowing shows example CLI display output for the command.

```
(Routing)#show ipv6 mld-proxy

Interface Index.................................. 0/3
Admin Mode....................................... Enable
Operational Mode................................. Enable
Version.......................................... 3
Num of Multicast Groups.......................... 0
Unsolicite Report Interval....................... 1
Querier IP Address on Proxy Interface............ fe80::1:2:5
Older Version 1 Querier Timeout.................. 00:00:00
Proxy Start Frequency.....................
```

Display Parameters

The command displays the following parameters only when you enable MLD-Proxy.

Interface Index	The interface number of the MLD-Proxy.
Admin Mode	Indicates whether MLD-Proxy is enabled or disabled.
Operational Mode	Indicates whether MLD-Proxy is operationally enabled or disabled. This is a status parameter.
Version	The present MLD host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the MLD-Proxy interface.
Unsolicited Report Interval	The time interval at which the MLD-Proxy interface sends unsolicited group membership report.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream Interface (MLD-Proxy interface).
Older Version 1 Querier Timeout	The interva| used to timeout the older version 1 queriers.
Proxy Start Frequency	The number of times the MLD-Proxy has been stopped and started.

10-40 show ipv6 mld-proxy interface

This command displays a detailed list of the host interface status parameters It displays the following parameters only when you enable MLD-Proxy.

show ipv6 mld-proxy interface

Parameters

None.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ipv6 mld-proxy interface

Interface Index.................................. 0/1

Ver     Query Rcvd   Report Rcvd  Report Sent  Leave Rcvd   Leave Sent
-----   ----------   -----------  -----------  -----------  -----------
1       2            0            0            0            2
2       3            0            4            -----        -----
```

Display Parameters

Interface Index	The *slot/port* of the MLD-proxy.

The column headings of the table associated with the interface are as follows:

Ver	The MLD version.
Query Rcvd	Number of MLD queries received.
Report Rcvd	Number of MLD reports received.
Report Sent	Number of MLD reports sent.
Leaves Rcvd	Number of MLD leaves received. Valid for version 2 only.
Leaves Sent	Number of MLD leaves sent on the Proxy interface. Valid for version 2 only.

10-41 show ipv6 mld-proxy groups

Use this command to display information about multicast groups that the MLD-Proxy reported.

show ipv6 mld-proxy groups

Parameters

None.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#shcw ipv6 mld-proxy groups

Interface Index.................................. 0/3

Group Address   Last Reporter   Up Time      Member State      Filter Mode     Sources
-------------   -------------   ---------    ---------------   ------------    --------
FF1E::1         FE80::100:2.3   00:01:40     DELAY_MEMBER      Exclude         2
FF1E::2         FE80::100:2.3   00:02:40     DELAV_MEMBER      Include         1
FF1E::3         FE80::100:2.3   00:01:40     DELAY_MEMBER      Exclude         0
FF1E::4         FE80::100:2.3   00:02:44     DELAV_MEMBER      Include         4
```

Display Parameters

Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group. on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: • **Idle_Member:** The interface has responded to the latest group membership query for this group. • **Delay_Member:** The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are **Include** or **Exclude**.
Sources	The number of sources attached to the multicast group.

10-42 show ipv6 mld-proxy groups detail

Use this command to display information about multicast groups that MLD-Proxy reported.

show ipv6 mld-proxy groups detail

Parameters

None.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ipv6 igmp-proxy groups

Interface Index................................. 0/3

Group Address   Last Reporter   Up Time      Member State      Filter Mode     Sources
-------------   -------------   ---------    ---------------   ------------    --------
FF1E::1         FE80::100:2.3   244          DELAY_MEMBER      Exclude         2

Group Source List       Expiry Time
--------------------    ---------------
2001::1                 00:02:40
2002::2                 --------

Group Address   Last Reporter   Up Time      Member State      Filter Mode     Sources
-------------   -------------   ---------    ---------------   ------------    --------
FF1E::2         FE80::100:2.3   243          DELAY_MEMBER      Include         1

Group Source List       Expiry Time
--------------------    ---------------
3001::1                 00:03:32
3002::2                 00:03:32

Group Address   Last Reporter   Up Time      Member State      Filter Mode     Sources
-------------   -------------   ---------    ---------------   ------------    --------
FF1E::3         FE80::100:2.3   328          DELAY_MEMBER      Exclude         0
FF1E::4         FE80::100:2.3   255          DELAY_MEMBER      Include         4

Group Source List       Expiry Time
--------------------    ---------------
4001::1                 00:03:40
5002::2                 00:03:40
4001::2                 00:03:40
5002::2                 00:03:40
```

Display Parameters

Interface	The interface number ofthe MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group. on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: • **Idle_Member:** The interface has responded to the latest group membership query for this group. • **Delay_Member:** The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are **Include** or **Exclude**.
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	The time left for a source to get deleted.

11. Border Gateway Protocol Commands

This section describes the commands you use to view and configure Border Gateway Protocol (BGP), which is an exterior gateway routing protocol that you use to route traffic between autonomous systems. The BGP CLI commands are available in the D-LINK OS software BGP package.

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.

BGP Commands

11-1 router bgp

This command enables BGP and identifies the autonomous system (AS) number of the router. Only a single instance of BGP can be run and the router can only belong to a single AS.

Use the **no** command to set BGP to disabled and all BGP configuration reverts to default values. Alternatively, you can use "no enable (BGP)" in BGP Router Configuration mode to disable BGP globally without clearing the BGP configuration.

router bgp *as-number*

no router bgp *as-number*

Parameters

as-number	The router's autonomous system number (ASN). The as-number ranges from 1-429496729.

Default

The default is an inactive BGP.

Command Mode

Global Config

11-2 address-family

To configure policy parameters within a peer template to be applied to a specific address family, use the **address-family** command in Peer Template Configuration mode. This command enters an Address Family Configuration mode within the peer template. Policy commands configured within this mode apply to the address family. The following commands can be added to a peer template in Address Family Configuration mode:

- "filter-list (BGP Router Config)"
- "filter-list (IPv6 Address Family Config)"
- "maximum-paths (BGP Router Config)"
- "maximum-paths (IPv6 Address Family Config)"

- “maximum-prefix (BGP Router Config)”
- “maximum-prefix (IPv6 Address Family Config)”
- “neighbor default-originate (BGP Router Config)”
- “neighbor filter-list (BGP Router Config)”
- “neighbor maximum-prefix (BGP Router Config)”
- “neighbor prefix-list”
- “neighbor route-map (BGP Router Config)”
- “neighbor route-map (IPv6 Address Family Config)”
- “redistribute (IPv6 Address Family Config)”
- “route-reflector-client”

address-family {ipv4 | ipv6}

Parameters

ipv4	Configure policy parameters to be applied to IPv4 routes.
ipv6	Configure policy parameters to be applied to IPv6 routes.

Default

The default is None.

Command Mode

Privileged EXEC

Example

In the following example of the command, the peer template AGGR sets the keepalive timer to 3 seconds, the hold timer to 9 seconds, allows communities to be sent for both IPv4 and IPv6 routes, and configures different inbound and outbound route maps for IPv4 and IPv6. Two neighbors, 172.20.1.2 and 172.20.2.2, inherit these parameters from the template.

```
(R1)(ConFig)#rourer bgp 65000
(R1)(Config-router)#neighbor 172.20.1.2 remote-as 65001
(R1)(Config-router)#neighbor 172.20.2.2 remote-as 65001
(R1)(Config-router)#template peer AGGR
(R1)(Config-rtr-tmplt)#timers 3 9
(R1)(Config-rtr-tmplt)#address-family ipv4
(R1)(Config-rtr-tmplt-af)#send-community
(R1)(Config-rtr-tmplt-af)#route-map RM4-IN in
(R1)(Config-rtr-tmplt-af)#route-map RM4-OUT out
(R1)(Config-rtr-tmplt-af)#exit
(R1)(Config-rtr-tmplt)#address-family ipv6
(R1)(Config-rtr-tmplt-af)#send-community
(R1)(Config-rtr-tmplt-af)#route-map RM6-IN in
(R1)(Config-rtr-tmplt-af)#route-map RM6-OUT out
(R1)(Config-rtr-tmplt-af)#exit
(R1)(Config-rtr-tmplt)#exit
(R1)(Config-router)#neighbor 172.20.1.2 inherit peer AGGR
(R1)(Config-router)#neighbor 172.20.2.2 inherit peer AGGR
(R1)(Config-router)#address-family ipv6
```

```
(R1)(Config-router)#neighbor 172.20.1.2 activate
(R1)(Config-router)#neighbor 172.20.2.2 activate
```

11-3 address-family ipv4

To enter IPv4 VRF Address Family Configuration mode to configure BGR VRF parameters, use the **address-family ipv4 vrf** command in BGP Router Configuration mode. Commands entered in this mode enable peering with BGP neighbors in this VRF instance. All the neighbor-specific commands are given in this mode as well.

Use the **no** command to delete the IPv4 VRF configuration.

address-family ipv4 vrf *vrf-name*

no address-family ipv4 vrf *vrf-name*

Parameters

vrf *vrf-name*	Indicates the name of the virtual router to configure.

Default

The default is a disabled VRF configuration.

Command Mode

BGP Router Config

11-4 address-family ipv6

To enter IPv6 Address Family Configuration mode in order to specify IPv6-specific configuration parameters, use the **address-family ipv6** command in BGP Router Configuration mode. Commands entered in this mode can be used to enable exchange of IPv6 routes, specify IPv6 prefixes to be originated, and configure inbound and outbound policies to be applied to IPv6 routes.

Use the **no** command to clear all IPv6 address family configuration.

address-family ipv6

no address-family ipv6

Parameters

None.

Default

The default is disabled IPv6 routes.

Command Mode

BGP Router Config

11-5 address-family vpnv4 unicast

This command enters into VPN4Address Family Configuration mode and sets up a routing session to carry VPN IPv4 (VPNv4) addresses across the backbone. When an iBGP neighbor is in this mode, each VPNv4 prefix is made globally unique by the addition of an 8-byte Route distinguisher (RD). Only unicast prefixes are carried to its peer.

The following commands are available in VPNv4 address family configuration mode.

- **neighbor** *ip-address* activate
- **neighbor** *ip-address* send-community extended

To exit from the VPNv4 address family mode, use the **exit** command.

Use the **no** command to deleie the configuration done in this mode.

address-family vpnv4 unicast

no address-family vpnv4 unicast

Parameters

None.

Default

The default is a disabled VPNv4 address family.

Command Mode

BGP Router Config

Example

The following example shows how to enter the VPNv4 address family mode and configure neighbor commands.

```
(Router)(Config)#router bgp 10
(Router)(Config-router)#neighbor 1.1.1.1 remote-as 10
(Router)(Config-router)#address-family vpnv4 unicast
(Router)(Config-router-af-vpnv4)#neighbor 1.1.1.1 activate
(Router)(Config-router-af-vpnv4)#neighbor 1.1.1.1 send-community extended
(Router)(Config-router-af-vpnv4)#exit
(Router)(Config-router)#
```

11-6 advertisement-interval (BGP Router Config)

Use this command to configure the minimum time that must elapse between advertisements of the same route to a given neighbor. RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not

limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

D-LINK OS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to return to the default the minimum time that must elapse between advertisements of the same route to a given neighbor.

advertisement-interval *seconds*

no advertisement-interval

Parameters

ip-address	The neighbor's IP address.
seconds	The minimum time between route advertisement, in seconds. The range is from 0 to 600 seconds.

Default

The default is as follows:

- 30 seconds for external peers
- 5 seconds for internal peers

Command Mode

BGP Router Config

11-7 advertisement-interval (IPv6 Address Family Config)

In IPv6 Address Family mode, this command controls the time between sending Update messages containing IPv6 routes.

D-LINK OS BGP enforces the advertisement intenral by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to return to the default the minimum time that must elapse between advertisements of the same IPv6 route to a given neighbor.

advertisement-interval *seconds*

no advertisement-interval

Parameters

ip-address	The neighbors IP address.
seconds	The minimum time between route advertisement, in seconds. The range is from 0 to 600 seconds.

Default

The default is as follows:

- 30 seconds for external peers
- 5 seconds for internal peers

Command Mode

IPv6 Address Family Config

11-8 aggregate-address (BGP Router Config)

To configure a summary address for BGP, use the **aggregate-address** command in Router Configuration mode. No aggregate addresses are configured by default.

To be considered a match for an aggregate address, a prefix must be more specific (i.e. have a longer prefix length) than the aggregate address. A prefix whose prefix length equals the length of the aggregate address is not considered a match.

When BGP originates a summary address, it installs a reject route in the common routing table for the summary prefix. Any received packets that match the summary prefix, but not a more specific route, match the reject route and are dropped.

BGP accepts up to 128 summary addresses for each address family.

Use the **no** command to delete a summary address for BGP. The *address mask* is a summary prefix and mask.

aggregate-address {*address mask* **|** *ipv6-prefix/pfx-len***} [as-set] [summary-only]**

no aggregate-address *address mask*

Parameters

address mask	Summary IPv4 prefix and mask. The default route (0.0.0.0 0.0.0.0) cannot be configured as an aggregate-address. The mask cannot be a 32-bit mask (255.255.255.255). The combination of prefix and mask must be a valid unicast destination prefix.
ipv6-prefix/pfx-len	Summary IPv6 prefix and prefix length. The range for prefix length is 1 to 127.
as-set	(Optional) If set, the aggregate is advertised with a non-empty AS_PATH. If the AS_PATH of all contained routes is the same, the AS_PATH of the aggregate is the AS_PATH of the contained route.
summary-only	(Optional) When the **summary-only** option is given, the more-specific routes within the aggregate address are not advertised to neighbors.

Default

The default is None.

Command Mode

BGP Router Config

11-9 aggregate-address (IPv4 VRF Address Family)

To configure a summaiy address for BGP, use the **aggregate-address** command in Router Configuration mode. No aggregate addresses are configured by default.

To be considered a match for an aggregate address, a prefix must be more specific (i.e. have a longer prefix length) than the aggregate address. A prefix whose refix length equals the length of the aggregate address is not considered a match.

When BGP originates a summary address, it installs a reject route in the common routing table for the summary prefix. Any received packets that match the summary prefix, but not a more specific route, match the reject route and are dropped.

BGP accepts up to 128 summary addresses for each address family.

Use the **no** command to delete a summary address for BGP. The *address mask* is a summary prefix and mask.

aggregate-address *address mask* **[as-set] [summary-only]**

no aggregate-address *address mask*

Parameters

address mask	Summary IPv4 prefix and mask. The default route (0.0.0.0 0.0.0.0) cannot be configured as an aggregate-address. The mask cannot be a 32-bit mask (255.255.255.255). The combination of prefix and mask must be a valid unicast destination prefix.
as-set	(Optional) If set, the aggregate is advertised with a non-empty AS_PATH. If the AS_PATH of all contained routes is the same, the AS_PATH of the aggregate is the AS_PATH of the contained route. Otherwise, if the contained routes have different AS_PATHs, the AS_PATH attribute includes an AS_SET with each of the AS numbers listed in the AS_PATHs of the aggregate routes.
summary-only	(Optional) When the **summary-only** option is given, the more-specific routes within the aggregate address are not advertised to neighbors.

Default

The default is None.

Command Mode

IPv4 VRF Address Family Config

11-10 bgp aggregate-different-meds

Use the **bgp aggregate-different-meds** command in BGP Router Configuration mode to allow the aggregation of routes with different MED attributes. By default, BGP only aggregates routes that have the same MED value, as prescribed by RFC 4271.

When this command is given, the path for an active aggregate address is advertised without a MED attribute. When this command is not given, if multiple routes match an aggregate address, but have different MEDs, the aggregate takes the MED of the first matching route. Any other matching prefix with the same MED is included in the aggregate. Matching prefixes with different MEDs are not considered to be part of the aggregate and continue to be advertised as individual routes.

Use the **no** command in BGP Router Configuration mode to return the command to the default.

bgp aggregate-different-meds

no bgp aggregate-different-meds

Parameters

None.

Default

The default is a matching MED val for all routes aggregated by a given aggregate address.

Command Mode

- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family Config

11-11 bgp always-compare-med

To compare MED values during the decision process in paths received from different ASs, use the **bgp always-compare-med** command. The MED is a 32-bit integer, commonly set by an external peer to indicate the internal distance to a destination. The decision process compares MED values to prefer paths that have a shorter internal distance. Since different ASs may use different internal distance metrics or have different policies for setting the MED, the decision process normally does not compare MED values in paths received from peers in different autonomous systems. This command allows you to force BGP to compare MEDs, regardless of whether paths are received from a common AS.

Use the **no** command to revert to the default behavior, only comparing MED values from paths received from neighbors in the same AS.

bgp always-compare-med

no bgp always-compare-med

Parameters

None.

Default

The default is a MED setting to only compare paths with peers within the same AS.

Command Mode

- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family Config

11-12 bgp bestpath as-path ignore

To ignore the AS-PATH length in the best path calculation during the decision process, use the **bgp bestpath as-path ignore** command in Router Configuration mode. For IPv6 routes, configure this command in Address Family IPv6 mode. To influence ECMP route calculations, configure the AS-PATH parameter.

Use the **no** command to revert to the default behavior, where AS-PATH length is not ignored in the BGP best path calculation.

bgp bestpath as-pat ignore

no bgp bestpath as-pat ignore

Parameters

None.

Default

The default is a behavior setting to avoid ignoring AS-PATH length in BGP best path calculations.

Command Mode

- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family Config

11-13 bgp client-to-client reflection

By default, a route reflector reflects routes received from its clients to its other clients. However, if a route reflector's clients have a full BGP mesh, the route reflector does not reflect to the clients. The bgp client-to-client refiection command enables client-to-client reflection for IPv4, lPV6, or IPv4 VRF routes.

Route reflection can change the routes clients select. A route reflector only reflects those routes it selects as best routes. Best route selection can be infiuenced by the IGP metric of the route to reach the BGP next hop. Since a clients IGP distance to a given next hop may differ from the route refiectors IGP distance, a route reflector may not readvertise a route a client would have selected as best in the absence of route reflection. One way to avoid this effect is to fully mesh the clients within a cluster. When

clients are fully meshed, there is no need for the clusters route reflectors to reflect client routes to other clients within the cluster. When client-to-client refiection is disabled, a route reflector continues to reflect routes from non-clients to clients and from clients to non-clients.

Use the **no** command to disable the BGP client-to-client reflection.

bgp client-to-client reflection

no bgp client-to-client reflection

Parameters

None

Default

The default is configured to enable client-to-client reflection when a router is configured as a route reflector.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-14 bgp cluster-id

Use the **bgp cluster-id** command to specify the cluster ID of a route refiector. To revert the cluster ID to its default, use the no form of this command.

A route reflector and its clients form a cluster. Since a cluster with a single route reflector has a single point of failure, a cluster may be configured with multiple route reflectors. To avoid sending multiple copies of a route to a client, each route reflector in a cluster should be configured with the same cluster ID. Route reflectors with the same cluster ID must have the same set of clients; othen/vise, some routes may not be reflected to some clients. The same cluster ID is used for both IPv4 and IPv6 route refiection.

Use the **no** command to revert the cluster ID to its default.

bgp cluster-id *cluster-id*

no bgp cluster-id *cluster-id*

Parameters

cluster-id	A non-zero 32-bit identifier that uniquely identifies a cluster of route reflectors and their clients. The cluster ID may be entered in dotted notation like an IPv4 address or as an integer.

Default

The default is configured to enable a route reflector with an unconfigured cluster ID to use its BGP router ID (configured with bgp router-id) as the cluster ID.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-15 bgp default local-preference

Use this command to specify the default local preference. Local preference is an attribute sent to internal peers to indicate the degree of preference for a route. A route with a numerically higher local preference value is preferred.

BGP assigns the default local preference to each path received from an external peer. (BGP retains the **LOCAL_PREF** on paths received from internal peers.) BGP also assigns the default local preference to locally-originated paths. If you change the default local preference, BGP automatically initiates a soft inbound reset for all peers to apply the new local preference.

Use the **no** command to set the default value of local preference of the BGP router.

bgp default local-preference *number*

no bgp default local-preference

Parameters

number	The value to use as the local preference for routes advertlsed to internal peers. The range is 0 to 4,294,967,295.

Default

The default is 100. When the command is not given, BGP advertises a local preference of 100 in Update messages to internal peers.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-16 bgp fast-external-failover

Use this command to configure BGP to immediately reset the adjacency with an external peer if the routing interface to the peer goes down. When BGP gets a routing interface down event, BGP drops the adjacency with all external peers whose IPv4 address is in one of the subnets on the failed interface. This behavior can be overridden for specific inte sing the command “ip bgp fast-external-failover”.

Use the **no** command to disable the BGP fast-external-failover.

bgp fast-external-failover

no bgp fast-external-failover

Parameters

None

Default

The default is Enabled.

Command Mode

- Router Config
- IPv4 VRF Address Family Config

11-17 bgp fast-internal-failover

Use this command to configure BGP to immediately reset the adjacency with an internal peer when there is a loss of reachability to an internal peer. BGP tracks the reachability of each internal peer's IP address. If a peer becomes unreachable (that is, the RIB no longer has a non-default route to the peer's IP address), then BGP drops the adjacency.

Use the **no** command to return the "bgp fast-internal-failover" command to the default.

bgp fast-internal-failover

no bgp fast-internal-failover

Parameters

None

Default

The default is Enabled.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-18 bgp listen

Use this command to activate the IPv4 BGP dynamic neighbors feature and create an IPv4 or IPv6 listen range and associate it with a specified peer template.

Use limit max-number to define the global maximum number of IPv4 BGP dynamic neighbors that can be created.

BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. Each range can be configured as a subnet IP address. After a subnet range is configured for a BGP peer group, and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created. Dynamically created neighbors are not displayed in the running-config.

If a template peer name is not specified, all dynamic neighbors that are created will inherit default parameters. The template peer name can be assigned/changed for a listen range in any time.

The total number of both IPv4 and IPv6 listen range groups you can configure are 10.

Use the **no** command to deactivate the IPv4 BGP dynamic neighbors feature and delete an IPv4 listen range and deassociate it with a specified peer template.

bgp listen {limit *max-number* **| range** *network/length* **[inherit peer** *peer-template-name***]}**

no bgp listen {limit | range *network/length* **[inherit peer** *peer-template-name***]}**

Parameters

limit *max-number*	Sets a maximum limit number of IPv4 BGP dynamic subnet range neighbors. Number from 1 to 100. Default is 20.
range *network/length*	Specifies a listen subnet range that is to be created. length is the IP prefix representing a subnet, and the length of the subnet mask in bits. network is a valid IPv4 prefix.
inherit peer *peer-template-name*	(Optional) Specifies a BGP peer template name that is to be associated with the specified listen subnet range and inherited with dynamically created neighbors. The template will be inherited with dynamically created neighbors.

Default

The default is as follows: BGP dynamic neighbor inactive; subnets are not associated with a BGP listen subnet range.

Command Mode

- BGP Router Config
- IPv6 Address Family Config

Example

The following commands show how to create a listen range with a template to be inherited with dynamically created BGP neighbors.

```
(Routing)#configure
(Routing)(Config)#router bgp 100
(Routing)(Config-router)#bgp listen limit 10
(Routing)(Config-router)#bgp listen range 10.12.0.0/16
(Routing)(fionfig-router)#bgp listen range 10.27.0.0/16 inherit peer ABC
```

11-19 bgp log-neighbor-changes

Use this command to enable logging of adjacency state changes. Both backward and forward adjacency state changes are logged. Forward state changes, except for transitions to the **Established** state, are logged at the **Informational** severity level. Backward state changes and forward changes to **Established** are logged at the **Notice** severity level.

Use the **no** command to return the "bgp log-neighbor-changes" command to the default.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Parameters

None

Default

The default is as follows: Neighbor State changes not logged.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-20 bgp maxas-limit

To specify a limit on the length of AS-PATHs that BGP accepts from its neighbors, use the bgp maxas-limit in Router Configuration mode. if BGP receives a path whose AS-PATH attribute is longer than the configured limit, BGP sends a NOTIFICATION and resets the adjacency.

Use the **no** command to revert to the default the limit on the length of AS-PATHs that BGP accepts from its neighbors.

bgp maxas-limit *number*

no bgp maxas-limit

Parameters

number	The maximum length of an AS-PATH that BGP will accept from any of its neighbors. The length is the number of autonomous systems listed in the path. The limit may be set to any value from 1 to 100.

Default

The default is as follows: D-Link OS BGP configuration accepting AS-PATHs containing up to 75 AS numbers.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-21 bgp router-id

Use this command to set the BGP router ID. There is no default BGP router ID. The system does not select a router ID automatically. You must configure one manually.

The BGP router ID must be a valid IPv4 unicast address, but is not required to be an address assigned to the router. The router ID is specified in the dotted notation of an IP address. Setting the router ID to

0.0.0.0 disables BGP. Changing the router ID disables and reenables BGP, causing all adjacencies to be reestablished.

Use the **no** command to reset the BGP router ID, disabling BGP.

bgp router-id *router-id*

no bgp router-id *router-id*

Parameters

router-id	An IPv4 address for BGP to use as its router ID.

Default

The default is 0.0.0.0.

Command Mode

BGP Router Config

11-22 default-information originate

Use this command to allow BGP to originate a default route (either BGP, IPv4 VRF, or IPv6, depending on the mode). By default, BGP does not originate a default route. If a default route is redistributed into BGP, BGP does not advertise the default route unless the **default-information originate** command has been given. The always option is disabled by default.

Use the **no** command to disable BGP from originating a default route.

default-information originate [always]

no default-information originate

Parameters

always	(Optional) This optional keyword allows BGP to originate a default route, even if the common routing table has no default route.

Default

The default is as follows: BGP configuration does not originate a default route. The **always** option is disabled.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config
- IPv6 Address Family Config

11-23 default metric

Use this command to set the value of the Multi Exit Discriminator (MED) attribute on redistributed routes (either BGP, IPv4 VRF, or IPv6 routes, depending on the mode) when no metric has been specified in the command "redistribute (BGP Router Config)".

Use the **no** command to delete the default for the metric of redistributed routes.

default-metric *vulue*

no default-metric

Parameters

vulue	The value to set as the MED. The range is 1 to 4,294,967,295.

Default

The default is as follows: metric is not set and MED is not included in redistributed routes.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config
- IPv6 Address Family Config Config

11-24 default-originate (BGP Router Config)

To configure BGP to originate a default route to a specific neighbor, use the neighbor default-originate command in BGP router configuration mode. By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the "default-information originate" command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the "show ip bgp" command), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the "show ip bgp neighbors advertised-routes" command).

Origination of the default route is not subject to a prefix filter configured with the command "distribute-list prefix out".

A route map may be configured to set attributes on the default route sent to the neighbor. if the route map includes a **match ip-address** term, that term is ignored. Ifthe route map includes **match community** or **match as-path** terms, the default route is not advertised. Ifthere is no route map with the route map name given, the default route is not advertised.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to prevent BGP from originating a default route to a specific neighbor.

default-originate [route-map *map-name***]**

no default-originate

Parameters

route-map *map-name*	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

Default

The default is not configured to originate a BGP default route.

Command Mode

BGP Router Config

11-25 neighbor default-originate (IPv6 Address Family Config)

To configure BGP to originate a default IPv6 route to a specific neighbor, use the neighbor default-originate command in IPv6 Address Family configuration mode. By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the "default-information originate" command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the "show ip bgp" command), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the "show ip bgp neighbors advertised-routes" command).

Origination of the default route is not subject to a prefix filter configured with the command "distribute-list prefix out".

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to prevent BGP from originating a default IPv6 route to a specific neighbor.

default-originate [route-map *map-name***]**

no default-originate [route-map *map-name***]**

Parameters

route-map *map-name*	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

Default

The default is not configured to originate a default.

Command Mode

IPv6 Address Family Config

11-26 distance (BGP Router Config)

Use this command to set the preference (also known as administrative distance) of BGP routes to specific destinations. You may enter up to 128 instances ofthis command. Two instances ofthis command may not have the same prefix and wildcard mask. If a distance command is configured that matches an existing distance Command's prefix and wildcard mask, the new command replaces the existing command. There can be overlap between the prefix and mask configured for different commands. When there is overlap, the command whose prefix and wildcard mask are the longest match for a neighbor address is applied to routes from that neighbor.

An ECMP route's distance is determined by applying distance commands to the neighbor that provided the best path.

The distance command is not applied to existing routes. To apply configuration changes to the distance command itself or the prefix list to which a distance command applies, you must force a hard reset of affected neighbors.

Use the **no** command to set the preference of BGP routes to the default.

distance *distance* **[prefix wildcard-mask [***prefix-list***]]**

no distance *distance* **[prefix wildcard-mask [***prefix-list***]]**

Parameters

distance	The preference value for matching routes. The range is 1 to 255.
prefix wildcard-mask	(Optional) Routes learned from BGP peers whose address falls within this prefix are assigned the configured distance value.The wildcard-mask is an inverted network mask whose 1 bits indicate the don't care portion of the prefix.
prefix-list	(Optional) A prefix list can optionally be specified to limit the distance value to a specific set of destination prefixes learned from matching neighbors.

Default

The default is as follows: BGP assigns preference values according to the **distance bgp** command, unless overridden for specific neighbors or prefixes.

Command Mode

BGP Router Config

Example

The following shows examples of the command.

To set the preference value of the BGP route to 100.0.0.0/8 from neighbor 10.1.1.1, use the following distance command.

```
(Routing)(Config)#ip prefix-list pfx-listl permit 100.0.0.0/8
(Routing)(Config)#router bgp 1
(Routing)(Config-router)#distance 25 10.1.1.1 0.0.0.0 pfx-list1
```

To set the preference value to 12 for all BGP routes from neighbor 10.1.1.1, use the following distance command.

```
(Routing)(Config-router)#distance 12 10.1.1.1 0.0.0.0
```

To set the preference value of all routes within 100.0.0.0/8 from any neighbor, use the following distance command.

```
(Routing)(Config)#ip prefix-list pfx-list2 permit 100.0.0.0/8 ge 8
(Routing)(Config)#router bgp 1
(Routing)(Config-router)#distance 25 0.0.0.0 255.255.255.255 pfx-1ist2
```

11-27 distance BGP (BGP Router Config)

Use this command to set the preference, (also known as administrative distance), of BGP routes. Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and reenabling BGP.

Use the **no** command to set the default route preference value of BGP routes in the router.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Parameters

external-distance	The preference value for routes learned from external peers. The range is 1 to 255.
internal-distance	The preference value for routes learned from internal peers. The range is 1 to 255.
local-distance	The preference value for locally-originated routes. The range is 1 to 255.

Default

The default is as follows: external – 20, internal – 200, local – 200.

Command Mode

BGP Router Config

11-28 distance BGP (IPv4 VRF Address Family)

Use this command to set the preference, (also known as administrative distance), of BGP routes. Different distance values can be configured for routes learned from external peers, routes learned from

internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and re-enabling BGP.

Use the **no** command to set the default route preference value of BGP routes in the router.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Parameters

external-distance	The preference value for routes learned from external peers. The range is 1 to 255.
internal-distance	The preference value for routes learned from internal peers. The range is 1 to 255.
local-distance	The preference value for locally-originated routes. The range is 1 to 255.

Default

The default is as follows: external – 20, internal – 200, local – 200.

Command Mode

IPv4 VRF Address Family Config

11-29 distance BGP (IPv6 Address Family Config)

Use this command to set the preference, (also known as administrative distance), for eBGP, iBGP, and locally-originated BGP IPv6 routes. Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for fonrvarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and reenabling BGP.

Use the **no** command to set the default route preference value for eBGP, iBGP, and locally-originated BGP IPv6 routes in the router.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Parameters

external-distance	The preference value for routes learned from external peers. The range is 1 to 255.
internal-distance	The preference value for routes learned from internal peers. The range is 1 to 255.
local-distance	The preference value for locally-originated routes. The range is 1 to 255.

Default

The default is as follows: external – 20, internal – 200, local – 200.

Command Mode

IPv6 Address Family Config

11-30 distribute-list prefix in

Use this command to configure a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix. The distribute list is applied to all routes received from all neighbors. Only routes permitted by the prefix list are accepted. If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

Use the **no** command to disable a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix.

distribute-list prefix *list-name* **in**

no distribute-list prefix *list-name* **in**

Parameters

list-name	A prefix list used to filter routes received from all peers based on destination prefix.

Default

The default is as follows: distribute lists are not defined.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-31 distribute-list prefix out

Use this command to configure a filter that restricte advertisement of routes based on destination prefix. Only one instance of this command may be defined for each route source (RIP. OSPF. static, connected). One instance of this command may also be configured as a global filter for outbound prefixes.

If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

When a distribute list is added, changed, or deleted for route redistribution, BGP automatically reconsiders all best routes.

Use the **no** command to reset the distribute-list out (BGP) command to the default.

distribute-list prefix *list-name* **out [protocol | connected | static]**

no distribute-list prefix *list-name* **out [protocol | connected | static]**

Parameters

list-name	A prefix list used to filter routes advertised to neighbors.
protocol | connected | static	(Optional) When a route source is specified, the distribute list applies to routes redistributed from that source. Only routes that pass the distribute list are redistributed. The protocol value may be either **rip** or **ospf**.

Default

The default is as follows: distribute lists are not defined.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-32 enable (BGP)

This command globally enables BGP, while retaining the configuration. BGP is enabled by default once you specify the local AS number with the "router bgp" command and configure a router ID with the "bgp maxas-limit" command. When you disable BGP, BGP retains its configuration. If you invoke the **no router bgp** command, all BGP configuration is reset to the default values.

When BGP is administratively disabled, BGP sends a **Notification** message to each peer with a Cease error code.

Use the **no** command globally to disable the administratrative mode of BGP on the system, while retaining the configuration.

enable

no enable

Parameters

None

Default

The default is None.

Command Mode

BGP Router Config

11-33 filter-list (BGP Router Config)

This command filters advertisements to or from a specific neighbor according to the advertisements AS-PATH. Only a single AS-PATH list can be configured in each direction for each neighbor. If you invoke the command a second time for a given neighbor, the new AS-PATH list number replaces the previous AS-PATH list number.

If you assign a neighbor filter list to a nonexistent AS-PATH access list, all routes are filtered. Issue this command in Address Family Configuration Mode to add it to a peer template.

Use the **no** command to unconfigure neighbor filter lists.

filter-list *as-path-list-number* **{in | out}**

no filter-list *as-path-list-number* **{in | out}**

Parameters

as-path-list-number	Identifies an AS-PATH list.
in	The AS-PATH list is applied to advertisements received from the neighbor.
out	The AS-PATH list is applied to advertisements to be sent to the neighbor.

Default

The default is as follows: neighbor filter lists are not defined.

Command Mode

BGP Router Config

11-34 filter-list (IPv6 Address Family Config)

This command filters BGP to apply an AS-PATH access list to UPDATE messages received from or sent to a specific neighbor. Filtering for IPv6 is independent of filtering configured for IPv4. If an UPDATE message includes both lPv4 and IPv6 NLRI, it could be filtered for lPv4 but accepted for IPv6 or vice versa.

If you assign a neighbor filter list to a nonexistent AS-PATH access list, all routes are filtered.

Issue this command in Address Family Configuration Mode to add it to a peer template.

Use the **no** command to unconfigure neighbor IPv6 filter lists.

filter-list *as-path-list-number* **{in | out}**

no filter-list *as-path-list-number* **{in | out}**

Parameters

as-path-list-number	Identifies an AS-PATH list.
in	The AS-PATH list is applied to advertisements received from the neighbor.
out	The AS-PATH list is applied to advertisements to be sent to the neighbor.

Default

The default is as follows: neighbor filter lists are not configured.

Command Mode

IPv6 Address Family Config

11-35 ip bgp fast-external-failover

This command configures fast external failover behavior for a specific routing interface.

This command overrides for a specific routing interface the fast external failover behavior configured globally. If permit is specified, the feature is enabled on the interface, regardless of the global configuration. If **deny** is specified, the feature is disabled on the interface, regardless of the global configuration.

Use the **no** command to unconfigure the feature on the interface, and the interface uses the global setting.

ip bgp fast-external-failover {permit | deny}

no ip bgp fast-external-failover

Parameters

permit	This keyword enables fast external failover on the interface, regardless of the global configuration of the feature.
deny	This keyword disables fast external failover on the interface, regardless of the global configuration of the feature.

Default

The default is global enabling of fast external failover. Interface configuration is also not enabled by default.

Command Mode

Interface Config

11-36 maximum-paths (BGP Router Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors outside the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS-PATH, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Use the **no** command to reset back to the default the number of next hops BGP may include in an ECMP route.

maximum-paths *number-of-paths*

no maximum-paths

Parameters

number-of-paths	The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or Security Device Manager (SDM) template further restricts the range.

Default

The default is a single next hop for BGP.

Command Mode

BGP Router Config

11-37 maximum-paths (IPv4 VRF Address Family Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors outside the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS-PATH, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Use the **no** command to reset back to the default the ext hops BGP may include in an ECMP route.

maximum-paths *number-of-paths*

no maximum-paths

Parameters

number-of-paths	The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

Default

The default is a single next hop for BGP.

Command Mode

IPv4 VRF Address Family Config

11-38 maximum-paths (IPv6 Address Family Config)

Use this command to limit the number of Equal Cost Multipath (ECMP) next hops in IPv6 routes from external peers. BGP may include in an ECMP route derived from paths received from neighbors outside the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS-PATH, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Use the **no** command to reset back to the default the number of ECMP next hops in IPv6 routes BGP may include in an ECMP route.

maximum-paths *number-of-paths*

no maximum-paths

Parameters

number-of-paths	The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

Default

The default is a single next hop for BGP.

Command Mode

IPv6 Address Family Config

11-39 maximum-paths igbp (BGP Router Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors within the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS-PATH, origin, MED, peer type, and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Use the **no** command to reset back to the default the number of next hops BGP may include in an ECMP route derived from paths received from neighbors within the local autonomous system.

maximum-paths igbp *number-of-paths*

no maximum-paths igbp

Parameters

number-of-paths	The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

Default

The default is a single next hop for BGP.

Command Mode

BGP Router Config

11-40 maximum-paths igbp (IPv4 VRF Address Family Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors within the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS-PATH, origin, MED, peer type, and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Use the **no** command to reset back to the default the number of next hops BGP may include in an ECMP route derived from paths received from neighbors within the local autonomous system.

maximum-paths igbp *number-of-paths*

no maximum-paths igbp

Parameters

number-of-paths	The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

Default

The default is a single next hop for BGP.

Command Mode

IPv4 VRF Address Family Config

11-41 maximum-paths igbp (IPv6 Address Family Config)

Use this command to limit the number of ECMP next hops in IPv6 routes from internal peers.

Paths are considered for ECMP when their attributes are the same (local preference, AS-PATH, origin, MED, peer type, and IGP distance) When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Use the **no** command to reset back to the default the number of ECMP next hops BGP may include in an ECMP route derived from IPv6 routes received from neighbors within the local autonomous system.

maximum-paths igbp *number-of-paths*

no maximum-paths igbp

Parameters

number-of-paths	The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

Default

The default is a single next hop for BGP.

Command Mode

IPv6 Address Family Config

11-42 maximum-prefix (BGP Router Config)

This command configures the maximum number of prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the "clear ip bgp" command is issued for the neighbor. The neighbor can also be brought back up using the "neighbor route-map (BGP Router Config)" command followed by the command **no neighbor shutdown**.

Issue this command in Address Family Configuration Mode to add it to a peer template.

Use the **no** command to revert to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

maximum-prefix {maximum | unlimited} [threshold] [warning-only]

no maximum-prefix

Parameters

maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum supported routes.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP discards excess prefixes and writes a log message rather than shutting down the adjacency.

Default

The default is as follows: prefix limit is set to the maximum number of supported routes in the forwarding table and the threshold is 75%. A neighbor exceeding the limit is shutdown unless the **warning-only** option is configured.

Command Mode

BGP Router Config

11-43 maximum-prefix (IPv6 Address Family Config)

This command specifies the maximum number of IPv6 prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the "clear ip bgp" command is issued for the neighbor. The neighbor can also be brought back up using the "neighbor shutdown" command followed by the command **no neighbor shutdown**.

Issue this command in Address Family Configuration Mode to add it to a peer template.

Use the **no** command to revert to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

maximum-prefix {maximum | unlimited} [threshold] [warning-only]

no maximum-prefix

Parameters

maximum	The maximum r of prefixes BGP will accept from this neighbor. Range is 0 to the maximum numb of routes the router supports.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP discards excess prefixes and writes a log message rather than shutting down the adjacency.

Default

The default is as follows: prefix limit is set to the maximum number of supported routes in the forwarding table and the threshold is 75%. A neighbor exceeding the limit is shutdown unless the **warning-only** option is configured.

Command Mode

IPv6 Address Family Config

11-44 neighbor activate (IPv4 VRF Address Family Config)

Use the **neighbor activate** command to enable exchange of IPv4 VRF prefixes with a neighbor.

Using this command under the **address-family vpnv4 unicast** mode enables the local BGP router to send IPv4 VRF prefixes to its BGP peer across the backbone. Each address carried in an NLRI is prefixed with an 8-byte Route distinguisher value.

When IPv4 VRF is enabled for a neighbor, the adjacency is brought down and restarted to communicate the change to the peer. It is recommended that the user completely configures all the required IPv4 routing policies for the peer before activating the peer.

Use the **no** command to disable exchange of IPv4 VRF prefixes with the neighbor and to disassociate the export map for the specified VRF instance.

neighbor *prefix* **activate**

no neighbor *prefix* **activate**

Parameters

prefix	An IPv4 address in dotted notation.

Default

The default is as follows: VPNv4 prefixes are not sent to the neighbor.

Command Mode

IPv4 VRF Address Family Config

Example

The following example enables the exchange of IPv4 VRF prefixes with the external peer at 1.1.1.1.

```
(Config)#router bgp 1
(Config-router)#neighbor 1.1.1.1 remote-as 2
(Config-router)#address-family vpnv4 unicast
(Config-router-af-vpnv4)#neighbor 1. 1 .1. 1 activate
```

11-45 neighbor activate (IPv6)

To enable exchange of IPv6 routes with a neighbor, use the neighbor activate command in IPv6 Address Family Configuration mode. The neighbor address must be the same IP address used in the neighbor remote-as command to create the peer.

When IPv6 is enabled or disabled for a neighbor, the adjacency is brought down and restarted to communicate to the change to the peer. You should completely configure IPv6 policy for the peer before activating the peer.

Use the **no** command to disable exchange of IPv6 routes.

neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} activate**

no neighbor *ipv4-address* **activate**

Parameters

ipv4-address	The IPv4 address of a peer.
ipv6-address	The IPv6 address of a peer.
interface *interface-name*	(Optional) If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto detected.

Default

The default is Disabled of IPv6 route exchange.

Command Mode

IPv6 Address Family Config

Example

The following example enables the exchange of IPv6 routes with the external peer at 172.20.1.2 and sets the next hop for IPv6 routes sent to that peer.

```
(Routing)(Config)#router bgp 1
(Routing)(Config-router)#neighbor 172.20.1.2 remote-as 2
(Routing)(Config-router)#address-family ipv6
(Routing)(Config-router-af)#neighbor 172.20.1.2.activate
(Routing)(Config-router-af)#neighbor 172.20 1.2.route-map SET-V6-NH out
(Routing)(Config-router-af)#exit
(Routing)(Config-router)#exit
(Routing)(Config)#route-map SET-V6-NH permit 10
(Routing)(route-map)#set ipv6 next:-hop 2001:1:200::1
```

11-46 neighbor advertisement-interval (BGP Router Config)

Use this command to configure the minimum time that must elapse between advertisements of the same route to a given neighbor. RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

D-LINK OS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Use the **no** command to return to the default the minimum time that must elapse between advertisements of the same route to a given neighbor.

neighbor {*ipv4-address* **|** *ipv6-address***} advertisement-interval** *seconds*

no neighbor {*ipv4-address* **|** *ipv6-address***} advertisement-interval**

Parameters

ipv4-address **|** *ipv6-address*	The neighbor's IP address.
seconds	The minimum time between route advertisement, in seconds. The range is from 0 to 600 seconds.

Default

The default is as follows: 30 seconds for external peers and 5 seconds for internal peers.

Command Mode

BGP Router Config

11-47 neighbor advertisement-interval (IPv4 VRF Address Family Config)

Use this command to configure the minimum time that must elapse between advertisements of the same route to a given neighbor. RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

D-LINK OS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Use the **no** command to return to the default the minimum time that must elapse between advertisements of the same route to a given neighbor.

neighbor *ip-address* **advertisement-interval** *seconds*

no neighbor *ip-address* **advertisement-interval**

Parameters

ip-address	The neighbor's IPv4 address.
seconds	The minimum time between route adverfisement, in seconds. The range is from 0 to 600 seconds.

Default

The default is as follows: 30 seconds for external and 5 seconds for internal peers.

Command Mode

IPv4 VRF Address Family Config

11-48 neighbor advertisement-interval (IPv6 Address Family Config)

ln IPv6 Address Family mode, this command controls the time between sending Update messages containing IPv6 routes. D-LINK OS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Use the **no** command to return to the default the minimum time that must elapse between advertisements of the same IPv6 route to a given neighbor.

neighbor *ip-address* **advertisement-interval** *seconds*

no neighbor *ip-address* **advertisement-interval**

Parameters

ip-address	The neighbor's IPv4 address.
seconds	The minimum time between route adverfisement, in seconds. The range is from 0 to 600 seconds.

Default

The default is as follows: 30 seconds for external and 5 seconds for internal peers.

Command Mode

IPv6 Address Family Config

11-49 neighbor connect-retry-interval

Use this command to configure the initial connection retry time for a specific neighbor. If a neighbor does not respond to an initial TCP connection attempt, D-LINK OS retries three times. The first retry is after the retry interval configured with neighbor connect-retry-interval. Each subsequent retry doubles the previous retry interval. So by default, the TCP connection is retried after 2, 4, and 8 seconds. If none of the retries is successful, the adjacency is reset to the IDLE state and the IDLE hold timer is started. BGP skips the retries and transitions to IDLE state if TCP returns an error, such as destination unreachable, on a connection attempt.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to reset to the default the initial connection retry time for a specific neighbor.

neighbor {*ip-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} connect-retry-interval** *retty-time*

no neighbor *ip-address* **connect-retry-interval**

Parameters

ip-address	The neighbor’s IP address.
ipv6-address	The neighbor’s IPv6 address.
interface *interface-name*	(Optional) If the neighbor’s IPv6 address is a link local address, the local

	interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbors link local iPv6 address is auto-detected.
retty-time	The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

Default

The default is 2 seconds.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config
- Peer Template Config

11-50 neighbor connect-retry-interval (IPv4 Address Family Config)

Use this command to configure the initial connection retry time for a specific neighbor. If a neighbor does not respond to an initial TCP connection attempt, D-LINK OS retries three times. The first retry is after the retry interval configured with neighbor connect-retry-interval. Each subsequent retry doubles the previous retry interval. So by default, the TCP connection is retried after 2, 4, and 8 seconds. If none of the retries is successful, the adjacency is reset to the IDLE state and the IDLE hold timer is started. BGP skips the retries and transitions to IDLE state if TCP returns an error, such as destination unreachable, on a connection attempt.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to reset to the default the initial connection retry time for a specific neighbor.

neighbor {*ip-address* **| autodetect interface** *interface-name***} connect-retry-interval** *retry-time*

no neighbor *ip-address* **connect-retry-interval**

Parameters

ip-address	The neighbors IP address.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local iPv6 address is auto-detected.
retry-time	The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

Default

The default is 2 seconds.

Command Mode

IPv4 VRF Address Family Config

11-51 neighbor default-originate (BGP Router Config)

To configure BGP to originate a default route to a specific neighbor, use the **neighbor default-originate** command in BGP router configuration mode. Use the optional **if-default-present** parameter to originate the default route to a specific neighbor only if the default route exists in the routing table.

By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor configured with the default-originate is placed in a separate update group from the neighbors that are not configured with this command which means the global default-originate command does not affect the neighbors configured with this command. The global default-originate command is overridden by the default-originate setting for a neighbor if enabled. The AS-PATH sent in the default route update sent to the neighbor as a result of this command includes only the originator's AS. Giving the optional if-default-present tells to originate the default route to this neighbor only if the default route is present in the routing table. This form of default origination does not install a default route in the Adj RIB Out for the update group of peers so configured (it will not appear in **show ip bgp neighbor advertised-routes**).

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Use the **no** command to prevent BGP from originating a default route to a specific neighbor.

neighbor *ip-address* **default-originate [if-default-present] [route-map** *map-name***]**

no neighbor *ip-address* **default-originate [if-default-present] [route-map** *map-name***]**

Parameters

ip-address	The neighbor’s IPv4 address.
if-default-present	(Optional) Use to route the originate default route to a specific neighbor only when the default route exists in the routing table.
route-map *map-name*	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

Default

The default is No Default originated.

Command Mode

BGP Router Config

11-52 neighbor default-originate (IPv4 VRF Address Family Config)

To configure BGP to originate a default route to a specific neighbor, use the **neighbor default-originate** command in IPv4 VRF Address Family Config mode. Use the optional **if-default-present** parameter to originate the default route to a specific neighbor only if the default route exists in the routing table.

By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor configured with the default-originate is placed in a separate update group from the neighbors that are not configured with this command which means the global default-originate

command does not affect the neighbors configured with this command. The global default-originate command is overridden by the default-originate setting for a neighbor if enabled. The AS-PATH sent in the default route update sent to the neighbor as a result of this command includes only the originator's AS. Giving the optional if-default-present tells to originate the default route to this neighbor only if the default route is present in the routing table. This form of default origination does not install a default route in the Adj RIB Out for the update group of peers so configured (it will not appear in **show ip bgp neighbor advertised-routes**).

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advenised.

Use the **no** command to prevent BGP from originating a default route to a specific neighbor.

neighbor ip-address default-originate [if-default-present][route-map map-name]

no enable password

neighbor *ip-address* **default-originate [if-default-present] [route-map** *map-name***]**

no neighbor *ip-address* **default-originate [if-default-present] [route-map** *map-name***]**

Parameters

ip-address	The neighbor's IPv4 address.
if-default-present	(Optional) Use to route the originate default route to a specific neighbor only when the default route exists in the routing table.
route-map *map-name*	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

Default

The default is No Default originated.

Command Mode

IPv4 VRF Address Family Config

11-53 neighbor default-originate (IPv6 Address Family Config)

To configure BGP to originate a default IPv6 route to a specific neighbor, use the neighbor default-originate command in IPv6 Address Family configuration mode. By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the "default-information originate" command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appate in the "show ip bgp" command), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the "show ip bgp neighbors advertised-routes" command).

Origination of the default route is not subject to a prefix filter configured with the command "distribute-list prefix out".

A route map may be configured to set attributeson the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised If there is no route map with the route map name given, the default route is not advertised.

Use the **no** command to prevent BGP from originating a default IPv6 route to a specific neighbor.

neighbor *ip-address* **default-originate [route-map** *map-name***]**

no neighbor *ip-address* **default-originate [route-map** *map-name***]**

Parameters

ip-address	The neighbor's IP address.
route-map *map-name*	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

Default

The default is No Default originated.

Command Mode

IPv6 Address Family Config

11-54 neighbor description

Use this command in BGP Router Config mode to record a text description of a neighbor. The description is informational and has no functional impact.

Use the **no** command to delete the text description of a neighbor.

neighbor *ip-address* **autodetect interface** *interface-name* **description** *text*

no neighbor *ip-address* **autodetect interface** *interface-name* **description**

Parameters

ip-address	The neighbor's IP address.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto detected.
text	Text description of neighbor. Up to 80 characters are allowed.

Default

The default is No Default originated.

Command Mode

- BGP Router Config

- IPv4 VRF Address Family Config
- Peer Template Config

11-55 neighbor ebgp-multihop

To configure BGP to form neighborship with non-directly-connected external peers, use the **neighbor ebgp-multihop** command.

This command is relevant only for external BGP neighbors. For internal BGP neighbors, the TTL value remains 64 and can't be modified. A neighbor can inherit this configuration from a peer template. To make the update-source config work for external BGP neighbors, **ebgp-multihop** hop-count should be configured to increase the TTL value instead of the default TTL of 1.

Issue this command in Peer Template Configuration mode to add it to a peer template.

Use the **no** command to remove neighborships.

neighbor {*ip-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} ebgp-multihop** *hop-count*

no neighbor {*ip-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} ebgp-multihop**

Parameters

ip-address	The neighbor's IPv4 address.
ipv6-address	The neighbor's IPv6 address.
interface *interface-name*	(Optional) If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
hop-count	The maximum hop-count allowed to reach the neighbor. The allowed range is 1-255.

Default

The default is 1.

Command Mode

- BGP Router Config
- Peer Template Config

Example

```
(Routing)(Conf:ig)#router bgp 65000
(Routing)(Config-router)#neighbor 172:20.1.2 remote-as 65001
(Routing)(Config-router)#neighbor 172.20.1.2 ebgp-multihop 3
(Routing)(Config-router)#neighbor 2001::2 remote-as 65003
(Routing)(Config-router)#neighbor 2001::2 ebgp-multihop 4
```

11-56 neighbor ebgp-multihop (IPv4 Address Family Config)

To configure BGP to form neighborship with non-directly-connected external peers, use the **neighbor ebgp-multihop** command.

This command is relevant only for external BGP neighbors. For internal BGP neighbors, the TTL value remains 64 and can't be modified. A neighbor can inherit this configuration from a peer template. To make the update-source config work for external BGP neighbors, **ebgp-multihop** hop-count should be configured to increase the TTL value instead of the default TTL of 1.

Use the **no** command to remove neighborships.

neighbor {*ip-address* **| autodetect interface** *interface-name***} ebgp-multihop** *hop-count*

no neighbor {*ip-address* **| autodetect interface** *interface-name***} ebgp-multihop**

Parameters

ip-address	The neighbor's IPv4 address.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
hop-count	The maximum hop-count allowed to reach the neighbor. The allowed range is 1-255.

Default

The default is 1.

Command Mode

IPv4 VRF Address Family Config

Example

```
(Routing)(Config)#router bgp 65000
(Routing)(Config-router)#neighbor 172.20.1.2 remote-as 65001
(Routing)(Config-router)#neighbor 172.20.1.2 ebgp-multihop 3
(Routing)(Config-router)#neighbor 2001::2 remote-as 65003
(Routing)(Config-router)#neighbor 2001::2 ebgp-multihop 4
```

11-57 neighbor filter-list (BGP Router Config)

This command filters advertisements to or from a specific neighbor according to the advertisements AS-PATH. Only a single AS-PATH list can be configured in each direction for each neighbor. If you invoke the command a second time for a given neighbor, the new AS-PATH list number replaces the previous AS-PATH list number.

If you assign a neighbor filter list to a non-existent AS-PATH access list, all routes are filtered.

Use the **no** command to unconfigure neighbor filter lists.

neighbor {*ipv4-address* **|** *ipv6-address***} filter-list** *as-path-list-number* **{in | out}**

no neighbor {*ipv4-address* **|** *ipv6-address***} filter-list** *as-path-list-number* **{in | out}**

Parameters

ipv4-address | *ipv6-address*	The neighbors IP address.
as-path-list-number	Identifies an AS-PATH list.
in	The AS-PATH list is applied to advertisements received from the neighbor.
out	The AS-PATH list is applied to advertisements to be sent to the neighbor.

Default

The default is No Neighbor Filter Lists configured.

Command Mode

BGP Router Config

11-58 neighbor filter-list (IPv4 VRF Address Family Config)

This command filters advertisements to or from a specific neighbor according to the advertisements AS-PATH.Only a single AS-PATH list can be configured in each direction for each neighbor. If you invoke the command a second time for a given neighbor, the new AS-PATH list number replaces the previous AS-PATH list number.

lf you assign a neighbor filter list to a nonexistent AS-PATH access list, all routes are filtered.

Use the **no** command to unconfigure neighbor filter lists.

neighbor *ip-address* **filter-list** *as-path-list-number* **{in | out}**

no neighbor *ip-address* **filter-list** *as-path-list-number* **{in | out}**

Parameters

ip-address	The neighbor’s IPv4 address.
as-path-list-number	Identifies an AS-PATH list.
in	The AS-PATH list is applied to advertisements received from the neighbor.
out	The AS-PATH list is applied to advertisements to be sent to the neighbor.

Default

The default is No Neighbor Filter Lists configured.

Command Mode

IPv4 VRF Address Family Config

11-59 neighbor filter-list (IPv6 Address Family Config)

This command filters BGP to apply an AS-PATH access list to UPDATE messages received from or sent to a specific neighbor. Filtering for IPv6 is independent of filtering configured for IPv4. If an UPDATE message includes both IPv4 and IPv6 NLRI, it could be filtered for IPv4 but accepted for IPv6 or vice versa.

If you assign a neighbor filter list to a non-existent AS-PATH access list, all routes are filtered.

Use the **no** command to unconfigure neighbor IPv6 filter lists.

neighbor *ip-address* **filter-list** *as-path-list-number* **{in | out}**

no neighbor *ip-address* **filter-list** *as-path-list-number* **{in | out}**

Parameters

ip-address	The neighbors IP address.
as-path-list-number	Identifies an AS-PATH list.
in	The AS-PATH list is applied to advertisements received from the neighbor.
out	The AS-PATH list is applied to advertisements to be sent to the neighbor.

Default

The default is No Neighbor Filter Lists configured.

Command Mode

IPv6 Address Family Config

11-60 neighbor inherit peer (BGP Router Config)

To configure a BGP peer to inherit peer configuration parameters from a peer template, use the neighbor inherit peer command in Router Configuration mode. Neighbor session and policy parameters can be configured once in a peer template and inherited by multiple neighbors, eliminating the need to configure the same parameters for each neighbor. Parameters are inherited from the peer template specified and from any templates it inherits from. A neighbor can inherit directly from only one peer template.

Use the **no** command in Router Configuration mode to remove the inheritance.

neighbor {*ip-address* **|** *ipv6-address* **[interface** *interface-name***] autodetect interface** *interface-name* **inherit peer** *template-name*

no neighbor *ip-address* **inherit peer** *template-name*

Parameters

ip-address	The IP address of a neighbor whose configuration parameters are inherited from the peer template.
ipv6-address	The neighbor's IPv6 address.
interface *interface-name*	(Optional) If the neighbor's IPv6 address is a link local address, the local interface must be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
template-name	The name of the peer template whose peer configuration parameters are to be inherited by this neighbor.

Default

The default is No Peer Configuration Parameters are inherited.

Command Mode

BGP Router Config

Example

The following shows an example of the command.

```
(Routing)(Config)#router bgp 65000
(Routing)(Config-router)#neighbor 172.20.1.2 remote-as 65001
(Routing)(Config-router)#neighbor 172.20.2.2 remote-as 65001
(Routing)(Config-router)#template peer AGGR
(Routing)(Config-rtr-tmp)#timers 3 9
(Routing)(Config-rtr-tmp)#address-family ipv4
(Routing)(Config-rtr-tmp-af)#send-community
(Routing)(Config-rtr-tmp-af)#route-map RM4-IN in
(Routing)(Config-rtr-tmp-af)#route-map RM4-OUT out
(Routing)(Config-rtr-tmp-af)#exit
(Routing)(Config-rtr-tmp)#exit
(Routing)(Config-router)#neighdor 172.20.1.2 inherit peer AGGR
(Routing)(Config-router)#neighdor 172.29.2.2 inherit peer AGGR
```

11-61 neighbor inherit peer (IPv4 Address Family Config)

To configure a BGP peer to inherit peer configuration parameters from a peer template, use the neighbor inherit peer command in Router Configuration mode. Neighbor session and policy parameters can be configured once in a peertemplate and inherited by multiple neighbors, eliminating the need to configure the same parameters for each neighbor. Parameters are inherited from the peer template specified and from any templates it inherits from. A neighbo r can inherit directly from only one peer template.

Use the **no** command in Router Configuration mode to remove the inheritance.

neighbor {*ip-address* **| autodetect interface** *interface-name* **inherit peer** *template-name*

no neighbor *ip-address* **inherit peer** *template-name*

Parameters

ip-address	The IP address of a neighbor whose configuration parameters are inherited from the peer template.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
template-name	The name of the peer template whose peer configuration parameters are to be inherited by this neighbor.

Default

The default is No Peer Configuration Parameters are inherited.

Command Mode

IPv4 VRF Address Family Config

Example

The following shows an example of the command.

```
(Routing)(ConFig)#router bgp 65000
(Routing)(Config-router)#neighbor 172.20.1.2 remote-as 65001
(Routing)(Config-router)#neighbor 172.29.2.2 remote-as 65001
(Routing)(Config-router)#template peer AGGR
(Routing)(Config-rtr-tmp)#timers 3 9
(Routing)(Config-rtr-tmp)#address-family ipv4
(Routing)(Config-rtr-tmp-af)#send-community
(Routing)(Config-rtr-tmp-af)#route-map RM4-IN in
(Routing)(Config-rtr-tmp-af)#route-map RM4-OUT out
(Routing)(Config-rtr-tmp-af)#exit
(Routing)(ConFig-rtr-tmp)#exit
(Routing)(Config-router)#neighbor 172.20.1.2 inherit peer AGGR
(Routing)(Config-router)#neighbor 172.20.2.2 inherit peer AGGR
```

11-62 neighbor local-as (BGP Router Config)

To configure BGP to advertise the local-as instead of the router's own AS in the routes advertised to the neighbor, use the **neighbor local-as** command in Router Configuration mode. This command is only allowed on the external BGP neighbors. A neighbor can inherit this configuration from a peer template.

neighbor {*ip-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} local-as** *as-number* **no-prepend replace-as**

Parameters

ip-address	The neighbor's IPv4 address.
ipv6-address	The neighbor's IPv6 address.
interface *interface-name*	If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.
as-number	The AS number to advertise as the local AS in the AS-PATH sent to the neighbor.
no-prepend	Does not prepend the local-AS in the AS-PATH received in the updates from this neighbor.
replace-as	Replaces the router's own AS with the local-AS in the AS-PATH sent to the neighbor.

Default

The default is No Local AS configured on a peer.

Command Mode

BGP Router Config

Example

```
(Routing)(Config)#router bgp 65000
(Routing)(Config-router)#neighbor 172.20.1.2 remote-as 65001
(Routing)(Config-router)#neighbor 172.20.1.2 local-as 65002 no-prepend replace-as
(Routing)(Config-router)#neighbor 2001::2 remote-as 65003
(Routing)(Config-router)#neighbor 2001::2 local-as 65002 no-prepend replace-as
```

11-63 neighbor local-as (IPv4 VRF Address Family Config)

To configure BGP to advertise the local-as instead of the router's own AS in the routes advertised to the neighbor, use the **neighbor local-as** command in Router Configuration mode. This command is only allowed on the external BGP neighbors. A neighbor can inherit this configuration from a peer template.

neighbor {*ip-address* **| autodetect interface** *interface-name***} local-as** *as-number* **no-prepend replace-as**

Parameters

ip-address	The neighbor's IPv4 address.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.
as-number	The AS number to advertise as the local AS in the AS-PATH sent to the neighbor.

no-prepend	Does not prepend the local-AS in the AS-PATH received in the updates from this neighbor.
replace-as	Replaces the router's own AS with the local-AS in the AS-PATH sent to the neighbor.

Default

The default is No Local AS configured on a peer.

Command Mode

IPv4 VRF Address Family Config

Example

The following shows an example of the command.

```
(R1)(Config)#router bgp 65000
(R1)(Config-router)#neighbor 172.20.1.2 remote-as 65001
(R1)(Config-router)#neighbor 172.20.1.2 local-as 65002 no-prepend replace-as
(R1)(Config-router)#neighbor 2001::2 remote-as 65003
(R1)(Config-router)#neighbor 2001::2 local-as 65002 no-prepend replace-as
```

11-64 neighbor maximum-prefix (BGP Router Config)

This command configures the maximum number of prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the "clear ip bgp" command is issued for the neighbor. The neighbor can also be brought back up using the "neighbor route-map (BGP Router Config)" command followed by the command **no neighbor shutdown**.

Use the **no** command to revert to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

neighbor {*ipv4-address* **|** *ipv6-address***} maximum-prefix {***maximum* **| unlimited} [***threshold***] [warning-only]**

no neighbor {*ipv4-address* **|** *ipv6-address***} maximum-prefix**

Parameters

ipv4-address | *ipv6-address*	The neighbor's IPv4 or IPv6 address.
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do nct enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes,

	BGP accepts the excess prefixes and writes a log message rather than shutting down the adjacency.

Default

The default is Prefix Limit maximum number of supported routes in the forwarding table. The default warning threshold is 75%. Neighbors exceeding the limit are shutdown unless the **warning-only** option is configured.

Command Mode

BGP Router Config

11-65 neighbor maximum-prefix (IPv4 VRF Address Family Config)

This command configures the maximum number of prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the "clear ip bgp" command is issued for the neighbor. The neighbor can also be brought back up using the "neighbor shutdown" command followed by the command **no neighbor shutdown**.

Use the **no** command to revert to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

neighbor *ip-address* **maximum-prefix {***maximum* **| unlimited} [***threshold***] [warning-only]**

no neighbor *ip-address* **maximum-prefix**

Parameters

ip-address	The neighbor's IPv4 address.
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do nct enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP accepts the excess prefixes and writes a log message rather than shutting down the adjacency.

Default

The default is Prefix Limit maximum number of supported routes in the forwarding table. The default warning threshold is 75%. Neighbors exceeding the limit are shutdown unless the **warning-only** option is configured.

Command Mode

IPv4 VRF Address Family Config

11-66 neighbor maximum-prefix (IPv6 Address Family Config)

This command specifies the maximum number of IPv6 prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down. the adjacency stays down until the "clear ip bgp" command is issued for the neighbor. The neighbor can also be brought back up using the "neighbor shutdown" command followed by the command **no neighbor shutdown**.

Use the **no** command to revert to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

neighbor *ip-address* **maximum-prefix {***maximum* **| unlimited} [***threshold***] [warning-only]**

no neighbor *ip-address* **maximum-prefix**

Parameters

ip-address	The neighbor's IP address.
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do nct enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP accepts the excess prefixes and writes a log message rather than shutting down the adjacency.

Default

The default is Prefix Limit maximum number of supported routes in the forwarding table. The default warning threshold is 75%. Neighbors exceeding the limit is shutdown unless the **warning-only** option is onfigured.

Command Mode

IPv6 Address Family Config

11-67 neighbor next-hop-self (BGP Router Config)

This command configures BGP to set the next hop attribute to a local IP address when advertising a route to an internal peer. Normally, BGP would retain the next hop attribute received from the external peer.

When the next hop attribute in routes from external peers is retained, internal peers must have a route to the external peer's IP address. This is commonly done by configuring the IGP on the border router to advertise the external (or DMZ) subnet. The next-hop-self option eliminates the need to advertise the external subnet in the IGP.

Use the **no** command to disable the peer as the next hop for the locally originated paths. After executing this command,the BGP peer must be reset before the changes take effect.

neighbor {*ipv4-address* **|** *ipv6-address***} next-hop-self**

no neighbor {*ipv4-address* **|** *ipv6-address***} next-hop-self**

Parameters

ipv4-address | *ipv6-address*	The neighbor's IPv4 or IPv6 address.

Default

The default is not Enabled.

Command Mode

BGP Router Config

11-68 neighbor next-hop-self (IPv4 VRF Address Family Config)

This command configures BGP to set the next hop attribute to a local IP address when advertising a route to an internal peer. Normally, BGP would retain the next hop attribute received from the external peer.

When the next hop attribute in routes from external peers is retained, internal peers must have a route to the external peer's IP address. This is commonly done by configuring the IGP on the border router to advertise the external (or DMZ) subnet. The next-hop-self option eliminates the need to advertise the external subnet in the IGP.

Use the **no** command to disable the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

neighbor *ip-address* **next-hop-self**

no neighbor *ip-address* **next-hop-self**

Parameters

ip-address	The neighbor's IP address.

Default

The default is Disabled.

Command Mode

IPv4 VRF Address Family Config

11-69 neighbor next-hop-self (IPv6 Address Family Config)

This command configures BGP to use a local address as the IPv6 next hop when advertising IPv6 routes to a specific peer. For IPv6, BGP uses an IPv6 address from the local interface that terminates the IPv4 peering session.

Use the **no** command to disable the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

neighbor *ip-address* **next-hop-self**

no neighbor *ip-address* **next-hop-self**

Parameters

ip-address	The neighbor's IP address.

Default

The default is Disabled.

Command Mode

IPv6 Address Family Config

11-70 neighbor password

Use this command to enable MD5 authentication of TCP segments sent to and received from a neighbor, and configures an authentication key.

MD5 must either be enabled or disabled on both peers. The same password must be configured on both peers. After a TCP connection is established, if the password on one end is changed, then the password on the other end must be changed to match before the hold time expires. With default hold times, both passwords must be changed within 120 seconds to guarantee the connection is not dropped.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to disable MD5 authentication of TCP segments sent to and received from a neighbor.

neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *Interface-name***} password** *string*

no neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *Interface-name***} password**

Parameters

ip-address	The neighbor's IPv4 address.
ipv6-address	The neighbor's IPv6 address.
interface *interface-name*	If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface	The routing interface on which the neighbors link local IPv6 address is

interface-name	auto-detected.
string	Case-sensitive password from 1 to 25 characters in length.

Default

The default is MD5 Authentication Disabled.

Command Mode

- BGP Rouier Config
- Peer Template Config

11-71 neighbor password (IPv4 VRF Address Family Config)

Use this command to enable MD5 authentication of TCP segments sent to and received from a neighbor, and configures an authentication key.

MD5 must either be enabled or disabled on both peers. The same password must be configured on both peers. After a TCP connection is established, if the password on one end is changed, then the password on the other end must be changed to match before the hold time expires. With default hold times, both passwords must be changed within 120 seconds to guarantee the connection is dropped.

Use the **no** command to disable MD5 authentication of TCP segments sent to and received from a neighbor.

neighbor {*ip -address* **| autodetect interface** *Interface-name***} password** *string*

no neighbor {*ip -address* **| autodetect interface** *Interface-name***} password**

Parameters

ip-address	The neighbor's IPv4 address.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.
string	Case-sensitive password from 1 to 25 characters in length.

Default

The default is MD5 Authentication Disabled.

Command Mode

IPv4 VRF Address Family Config

11-72 neighbor prefix-list

This command filters advertisements sent to a specific neighbor based on the destination prefix of each route.

Only one prefix list may be defined for each neighbor in each direction. If you assign a prefix list that does not exist, all prefixes are permitted.

Use the **no** command to disable filtering advertisements sent to a specific neighbor based on the destination prefix of each route.

neighbor {*ipv4-address* **|** *ipv6-address***) prefix-list** *prefix-list-name* **{in | out}**

no enable password

Parameters

ipv4-address **|** *ipv6-address*	The neighbor's IPv4 or IPv6 address.
prefix-list-name	The name of an IP prefix list.
in	Apply the prefix list to advertisements received from this neighbor.
out	Apply the prefix list to advertisements to be sent to this neighbor.

Default

The default is Prefix List not configured.

Command Mode

BGP Router Config

11-73 neighbor remote-as (BGP Router Config)

This command configures a neighbor and identifies the neighbor's autonomous system. The neighbor's AS number must be specified when the neighbor is created. Up to 256 neighbors may be configured. inheriting a template with the remote-as parameter automatically creates the neighbor if the neighbor does not exist.

Use the **no** command to unconfigure neighbors.

neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name* **remote-as** *as-number*

no neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name* **remote-as**

Parameters

ipv4-address	The neighbor's IPv4 address.
ipv6-address	The neighbor's IPv6 address.
interface *interface-name*	If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.

as-number	The autonomous system number of the neighbor's AS. The range is 1 to 429496729. If the neighbor's AS number is the same as the local router, the peer is an internal peer. Otherwise, the peer is an external peer. A neighbor can inherit this configuration from a peer template.

Default

The default is Neighbors not configured.

Command Mode

- BGP Router Config
- Peer Template Config

11-74 neighbor remote-as (IPv6 Address Family Config)

This command configures a neighbor and identifies the neighbor's autonomous system. The neighbor's AS number must be specified when the neighbor is created. Up to 128 neighbors may be configured. inheriting a template with the remote-as parameter automatically creates the neighbor if the neighbor does not exist.

Use the **no** command to unconfigure neighbors.

neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name* **remote-as** *as-number*

no neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name* **remote-as**

Parameters

ipv4-address	The neighbor's IPv4 address.
ipv6-address	The neighbor's IPv6 address.
interface *interface-name*	If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.
as-number	The autonomous system number of the neighbor's AS. The range is 1 to 65,535. If the neighbor's AS number is the same as the local router, the peer is an internal peer. Otherwise, the peer is an external peer. A neighbor can inherit this configuration from a peer template.

Default

The default is Neighbors not configured.

Command Mode

- IPv6 Address Family Config
- Peer Template Config

11-75 neighbor remove-private-as (BGP Router Config)

Use this command in router configuration mode to remove private AS numbers when advertising IPv4 routes to an external peer. To stop removing private AS numbers, use the no form of this command.

This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS-PATH includes any non-private AS numbers. The AS-PATH advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Although 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Use the **no** command to stop removing private AS numbers.

neighbor *ip-address* **remove-private-as [all replace-as]**

no neighbor *ip-address* **remove-private-as**

Parameters

ip-address	The neighbor's IPv4 address.
all replace-as	(Optional) To retain the original AS-PATH length, replace each Private AS number with the local AS number.

Default

The default is Private AS numbers not removed.

Command Mode

BGP Router Config

11-76 neighbor remove-private-as (IPv4 VRF Address Family Config)

Use this command in router configuration mode to remove private AS numbers when advertising IPv4 routes to an external peer. To stop removing private numbers, use the no form of this command.

This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS-PATH includes any non-private AS numbers. The AS-PATH advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Althou 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Use the **no** command to remove private AS numbers.

neighbor *ip-address* **remove-private-as [all replace-as]**

no neighbor *ip-address* **remove-private-as**

Parameters

ip-address	The neighbor's IPv4 address.
all replace-as	(Optional) To retain the original AS-PATH length, replace each Private AS number with the local AS number.

Default

The default is Private AS numbers not removed.

Command Mode

IPv4 VRF Address Family Config

11-77 neighbor remove-private-as (IPv6 Address Family Config)

Use this command in router configuration mode to remove private AS numbers when advertising IPv6 routes to an external peer. To stop removing private AS numbers, use the no form of this command.

This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS-PATH includes any non-private AS numbers. The AS-PATH advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Although 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Use the **no** command to stop removing private AS numbers.

neighbor *ip-address* **remove-private-as [all replace-as]**

no neighbor *ip-address* **remove-private-as**

Parameters

ip-address	The neighbor's IPv4 or IPv6 address.
all replace-as	(Optional) To retain the original AS-PATH length, replace each Private AS number with the local AS number.

Default

The default is Private AS numbers not removed.

Command Mode

IPv6 Address Family Config

11-78 neighbor rfc5549-support

To enable advertisement of IPv4 routes over IPv6 next hops selectively to an external BGP IPv6 peer, use the **neighbor rfc5549-support** command. This command may only be applied to external BGP peers via single hop.

Use the **no** command to disable advertisement of IPv4 route over IPv6 next hops.

neighbor {*ipv6-address* **| autodetect interface** *interface-name***} rfc5549-support**

no neighbor {*ipv6-address* **| autodetect interface** *interface-name***} rfc5549-support**

Parameters

ipv6-address	The neighbor's IPv6 address.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto detected.

Default

The default is RFC 5549 support for IPv6 neighbors enabled.

Command Mode

BGP Router Config

Example

The following shows an example of the command.

```
(Routing)#configure
(Routing)(Config)#router bgp 100
(Routing)(Config-router)#neighbor 2001::2 rfc5549-support
```

11-79 neighbor route-map (BGP Router Config)

To apply a route map to incoming or outgoing routes for a specific neighbor, use the **neighbor route-map** command in Router Configuration mode. A route map can be used to change the local preference, MED, or AS-PATH of a route. Routes can be selected for filtering or modification using an AS-PATH access list or a prefix list.

Use the **no** command to remove the route map.

neighbor {*ipv4-address* **|** *ipv6-address***} route-map** *map-name* **{in | out}**

no neighbor {*ipv4-address* **|** *ipv6-address***} route-map** *map-name* **{in | out}**

Parameters

ipv4-address **|** *ipv6-address*	The neighbor's IPv4 or IPv6 address.
map-name	The name of the route map to be applied.
**in	out**	Whether the route map is applied to incoming or outgoing routes.

Default

The default Route Maps are not applied.

Command Mode

BGP Router Config

11-80 neighbor route-map (IPv4 VRF Address Family Config)

To apply a route map to incoming or outgoing routes for a specific neighbor, use the **neighbor route-map** command in Router Configuration mode. A route map can be used to change the local preference, MED, or AS-PATH of a route. Routes can be selected for filtering or modification using an AS-PATH access list or a prefix list.

Use the **no** command to remove the route map.

neighbor *ip-address* **route-map** *map-name* **{in | out}**

no neighbor *ip-address* **route-map** *map-name* **{in | out}**

Parameters

ip-address	The neighbor's IP address.
map-name	The name of the route map to be applied.
in | out	Whether the route map is applied to incoming or outgoing routes.

Default

The default Route Maps are not applied.

Command Mode

IPv4 VRF Address Family Config

11-81 neighbor route-map (IPv6 Address Family Config)

This command specifie a route map to be applied to inbound or outbound IPv6 routes.

Use the **no** command to remove the route map.

neighbor *ip-address* **route-map** *map-name* **{in | out}**

no neighbor *ip-address* **route-map** *map-name* **{in | out}**

Parameters

ip-address	The neighbor's IP address.

map-name	The name of the route map to be applied.
in | out	Whether the route map is applied to incoming or outgoing routes.

Default

The default Route Maps are not applied.

Command Mode

IPv6 Address Family Config

11-82 neighbor route-reflector-client (BGP Router Config)

Use this command in BGP router configuration mode to configure an internal peer as an IPv4 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the bgp cluster-id command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Use the **no** command to remove the IPv4 route reflector client.

neighbor {*ip-address***} reoute-reflector-client**

no neighbor {*ip-address***} reoute-reflector-client**

Parameters

ip-address	The neighbor's IPv4 address.

Default

The default is Peers are not route reflector clients.

Command Mode

BGP Router Config

11-83 neighbor route-reflector-client (IPv4 VRF Address Family Config)

Use this command in IPv4 VRF Address Family mode to configure an internal peer as an IPv4 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the bgp cluster-id command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Use the **no** command to remove the IPv4 route reflector client.

neighbor {*ip-address***} reoute-reflector-client**

no neighbor {*ip-address***} reoute-reflector-client**

Parameters

ip-address	The neighbor's IPv4 address.

Default

The default is Peers are not route reflector clients.

Command Mode

IPv4 VRF Address Family Config

11-84 neighbor route-reflector-client (IPv6 Address Family Config)

Use this command in IPv6 Addres Family Config mode to configure an internal peer as an IPv6 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a rout ctor client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

lf you configuremultiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same ID. Use the bgp cluster-id command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Use the **no** command to remove the IPv6 reflector client.

neighbor {*ip-address***} reoute-reflector-client**

no neighbor {*ip-address***} reoute-reflector-client**

Parameters

ip-address	The neighbor's IPv4 or IPv6 address.

Default

The default is Peers are not route reflector clients.

Command Mode

IPv6 Address Family Config

11-85 neighbor send-community extended

To configure the local router to send the BGP community attributes in Update messages to a specific neighbor, use the **neighbor send-community extended** command in BGP VPNv4 Address Family Configuration mode.

Using this command under the **address-family vpnv4 unicast** mode enables the local BGP router to send extended communities attribute to its BGP peer across the backbone. The neighbor address must be the same IP address used in the **neighbor remote-as** command to create the peer.

Use the **no** command to disable the exchange of VPNv4 prefixes with the neighbor.

neighbor *ip-address* **send-community [extended | both]**

no neighbor *ip-address* **send-community**

Parameters

ip-address	The neighbor's IPv4 address.
extended | both	(Optional) One of the following: • extended enables the router to send only extended community attributes. • both enables the router to send both standard and extended community attributes.

Default

The default is Extended Communities Attribute is not sent.

Command Mode

VPNv4 Address Family Config

Example

The following example enables sending of the extended communities attribute to external peer at 1.1.1.1.

```
(Config)#router bgp 1
(Config-router)#neighbor 1.1.1.1 remote-as 2
(Config-router)#address-family vpnv4 unicast(R1)(Config-router-af-vpnv4)#neighbor
1.1.1.1 send-communlty extended
```

```
(Config-router-af-vpnv4)#neighbor 1.1.1.1 activate
```

11-86 neighbor send-community

To configure the local router to send the BGP community attributes in Update messages to a specific neighbor, use the **neighbor send-community** command.

Use the **no** command to return to the default configuration.

neighbor {*ipv4-address* **|** *ipv6-address***) send-community**

no neighbor {*ipv4-address* **|** *ipv6-address***) send-community**

Parameters

ipv4-address **|** *ipv6-address*	The neighbor's IPv4 or IPv6 address.

Default

The default is Communities Attribute is not sent to neighbors.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config
- IPv6 Address Family Config

11-87 neighbor send-community (IPv4 VRF Address Family Config)

To configure the local router to send the BGP community attributes in Update messages to a specific neighbor, use the **neighbor send-community** command.

Use the **no** command to return to the default configuration.

neighbor *ipv4-address* **send-community**

no neighbor *ipv4-address* **send-community**

Parameters

ipv4-address	The neighbor's IPv4 address.

Default

The default is Communities Attribute is not sent to neighbors.

Command Mode

IPv4 VRF Address Family Config

11-88 neighbor shutdown

Use this command to bring down the adjacency with a specific neighbor. If the adjacency is up when the command is given, the peering session is dropped and all route information learned from the neighbor is purged.

When a neighbor is shut down, BGP first sends a NOTIFICATION message with a Cease error code. When an adjacency is administratively shut down, the adjacency stays down until administratively reenabled (using the command no neighbor shutdown).

Issue this command in Peer Template Configuration Mode to to a peer template.

Use the **no** command to enable a BGP peer administratively.

neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} shutdown**

no neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} shutdown**

Parameters

ipv4-address **|** *ipv6-address*	The neighbor's IPv4 or IPv6 address on the link that connects the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
interface *interface-name*	(Optional) Specify the local interface (*interface-name*) when the neighbor's IPv6 address is a local link address.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.

Default

The default is as follows: Neighbors are not shutdown.

Command Mode

- BGP Router Config
- Peer Template Config

11-89 neighbor shutdown (IPv4 VRF Address Family Config)

Use this command to bring down the adjacency with a specific neighbor. If the adjacency is up when the command is given, the peering session is dropped and all route information learned from the neighbor is purged.

When a neighbor is shut down, BGP first sends a NOTIFICATION message with a Cease error code. When an adjacency is administratively shut down, the adjacency stays down until administratively reenabled (using the command no neighbor shutdown).

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to enable a BGP peer administratively.

neighbor { neighbor {*ipv4-address* **| autodetect interface** *interface-name***} shutdown**

no neighbor {*ipv4-address* **| autodetect interface** *interface-name***} shutdown**

Parameters

ipv4-address	The neighbor's IPv4 address on the link that connects the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
interface *interface-name*	Indicates a specified interface name on the link connecting the two peers.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.

Default

The default is as follows: Neighbors are not shutdown.

Command Mode

IPv4 VRF Address Family Config

11-90 neighbor timers

Use this command to override the global timer values and set the keepalive and hold timers for a specific neighbor. The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an adjacency is formed.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to revert the keep alive and hold time for a peer to their defaults. After executing this command, the BGP peer must be reset before the changes will take effect.

neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autocletect interface** *interface-name***} timers** *keepalive holdtime*

no neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autocletect interface** *interface-name***} timers**

Parameters

ipv4-address **|** *ipv6-address*	The neighbor's IPv4 or IPv6 address on the link that connects the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
interface *interface-name*	(Optional) Indicates a specified interface name on the link connecting the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.

keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is from 0 to 65,535 seconds. Jitter is applied to the keepalive interval.
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0 to 65,535 seconds.

Default

The default for <keepalive> is 60 seconds.

The default for <holdtime> is 180 seconds.

Command Mode

- BGP Router Config
- Peer Template Config

11-91 neighbor timers (IPv4 VRF Address Family Config)

Use this command to override the global timer values and set the keepalive and hold timers for a specific neighbor. The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an ad adjacency is formed.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to revert the keep alive and hold time for a peer to their defaults. After executing this command, the BGP peer must be reset before the changes will take effect.

neighbor {*ipv4-address* **| autocletect interface** *interface-name***} timers** *keepalive holdtime*

no neighbor {*ipv4-address* **| autocletect interface** *interface-name***} timers**

Parameters

ipv4-address	The neighbor's IPv4 address. This is the IP address on the link that connects the two peers.
autodetect interface *interface-name*	The routing interface on which the neighbors link local IPv6 address is auto-detected.
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is from 0 to 65,535 seconds. Jitter is applied to the keepalive interval.
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is from 0 to 65,535 seconds.

Default

The default is Keepalive and Hold Timers are configured to values by "redistribute (IPv4 VRF Address Family Config)".

Command Mode

IPv4 VRF Address Family Config

11-92 neighbor update-source

Use this command to configure BGP to use a specific IP address as the source address for the TCP connection with a neighbor. This IP address must be the IP address configured on the peer as its neighbor address for this router.

The IP address used as the source address in IP packets sent to a neighbor must be the same address used to configure the local system as a neighbor of the neighbor router. In other words, if the update source is configured, it must be the same IP address used in the neighbor remote-as command on the peer.

It is common to use an IP address on a loopback interface because a loopback interface is always reachable, as long as any routing interface is up. The peering session can stay up as long as the loopback interface remains reachable. If you use an IP address on a routing interface, then the peering session will go down if that routing interface goes down.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to configure BGP to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} update-source** *interface*

no neighbor {*ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name***} update-source**

Parameters

ipv4-address **|** *ipv6-address*	The neighbor's IPv4 or IPv6 address. This is the IP address on the link that connects the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
interface *interface-name*	(Optional) Indicates the primary interface name on this interface for the TCP connection with the neighbor. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The neighbor's IPv6 link local address that will be auto detected on the specified interface.
interface	The primary IPv4 address on this interface is used as the source IP address for the TCP connection with the neighbor.

Default

The default is TCP Connections defined, if update source is not configured, by primary IPv4 address on outgoing interface to the neighbor.

Command Mode

- BGP Router Config
- Peer Template Config

11-93 neighbor update-source (IPv4 VRF Address Family Config)

Use this command to configure BGP to use a specific IP address as the source address for the TCP connection with a neighbor. This IP address must be the IP address configured on the peer as its neighbor address for this router.

The IP address used as the source address in IP packets sent to a neighbor must be the same address used to configure the local system as a neighbor of the neighbor router. In other words, if the update source is configured, it must be the same IP address used in the neighbor remote-as command on the peer.

It is common to use an IP address on a loopback interface because a loopback interface is always reachable, as long as any routing interface is up. The peering session can stay up as long as the loopback interface remains reachable. If you use an IP address on a routing interface, then the peering session will go down if that routing interface goes down.

The **update-source** option is not allowed for eBGP peers as this requires multi-hop eBGP to be working. Multi- hop eBGP is not supported.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Use the **no** command to configure BGP to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

neighbor {*ipv4-address* **| autodetect interface** *interface-name***} update-source** *interface*

no neighbor {*ipv4-address* **| autodetect interface** *interface-name***} update-source**

Parameters

ipv4-address	The neighbor's IPv4 address. This is the IP address on the link that connects the two peers.
interface *interface-name*	(Optional) Indicates the primary interface name on this interface for the TCP connection with the neighbor. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The neighbor's IPv6 link local address that will be auto detected on the specified interface.
interface	The primary IPv4 address on this interface is used as the source IP address for the TCP connection with the neighbor.

Default

The default is TCP Connections defined, if update source is not configured, by primary IPv4 address on outgoing interface to the neighbor.

Command Mode

IPv4 VRF Address Family Config

11-94 network (BGP Router Config)

This command configures BGP to advertise an address prefix.The prefix is only advertised if the common routing table includes a non-BGP route with the same prefix. The route may be a connected route, a static route, or a dynamic route from another routing protocol.

BGP accepts up to 64 networks per address family. The network command may specify a default route (network 0.0.0.0 mask 0.0.0.0).

If a route map is configured to set attributes on the advertised routes, **match as-path** and **match community** terms in the route map are ignored. A **match ip-address prefix-list** term is honored in this context. If your route map includes such a match term, the network is only advertised if the prefix list permits the network prefix. If there is no route map with the name given, the network is not advertised.

Use the **no** command to disable BGP from advertising an address prefix.

network *prefix* **mask** *network-mask* **[route-map** *rm-name***]**

no network *prefix* **mask** *network-mask* **[route-map** *rm-name***]**

Parameters

prefix	An IPv4 address Prefix in dotted notation.
mask *network-mask*	The network mask for the prefix in dotted quad notation (e.g., 255.255.0.0).
route-map *rm-name*	(Optional) A route map can be used to set path attributes on the route.

Default

The default is Networks are not advertised.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-95 network (IPv6 Address Family Config)

This command identifies network IPv6 prefixes that BGP originates in route advertisements to its neighbors. The prefix is only advertised if the common routing table includes a non-BGP route with the same prefix. The route may be a connected route, a static route, or a dynamic route from another routing protocol.

BGP accepts up to 64 networks per address family. The network command may specify a default route (network 0.0.0.0 mask 0.0.0.0).

If a route map is configured to set attributes on the advertised routes, match as-path and match community terms in the route map are ignored. A match ip-address prefix-list term is honored in this context. If your route map includes such a match term, the network is only advertised if the prefix list permits the network prefix. If there is no route map with the name given, the network is not advertised.

Use the **no** command to disable BGP from advertising an address prefix.

network *ipv6-address* **|** *prefix-length* **[route-map** *rm-name***]**

no network *ipv6-address* **|** *prefix-length* **[route-map** *rm-name***]**

Parameters

ipv6-address	Network IPv6 prefixes.
prefix-length	An IPv4 address prefix in dotted notation.
route-map *rm-name*	(Optional) A route map can be used to set path attributes on the route.

Default

The default is Networks are not advertised.

Command Mode

IPv6 Address Family Config

11-96 rd

Use this command to specify the route distinguisher (RD) for a VRF instance that is used to create a VPNv4 prefix. An RD creates routing and fowvarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the IPv4 prefixes to change them into globally unique VPNv4 prefixes.

An RD is either:

- 2-byte ASN-related: Composed of an autonomous system number and an arbitrary number.
- IP address-related: Composed of an IP address and an arbitrary number.
- 4-byte ASN related: Composed of an 4-byte autonomous system number and an arbitrary number.

Note: This command is effective only if BGP is running on the router. The RD for a VRF once configured cannot be removed or changed. Forthis reason, this command does not have the no form. To change the configured RD value, remove the VRF (using the **no ip vrf** command) and reconfigure the VRF.

rd *route-distinguisher*

Parameters

route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPNv4 prefix. The RD value can be specified in either of the following formats: • 16-bit AS number: your 32-bit value (Ex : 100 :11) • 32-bit IPv4 address: your 16-bit value (Ex: 10.1.1.1 :22) • 4-byte AS number: your 32-bit value (Ex : 66666 :33)

Default

The default is VRF not associated with any RD.

Command Mode

Global Config

Example

The following example shows how to configure a RD for a VRF instance in ASN format.

```
(Router)(Config)#ip vrf Red
(Router)(Config-vrf-Red)#rd 62001:10
(Router)(Config-vrf-Red)#exit
```

The following example shows how to configure a RD for a VRF instance in IP address format.

```
(Router)(Config)#ip vrf Red
(Router)(Config-vrf-Red)#rd 192.168.10.1:10
(Router)(Config-vrf-Red)#exit
```

The following example shows how to configure a RD for a VRF instance in 4-byte ASN format.

```
(Router)(Config)#ip vrf Green
(Router)(Config-vrf-Red)#rd 77777:20
(Router)(Config-vrf-Red)#exit
```

11-97 redistribute (BGP Router Config)

This command configures BGP to advertise routes learned by means outside of BGP. BGP can redistribute local (connected), static, and OSPF routes.

The distribute-list out command can also be used to filter redistributed routes by prefix. Eithera redistribute route map or a distribute list may be configured, but not both.

A default route cannot be redistributed unless the “default-information originate” command is given.

If a route map is configured, **match as-path** and **match community** terms are ignored. If no route map is configured with the name given, no prefixes are redistributed.

Use the **no** command to remove the configuration for the redistribution for BGP protocol from the specified source protocol/routers. The command **no redistribute ospf match external 1** will withdraw only OSPF external type 1 routes, ospf inter routes will still be redistributing.

redistribute {ospf |connected | static} [metric *metric-value***] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map** *map-tag***]**

no redistribute {ospf |connected | static} [metric *metric-value***] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map** *map-tag***]**

Parameters

ospf |connected | static	A source of routes to redistribute.
metric *metric-value*	(Optional) When this option is specified, BGP advertises the prefix with the Multi Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP, the MED is set to the default metric. If a default metric is not configured,

	the prefix is advertised without a MED attribute.
match	(Optional) If you configure BGP to redistribute OSPF routes, BGP by default only redistributes internal routes (OSPF intra-area and inter-area routes). Use the match option to configure BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes.
route-map *map-tag*	(Optional)A route map can be used to filter redistributed routes by destination prefix using a prefix list. A rout map can be used to set attributes on redistributed routes.

Default

The default is BGP does not distribute routes. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.

Command Mode

BGP Router Config

Example

The routes obtained from the kernel can be configured to redistributed in the kernel. The following CLI commands (in both IPv4 and Pv6) BGP Router mode use the kernel option.

```
(Routing)(Config)#router bsp 65401
(Routing)(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

(Routing)(Config-router)#redistribute

Incorrect protocol! Use '<rip|ospf|static|connected>'

(Routing)(Config-router)#address-family ipv6
(Routing)(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
```

11-98 redistribute (IPv4 VRF Address Family Config)

This command configures BGP to advertise routes learned by means outside of BGP. BGP can redistribute local (connected), static, OSPF, and RIP routes.

The distribute-list out command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

A default route cannot be redistributed unless the "default-information originate" command is given.

If a route map is configured, **match as-path** and **match community** terms are ignored. If no route map is configured with the name given, no prefixes are redistributed.

Use the **no** command to remove the configuration for the redistribution for BGP protocol from the specified source protocol/routers. The command **no redistribute ospf match external 1** will withdraw only OSPF external type 1 routes, ospf inter routes will still be redistributing.

redistribute {ospf | rip | connected | static} [metric *metric-value*] **[match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-ma** *map-tag*]

no redistribute {ospf | rip | connected | static} [metric *metric-value*] **[match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-ma** *map-tag*]

Parameters

ospf |connected | static	A source of routes to redistribute.
metric *metric-value*	(Optional) When this option is specified, BGP advertises the prefix with the Muiti Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP, the MED is set to the default metric. If a default metric is not configured, the prefix is advertised without a MED attribute.
match	(Optional) If you configure BGP to redistribute OSPF routes, BGP by default only redistributes internal routes (OSPF intra-area and inter-area routes). Use the match option to configure BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes.
route-map *map-tag*	(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list. A route map can be used to set attributes on redistributed routes.

Default

The default is BGP does not distribute routes. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.

Command Mode

IPv4 VRF Address Family Config

11-99 redistribute (IPv6 Address Family Config)

This command configures BGP to non-BGP routes from the lPv6 routing table.

The distribute-list out command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

A default route cannot be redistributed unless the "default-information originate" command is given.

If a route map is configured, **match as-path** and **match community** terms are ignored. If no route map is configured with the name given, no prefixes are redistributed.

Use the **no** command to remove the configuration for the redistribution for BGP protocol from the specified source protocol/routers. The command **no redistribute ospf match external 1** will withdraw only OSPF external type 1 routes, ospf inter routes will still be redistributing.

redistribute {ospf | rip | connected | static} [metric *metric-value***] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-ma** *map-tag***]**

no redistribute {ospf | rip | connected | static} [metric *metric-value***] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-ma** *map-tag***]**

Parameters

ospf |connected | static	A source of routes to redistribute.
metric *metric-value*	(Optional) When this option is specified, BGP advertises the prefix with the Muiti Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP, the MED is set to the default metric. If a default metric is not configured, the prefix is advertised without a MED attribute.
match	(Optional) If you configure BGP to redistribute OSPF routes, BGP by default only redistributes internal routes (OSPF intra-area and inter-area routes). Use the match option to configure BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes.
route-map *map-tag*	(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list. A route map can be used to set attributes on redistributed routes.

Default

The default is BGP does not distribute routes. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.

Command Mode

IPv6 Address Family Config

Example

The routes obtained from the kernel can be configured to redistributed in the kernel. The following CLI commands (in both IPv4 and Pv6) BGP Router mode use the kernel option.

```
(Routing)(Config)#router bgp 65401
(Routing)(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
```

```
(Routing)(Config-router)#redistribute

Incorrect protocol! Use '<rip|ospf|static|connected>'

(Routing)(Config-router)#address-family ipv6
(Routing)(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
```

11-100 route-reflector-client

Use this command in BGP router configuration mode to configure an internal peer as an IPv4 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the bgp cluster-id command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

neighbor {*ip-address***} route-reflector-client**

Parameters

ip-address	The neighbor's IPv4 address.

Default

The default is as follows: Peers are not route reflector clients.

Command Mode

BGP Router Config

11-101 route-target

Use this command to create a list of export, import, or both route target (RT) extended communities for the specified VRF instance. Enter the route-target command one time for each target extended community. Routes that are learned and carry a specific route-target extended community are imported into all VRFs configured with that extended community as an import route target.

The configured export RT is carried as an extended community in the MP-BGP format to the eBGP peer. An RT is either:

- 2-byte ASN-related: Composed of an autonomous system number and an arbitraw number.
- IP address-related: Composed of an IP address and an arbitrary number.
- 4-byte ASN related: Composed of of an 4-byte autonomous system number and an arbitrary number.

Use the **no** command to remove the route target specified for a VRF instance.

Note: This command is effective only if BGP is running on the router.

route-target {export | import | both} *rt-ext-comm*

no route-target {export | import | both} *rt-ext-comm*

Parameters

export	Exports routing information to the target VPN extended community.
import	Imports routing information from the target VPN extended community.
both	Exports/imports the routing information to/from the target VPN extended community.
rt-ext-comm	The route-target extended community attributes to be added to the list of import, export or both (import and export) route-target extended communities. The route target specifies a target VPN extended community. Like a route distinguisher, the route-target extended community can be specified in one of the following formats: • 16-bit AS number: your 32-bit value (Ex : 100 :11) • 32-bit IPv4 address: your 16-bit value (Ex : 10.1.1.1 :22) • 4-byte AS number: your 32-bit value (Ex: 66666 :33)

Default

The default is VRF does not associate with any RT.

Command Mode

Virtual Router Config

Example

The following example shows how to configure route target extended community attributes for a VRF instance in IPv4. The result of this command sequence is that VRF named Red has two export extended communities (100:10 and 300:10) and two import extended communities (300:10 and 192.168.10.1:10).

```
(Router)(Config)#ip vrf Red
(Router)(Config-vrf-Red)#route-target export 100:10
(Router)(C0nfig-vrf-Red)#route-target import 192.168.10.1:10
(Router)(Config-vrf-Red)#route-target both 300:10
(Router)(Config-vrf-Red)#route-target export 88888:80
(Router)(Config-vrf-Red)#exit
```

11-102 template peer

To create a BGP peer template and enter Peer Template Configuration mode, use the template peer command in Router Configuration mode. A peer template can be configured with parameters that apply to many peers. Neighbors can then be configured to inherit parameters from the peer template. A peer template can include both session parameters and peer policies. Peer policies are configured with an address family configuration mode and apply onty to that address family. You can configure up to 32 peer templates. When you make a change to a template, the change is immediately applied to all neighbors that inherit from the template (although policy changes are subject to a three-minute delay).

Note: D-LINK OS does not support a **remote-as** *as-number* command in Peer Template Configuration mode. The neighbor's AS number must be specified when the neighbor is created.

Use the **no** command to delete a peer template.

template peer *name*

no template peer *name*

Parameters

name	The name of the template. The name may be no more than 32 characters.

Default

The default is Peer templates are not configured.

Command Mode

BGP Router Config

Example

The following shows an example of the command.

```
(Routing)(ConFig)#router bgp 65000
(Routing)(Config-router)#neighbor 172.20.1.2 remote-as 65001
(Routing)(Config-router)#neighbor 172.20.2.2 remote-as 65001
(Routing)(Config-router)#template peer AGGR
(Routing)(Config-rtr-tmplt)#timers 3 9
(Routing)(Config-rtr-tmplt)#local-as 65002 no-prepend replace-as
(Routing)(Config-rtr-tmplt)#address-family ipv4
(Routing)(Config-rtr-tmplt-af)#send-community
(Routing)(Config-rtr-tmplt-af)#route-map RM4-IN in
(Routing)(Config-rtr-tmplt-af)#route-map RM4-OUT out
(Routing)(Config-rtr-tmplt-af)#exit
(Routing)(Config~rtr-tmplt)#address-family ipv6
(Routing)(Config-rtr-tmplt-af)#send-community
(Routing)(Config-rtr-tmplt-af)#route-map RM6-IN in
(Routing)(Config-rtr-tmplt-af)#route-map RM6-0UT out
(Routing)(Config-rtr-tmplt-af)#exit
(Routing)(Config-rtr-tmplt)#exit
(Routing)(Config-router)#neighbor 172.20.1.2 inherit peer AGGR
```

```
(Routing)(Config-router)#neighbor 172.20.2.2 inherit peer AGGR
(Routing)(Config-router)#address-family ipv6
(Routing)(Config-router)#neighbor 172.20.1.2 activate
(Routing)(Config-router)#neighbor 172.20.2.2 activate
```

11-103 update-source

Use this command in Peer Template Configuration mode to configure a peer template to use a specific IP address as the source address for the TCP connection with a neighbor. This IP address must be the IP address configured on the peer as its neighbor address for this router.

Use the **no** command to configure the peer template to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

update-source {*slot/port* **| vlan** *id***}**

no enable password

Parameters

slot/port	Specifies the slot/port of the source/interface to receive the routing updates.
vlan *id*	Specifies the VLAN identifier for the interface.
update-source interface	The primary IPv4 address on this interface is used as the source IP address for the TCP connection with the neighbor.

Default

The default is TCP connections (when an update source is not configured) use the primary IPv4 address on the outgoing interface to the neighbor.

Command Mode

Peer Template Config

11-104 timers bgp

This command configures the keepalive and hold times that BGP uses for all of its neighbors.

When BGP establishes an adjacency, the neighbors agree to use the minimum hold time configured on either neighbor. BGP sends KEEPALIVE messages at either 1/3 of the negotiated hold time or the configured keepalive interval, whichever is more frequent.

The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an adjacency is formed.

Use the **no** command to set to the default the keepalive and hold times that BGP uses for all of its neighbors.

timers bgp *keepalive holdtime*

no timers bgp

Parameters

keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is from 0 to 65,535 seconds. Jitter is applied to the keepalive time.
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. lfthe hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is from 0 to 65,535 seconds.

Default

The default keepalive time is 30 seconds. The default hold time is 90 seconds.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-105 timers policy-apply delay

This command configures the delay after which any change to the global or per BGP neighbor inbound/ outbound policies are applied.

Whenever policies (route-maps/prefix-lists/as-path-lists) or neighbor attributes like send-community, remove-private-asn etc. are modified by the user, the policies are scheduled to be applied after the current delay timeout. Whenever the delay is configured by the user, the pending polic ges if any are rescheduled with the new delay if the previous delay timeout is not expired yet. Configuring the delay with the value of 0 seconds means, the changes are applied immediately.

For any change in the outbound policies applicable to a neighbor, the WITHDRAW packets are sent followed by the UPDATE packets when they are applied after the delay timeout. In case of changes to other neighbor attributes like send-community, remove-private-asn etc, the WITHDRAW packets are not sent-instead, the new UPDATEs are sent after the delay timeout.

Use the **no** command to set to the default the delay after which any change to the global or per BGP neighbor inbound/outbound policies are applied.

timers policy-apply delay *delay*

no timers policy-apply delay

Parameters

delay	The time. in seconds, after which the global or per neighbor policies are applied. The range is 0 to 180 seconds.

Default

The default delay time is 180 seconds.

Command Mode

- BGP Router Config
- IPv4 VRF Address Family Config

11-106 clear ip bgp

This command resets peering sessions with all or a subnet of BGP peers. The command arguments specify which peering sessions are reset and the type of reset performed. Soft inbound reset causes BGP to send a Route Refresh request to each neighbor being reset. If a neighbor does not support the Route Refresh capability, then updated policy is applied to routes previously received from the neighbor.

When a change is made to an outbound policy, BGP schedules an outbound soft reset to update neighbors according to the new policy. Use interface specifies if the changes apply to a specific port or to a VLAN.

This command applies to routes for all address families.

clear ip bgp [vrf *vrf-name***] {* | ***as-number* | *ipv4-address* | *ipv6-address* [interface** *interface-name***] | interface** *interface-name* **| [listen range** *network/length***]} [soft [in | out]**

Parameters

vrf *vrf-name*	(Optional) The name of the VRF instance.
*****	Reset adjacency with every BGP peer.
as-number	Only reset adjacencies with BCP peers in the given autonomous system.
ipv4-address	Only reset the adjacency with a single specified peer with a given IPv4 peer address.
ipv6-address	Only reset the adjacency with a single specified peer with a given IPv6 peer address. An adjacency that is formed with the autodetect feature cannot be reset with the command.
interface *interface-name*	(Optional) Only reset the aégcency on a specified interface. The adjacency must be formed with IPv6 link-local or with t e auto detect feature.
listen range *network/length*	Reset all adjacency that are included in the listen subnet range.
soft	(Optional) By default, adjacencies are torn down and reestablished. If the soft keyword is given, BGP resends all updates to the neighbors and reprocesses updates from the neighbors.
in | out	(Optional) If the **in** keyword is given, then updates from the neighbor are reprocessed. If the **out** keyword is given, then updates are resent to the neighbor. If neither keyword is given, then updates are reprocessed in both directions.

Default

The default is None.

Command Mode

Privileged EXEC

11-107 clear ip bgp counters

This command resets all BGP counters to 0. These counters include send and receive packet and prefix counters for all neighbors.

clear ip bgp [vrf *vrf-nume***] counters**

Parameters

vrf *vrf-nume*	(Optional) Enter a numberic value to identify the VRF member.

Default

The default is None.

Command Mode

Privileged EXEC

11-108 show ip bgp

To view IPv4 routes in the BGP routing table, use the **show ip bgp** command in Privileged EXEC mode. The output lists both best and non-best paths to each destination. If a VRF instance is specified, the IPv4 routes in the BGP routing table of the VRF instance are displayed.

show ip bgp [vrf *vrf-name***] [***network/pfx-len* **[longer-prefixes | shorter-prefixes [***length***]] | filter-list** *as-path-list* **| prefix-list** *pfx-list-name***]**

Parameters

vrf *vrf-name*	(Optional) Enter the Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table select.
network/pfx-len	(Optional) Display a specific route identified by its destination prefix.
longer-prefixes	(Optional) Used with the network/pfx-len option to show routes whose prefix length is equal to or longer than pfx-len. This option may not be given if the **shorter-prefixes** option is given.
shorter-prefixes [*length***]**	(Optional) Used with the network/pfx-len option to show routes whose prefix length is shorter than pfx-len, and, optionally, ionger than a

	specified length. This option may not be given if the **longer-prefixes** option is given.
filter-list *as-path-list*	(Optional) Filter the output to the set of routes that match a given AS-PATH list. This option may not be given if a network/pfx-len option is given, or when a prefix list is given.
prefix-list *pfx-list-name*	(Optional) Filter the output to the set of routes that match a given prefix list. This option may not be given if a network/pfx-len option is given or when a filter list is given.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    Network          Next Hop     Metric     LocPrf     Path
*>  172.20.1.0/24    100.10.1.1   10         100        20 10      i
                     200. 10. 1.1
*>  172.20.2.0/24    100.10.1.1   10         100        20 10      ?
```

If one or more of the three well-known communities in RFC 1997 is attached to a path, **show ip bgp** lists them.

```
(Routing)#show ip bgp

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    Network          Next Hop     Metric     LocPrf     Path
*> 172.20.1.0/24     100.10.1.1   10         100        20 10      i
    Communities: no-export
*> 24.95.16.0/24     100.10.1.1   10         100        20 10      i
    Communities: no-advertise
*> 24.14.8.0/24      100.10.1.1   10         100        20 10      i
    Communities: no-export-subconfed
```

The following shows example CLI display output for the command.

```
(R1)#show ip bgp 172.20.1.0/24
```

```
Prefix/Prefix Length.......................... 172.20.1.0/24
Generation ID................................. 2056
Forwarding.................................... Yes
Advertised to Update Groups................... 1, 5

Best Path:
Local Preference.............................. 100
AS Path ...................................... 20 10
Origin........................................ IGP
Metric........................................ 10
Type.......................................... External
IGP COST...................................... 30
Peer (Peer ID)................................ 100.10.1.1(32.4.1.1)
BGP Next Hop.................................. 100.10.1.1
Atomic Aggregate.............................. Included
Aggregator (AS, Router ID).................... 300, 14.1.1.1
Communities................................... no-export

Non-best Paths:
Local Preference.............................. 200
AS Path ...................................... 18 50 27
Origin........................................ Incomplete
Type.......................................... External
IGP Cost...................................... 10
Peer (Peer ID)................................ 200.1.1.1.(18.24.1.3)
BGP Next Hop.................................. 200.1.1.1
```

Display Parameters

The command output displays the following information.

BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.
Status codes	• s: The route is aggregated into an aggregate address configured with the summary-only option • *: D-LINK OS BGP never displays invalid routes; so this code is always displayed • >: Indicates that BGP has selected this path as the best path to the destination • I: If the route is learned from an internal peer
Network	Destination prefix.
Next Hop	The route's BGP NEXT HOP.
Metric	Multi Exit Discriminator.
LocPrf	The local preference.
Path	The AS-PATH. **Note:** The value of the ORIGIN attribute follows immediately after the AS-PATH.

lf the command is given with network/pfx-Ien option and without any additional options, then the output format lists more information about the individual prefix. The best path is always listed first, followed by any non-best paths. The output only shows attributes that are included with each path.

Prefix/Prefix Length	The destination prefix and prefix length.
Generation ID	The version of the BGP routing table when this route last changed.
Forwarding	Whether this BGP route is used for fon/varding.
Advertised Update GroupsTo	The outbound update groups that this route is advertised to.
Local Preference	The local preference, either as received from the peer or as set according to local policy.
AS Path	The AS-PATH. This form of show ip bgp displays AS-PATHs as long as allowed by bgp maxas-limit.
Origin	Value of the ORIGIN attribute.
Metric	Value of the MED attribute, if included.
Type	Whether the path is received from an internal or external peer.
IGP Cost	The interior gateway cost (e.g., OSPF cost) to the BGP NEXT HOP.
Peer (Peer ID)	The IP address of the peerthat sent this route, and its router ID.
BGP Next Hop	The BGP NEXT HOP attribute.
Atomic Aggregate	If the ATOMIC AGGEGATE attribute is attached to the path.
Aggregator	The AS number and router ID of the speaker that aggregated the route.
Communities	The BGP communities attached to the path.
Originator	The value of the ORIGINATOR attribute, if the attribute is attached to the path.
Cluster list	The value of the CLUSTER LIST attribute, if the attribute is attached to the path.

11-109 show ip bgp aggregate-address

This command lists aggregate addresses that have been configured and indicates whether each is currently active. If a VRF is specified, the aggregate addresses configured in a VRF instance are displayed.

show ip bgp [vrf *vrf-name***] aggregate-address**

Parameters

vrf *vrf-name*	(Optional)

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp aggregate-address

Prefix/Len   AS Set     Summary Only    Active
10.0.0.0/8   N          Y               Y
20.0.0.0/8   N          Y               N
```

Display Parameters

PrefixlLen	Destination prefix and prefix length.
AS Set	Indicates whether an empty AS-PATH is advertised with the aggregate address (N) or an AS SET is advertised with the set ofAS numbers for the paths contributing to the aggregate (Y).
Summary Only	Indicates whether the individual networks are suppressed (Y) or advertised (N).
Active	Indicates whether the aggregate is currently being advertised.

11-110 show ip bgp community

This command shows BGP IPv4 routes that belong to a specified set of communities.

show ip bgp [vrf *vrf-name***] community** *communities* **[exact-match]**

Parameters

vrf *vrf-name*	(Optional) Displays routes belonging to communities within a VRF instance.
communities	A string of zero or more community values, which may be in either format and may contain the well-known community keywords no-advertise and no-export. The output displays routes that belong to every community specified in the command.
exact-match	(Optional) Only displays routes that are members of those and only those communities specified in the command.

Default

The default is None.

Command Mode

Privileged EXEC

11-111 show ip bgp community-list

This command displays IPv4 routes that match a community list. The output format and field descriptions are the same as for "show ip bgp".

show ip bgp community-list [*list-name***] [exact-match]**

Parameters

vrf *vrf-name*	(Optional) Displays routes belonging to communities within a VRF instance
communities	Displays the BGP communities attached to the path.
exact-match	(Optional) Displays only routes that are an exact match for the set of communities in the matching community list statement.

Default

The default is None.

Command Mode

Privileged EXEC

11-112 show ip bgp extcommunity-list

This command displays all the permit and deny attributes of the given extended community list. If the list-name is specified, the output is displayed that matches the given list-name; else all the lists are displayed.

show ip bgp extcommunity-list [*list-name***]**

Parameters

list-name	A standard extended community list name.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#show ip bgp extcommunity-list 1
```

```
Standard extended community-list list1
permit RT:1:100 RT:2:100
deny RT:6:600
permit RT:5:200
permit SOO:9:900
```

Display Parameters

Standard extended community-list	The standard named extended community list.
permit	Permits access for a matching condition. Once a permit value has been configured to match a given set of extended communities the extended community list defaults to an implicit deny for all other values.
RT	The route target extended community attribute.
deny	Denies access for a matching condition.

11-113 show ip bgp listen range

This command displays information about the IPv4 BGP listen subnet ranges. If network/length are specified, information about the specified listen range are displayed.

show ip bgp [*network/length***]**

Parameters

network/length	(Optional) Indicates the network number and length (bits) of the network mask.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)(Config-router)#show ip bgp listen range

Listen Range..................................... 10.27.0.0/16
Inherited Template............................... template_10_27

Member            ASN       State
---------------   -------   ------------
10.27.8.189       65001     OPENCONFIRM
```

```
10.27.128.235      0          ACTIVE

Listen Range..................................... 15.15.0.0/24
Inherited Template.............................. template_15_15

Member             ASN        State
---------------    -------    ------------
```

11-114 show ip bgp neighbors policy

This command displays the inbound and outbound IPv4 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template.

show ip bgp [vrf *vrf-name***] neighbors** *ipv4-address* **[interface** *interface-name***] policy**

Parameters

vrf *vrf-name*	(Optional) Displays routes belonging to communities within a VRF instance.
ipv4-address	Specifies an IPv4 address of a neighbor to which to limit the output.
interface *interface-name*	(Optional) Displays the neighbor's IPv4 address.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp neighbors 172.20.101.100 policy

Neighbor           Policy                                          Template
---------------    ----------------------------------------------  ----------
172.26.191.100     advertisement-interval 600
                   default-originate
                   filter-list 500 in
                   filter-list 500 out
                   prefix-list barney in
                   prefix-list wilma out
                   maximum-prefix unlimited 100 warning-only       torPeers
                   route-map fred in                               torPeers
                   route-map dino out                              torPeers
                   send-community                                  torPeers
                   advertisement-interval 600                      torPeers
```

```
                    default-originate                                   torPeers
```

Display Parameters

Neighbor	The peer address of a neighbor.
Policy	A neighbor-specific BGP policy.
Template	If the policy is inherited from a peer template, this field lists the template name.

11-115 show ip bgp neighbors

This command shows details about BGP neighbor configuration and status. if the neighbor is configured to inherit configuration parameters from a peer template, the output shows the inherited values. If a VRF is specified, neighbors belonging to the VRF instance are displayed.

Note: Policy configuration is moved from this command to the command “show ip bgp neighbors policy”.

show ip bgp [vrf *vrf-name***] neighbors [***ip-address***]**

Parameters

vrf *vrf-name*	(Optional) Display routes belonging to communities within a VRF instance.
ip-address	(Optional) The IP address of a neighbor. Used to limit the output to show a single neighbor.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp neighbors 172.20.1.100

Description: spine 1 router 1

Remote Address.................................. 172.20.1.100
Remote AS....................................... 100
BFD Enabled to Detect Fast Fallover.............. Yes
Peer ID......................................... 14.3.0.1
Peer Admin Status............................... START
Peer State...................................... ESTABLISHED
Peer Type....................................... DYNAMIC
```

```
Listen Range..................................... 172.20.0.0/16
Local Interface Address.......................... 172.20.1.2
Local Port....................................... 179
Remote Port...................................... 58265
Connection Retry Interval........................ 120 sec
Neighbor Capabilities............................ None
IPv4 Unicast Support............................. Both
IPv6 Unicast Support............................. Sent

Update Source.....................................
Configured Hold Time............................. 90 sec
Configured Keep Alive Time....................... 30 sec
Negotiated Hold Time............................. 30 sec
Keep Alive Time ................................. 16 sec

MD5 Password..................................... password

Last Error (Sent)................................ Hold Timer Expired
Last SubError.................................... None
Time Since Last Error............................ 0 day 0 hr 4 min 27 sec
Established Transitions.......................... 1
Established Time................................. 0 day 0 hr 4 min 25 sec
Time Elapsed Since Last Update................... 0 day 0 hr 4 min 245 sec
Outbound Update Group............................ 3

           Open     Update    Keepalive    Notification    Refresh   Total
Msgs Sent     1          0           10               0          0      11
Msgs Rcvd     1          1           11               0          0      12

Received UPDATE Queue Size: 0 bytes. High: 355. Limit 196096. Drops 0.

IPv4 Prefix Statistics:
                        Inbound     Outbound
Prefixes Advertised           1            0
Prefixes Withdrawn            0            0
Prefixes Current              1            0
Prefixes Accepted             1          N/A
Prefixes Rejected             1          N A
Max NLRI per Update           1            0
Min NLRI per Update           1            0

IPv6 Prefix Statistics:
                        Inbound     Outbound
Prefixes Advertised           1            0
Prefixes withdrawn            0            0
Prefixes Current              1            0
Prefixes Accepted             1          N/A
Prefixes Rejected             1          N/A
Max NLRI per Update           1            0
Min NLRI per Update           1            0
```

In this example, BGP has received an UPDATE message from an external peer 172.20.101.100 with something otherthan the peer's ASN as the first ASN in the AS-PATH. The additional counter shows that this occurred one time.

```
(Routing)#show ip bgp neighbors 172.20.101.100

Remote Address..................................... 172.20.101.100
Remote AS.......................................... 101

Last Error......................................... UPDATE Message Error
Last SubError...................................... Malformed AS_PATH
Unexpected first ASN in AS path ................... 1

Established Transitions............................ 1
Established Time................................... 0 days 00 hrs 00 mins 10 secs
```

Display Parameters

Description	Text string assigned using the command "neighbor description". This text string only appears if a description is configured.
Remote Address	The neighbor's IP address.
Remote AS	The neighbor's autonomous system number.
BFD Enabled to Detect Fast Failover	Specifies if BFD has been enabled for BGP neighbors.
Peer ID	The neighbors BGP router ID.
Peer Admin Status	START or STOP.
Peer Type	If a neighbor was created with the BGP dynamic neighbors feature, Dynamic is shown.
Listen Range	If the neighbor was created with the BGP dynamic neighbors feature, the field shows the listen range to which the neighbor belongs.
Listen Range	The listen range.
Local Interface Address	The IPv4 address used as the source IP address in packets sent to this neighbor.
Local Port	TCP port number on the local end of the connection.
Remote Port	TCP port number on the remote end of the connection.
Connection Retry Interval	How long BGP waits between connection retries.
Neighbor Capabilities	Optional capabilities reported by the neighbor, recognized and accepted by this router. Codes listed in the show output are as follows: • MP: Multiprotocol • RF: Route Refresh • AS4: 4-Byte ASN This version of D-LINK OS does not support any multiprotocol AFI/SAFI pairs other than IPv4 unicast. The presence of this capability does not imply otherwise.

IPv4 Unicast Support	Indicates whether IPv4 unicast routes can be exchanged with this peer. **Both** indicates that IPv4 is active locally and the neighbor indicated support for IPv4 unicast in its OPEN message. **Sent** indicates that IPv4 unicast is active locally, but the neighbor did not include this AFI/SAFI pair in its OPEN message. IPv4 unicast is always enabled locally and cannot be disabled.
IPv6 Unicast Support	Indicates whether IPv6 unicast routes can be exchanged with this peer. **Both** and **Sent** have the same meaning as for IPv4. **None** indicates that neither the local router northe peer has IPv6 enabled for this adjacency. **Received** indicates that the peer advertised the IPv6 unicast capability, but it is not enabled locally. IPv6 unicast is enabled locally using the neighbor activate command in address-family IPv6 configuration mode.
Update Source	The configured value for the source IP address of packets sent to this peer. This field is only included in the output if the update source is configured.
Configured Hold Time	The time, in seconds, that this router proposes to this neighbor as the hold time.
Configured Keep Alive Time	The configured KEEPALIVE interval for this neighbor.
Negotiated Hold Time	The minimum of the configured hold time and the hold time in the OPEN message received from this neighbor. If the local router does not receive a KEEPALIVE or UPDATE message from this neighbor within this interval of time, the local router drops the adjacency. This field is only shown if the adjacency state is OPEN CONFIRM or greater.
MD5 Password	The TCP MD5 password, if one is configured, in plain text.
Keep Alive Time	The number of seconds between KEEPALIVE messages sent to this neighbor. This field is only shown if the adjacency state is OPEN CONFIRM or greater.
Last Error (Sent)	The last error that occurred on the connection to this neighbor.
Last SubError	The suberror reported with the last error.
Established Tranitions	The number of times the adjacency has transitioned into the Established state.
Established Time	How long since the connection last transitioned to or from the Established state.
Time Since Last Update	How long since an UPDATE message has been received from this neighbor.
Message Table	The number of BGP messages sent to and received from this neighbor.
Received UPDATE Queue Size	Received UPDATE messages are queued for processing. This section shows the current length of the neighbors UPDATE queue in bytes, the high water mark, the limit, and the number of UPDATEs that have been dropped because the queue reached the limit.
The following fields are displayed for IPv4, and if IPv6 is running, for IPv6 as well.	
Prefixes Advertised	A running count of the number of prefixes advertised to or received from this neighbor.
Prefixes Withdrawn	A running count of the number of prefixes included in the Withdrawn Routes portion of UPDATE messages, to and from this neighbor.

Prefixes Current	The number of prefixes currently advertised to or received from this neighbor. For inbound prefixes, this count only includes prefixes that passed inbound policy.
Prefixes Accepted	The number of prefixes from this neighborthat are eligible to become active in the local RIB. Received prefixes are ineligible if their BGP Next Hop is not resolvable or if the AS-PATH contains a loop. A prefix is only considered accepted if it passes inbound policy.
Prefixes Rejected	The number of prefixes currently received from this neighbor that fail inbound policy.
Max NLRI per Update	The maximum number of prefixes included in a single UPDATE message, to and from this neighbor.
Min NLRI per Update	The minimum number of prefixes included in a single UPDATE message, to and from this neighbor.

If the router receives an UPDATE message with an invalid path attribute, the router will in most cases send a NOTIFICATION message and reset the adjacency. BGP maintains a per-neighbor counter for each type of path attribute error. This show command ts each non-zero counter, just after the LastSubError. The counters that may be listed are as follows:

Path with duplicate attribute	The peer sent an UPDATE message containing the same path attribute more than once.
Path with well-known/optional conflict	A received path attribute was flagged as both well-known and optional or neither well-known nor optional.
Transitive f gt set on transitive attr	A received path attribute is known to be transitive, but the transitive flag is not set.
Manda attribute non-transitive or partial	A mandatory path attribute was received with either the transitive or partial flag set.
Optional attribute non-transitive and partial	An optional path attribute has the transitive flag clear and the partial flag set.
Path attribute too long	A received path attribute was longer than the expected length.
Path attribute length error	A received path attribute has a length value that exceeds the remaining length of the path attributes field.
Invalid ORIGIN code	A received UPDATE message included an invalid ORIGIN code.
Unexpected first ASN in AS path	The AS-PATH attribute from an external peer did not include the peer’s AS number as the first AS.
Invalid AS path segment type	The AS-PATH includes a segment with an invalid segment type.
Invalid BGP NEXT HOP	The BGP NEXT HOP is not a valid unicast address.
Bad BGP NEXT HOP	The BGP NEXT HOP was either the receiver's IP address or an IP address outside the subnet to the peer.
Invalid AGGREGATOR attribute	The AGGREGATOR attribute was invalid.
Unrecognized well-known path attribute	An UPDATE message contained a path attribute with the Optional flag clear, but this router does not recognize the attribute.

Missing mandatory path attribute	An UPDATE message was received without a mandatory path attribute.
Missing LOCAL PREF attribute	An UPDATE message received from an internal peer without the LOCAL PREF attribute.
Invalid prefix in UPDATE NLRI	An UPDATE message received from this peer contained a syntactically incorrect prefix.

11-116 show ip bgp neighbors advertised-routes

This command displays the list of IPv4 routes advertised to a specific neighbor. These are the routes in the adjacent RIB out for the neighbor's outbound update group.

show ip bgp [vrf *vrf-name***] neighbors** *ip-address* **advertised-routes**

Parameters

vrf *vrf-name*	(Optional) Display routes belonging to communities within a VRF instance.
ip-address	The IP address of a neighbor.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp neighbors 172.20.101.100 advertised-routes

BGP table version is 5, local router ID is 20.1.1.1
Status codes: p advertisement pending
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Version    Network         Next Hop          Metric     Local Pref    Path
5          172.20.1.0/24   172.20.101.1      10         100           20 10    i
p 5        20.1.1.0/24     172.20.161.1                 100           20       ?
```

Note: This output differs slightly from the output in **show ip bgp**. Suppressed routes and non-best Routes are not advertised, so these status codes are not relevant here. Advertised routes always have A single next hop, the BGP NEXT HOP advertised to the peer. Local preference is never sent to external peers.

The output indicates whether BGP is configured to originate a default route to this peer (neighbor default-originate).

Display Parameters

BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.
Status codes	p – The route has been updated in Adj-RIB-Out since the last UPDATE message was sent. Transmission of an UPDATE message is pending.
Network	Destination prefix.
Next Hop	The BGP NEXT HOP as advertised to the peer.
Local Pref	The local preference. Local preference is never advertised to external peers.
Metric	The value of the Multi Exit Discriminator, if the MED is advertised to the peer.
Path	The AS-PATH. The AS-PATH does not include the local AS number, which is added to the beginning of the AS-PATH when a route is advertised to an external peer. **Note:** The value of the ORIGIN attribute follows immediately after the AS-PATH.

11-117 show ip bgp neighbors policy

This command displays the inbound and outbound IPv4 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template.

show ip bgp neighbors [*ip-address***] policy**

Parameters

ip-address	(Optional) Specifies an IPv4 address of a neighbor to which to limit the output.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI dis display output for the command.

```
(Routing)#show ip bgp neighbors 172.20.101.100 policy

Neighbor          Policy                                          Template
---------------   ----------------------------------------------  ----------
```

```
172.20.101.100     advertisement-inter'vak600
                   default-originate
                   filter-list 500 in
                   filter-list 500 out
                   prefix-list barney in
                   prefix-list Wilma out
                   maximum-prefix unlimited 100 warning-only      torPeers
                   route-map fred in                              torPeers
                   route-map dino out                             torPeers
                   send-community                                 torPeers
                   advertisement-interval 600                     torPeers
                   default-originate                              torPeers
```

Display Parameters

Neighbor	The peer address of a neighbor.
Policy	A neighbor-specific BGP policy.
Template	If the policy is inherited from a peer te this field lists the template name.

11-118 show ip bgp neighbors {received-routes | routes | rejected-routes}

This command displays the list of IPv4 routes received from a specific neighbor. The list includes either all routes received from the neighbor, received routes that passed inbound policy, or routes rejected by inbound policy. If a VRF instance is specified, the routes information is displayed for the neighbors in the VRF instance.

show ip bgp [vrf *vrf-name***] neighbors [***ip-address* **{received-routes | routes | rejected-routes}]**

Parameters

vrf *vrf-name*	(Optional) Display the routes belonging to communities within a VRF instance.
ip-address	(Optional) The IP address of a neighbor.
received-routes	Display all routes received from this neighbor, regardless of if the routes passed inbound policy.
routes	Display only routes that passed inbound policy.
rejected-routes	Display only routes rejected by inbound policy.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp neighbors 172.20.101.100 received-routes

local router ID is 20.1.1.1
Origin codes: i - IGP, e - EGP, ? - incomplete

Network         Next Hop       Metric   Local Pref    Path  Origin
172.20.1.0/24   172.20.101 1       10       100 20      10       i
20.1.1.0/24     172.20.101 1                  100      20       ?
```

Display Parameters

Network	Destination prefix.
Next Hop	The BGP NEXT HOP as advertised by the peer.
Metric	The value of the Multi Exit Discriminator, if a MED is received from the peer.
Local Pref	The local preference received from the peer.
Path	The AS-PATH as received from the peer.
Origin	The value of the Origin attribute as received from the peer.

11-119 show ip bgp route-reflection

This command displays all global configuration related to IPv4 route reflection, including the cluster ID and whether client-to-client route reflection is enabled, and lists all the neighbors that are configured as route reflector clients. If a VRF instance is specified, the routes belonging to communities within a VRF instance are displayed.

If a route reflector client is configured with an outbound route map, the output warns that set statements in the route map are ignored when reflecting routes to this client.

show ip bgp [vrf *vrf-name***] route-reflection**

Parameters

vrf *vrf-name*	(Optional) Displays 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.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp route-reflection

Cluster ID..................................... 1.1.1.1 (configured)
Client-to-client Reflection..................... Enabled
Clients: 172.20.1.2, 172.20.3.2, 172.20.5.2
Non-client Internal Peers: 192.168.1.2, 192.162.2.2
Skipping set statements in outbound route map gandolf when reflecting to internal peer
172.20.1.2.
```

Display Parameters

Cluster ID	The cluster ID used by this router. The value configured with the bgp cluster-id command is displayed. If no cluster ID is configured, the local router ID is shown and tagged as default.
Client-to-client Reflection	Displays Enabled when this router reflects routes received from its clients to its other clients;otherwise Disabled displays.
Clients	A list of this router's internal peers that have been configured as route reflector clients.
Non-client Internal Peers	A list of this router's internal peers that are not configured as route reflector clients. Routes from non-client peers are reflected to clients and vice-versa.

11-120 show ip bgp statistics

This command displays recent decision process history. Phase 1 of the decision process reacts to UPDATE messages received from peers, determining what new routes are accepted and deleting withdrawn routes from the Adj-RIB-In. Phase 2 determines the best path for each destination, updates the BGP route table, and updates the common RIB. Phase 3 is run independently for each outbound update group and determines which routes should be advertised to neighbors in each group. Each entry in the table shows statistics for one phase of the decision process. The table shows the 20 most recent decision process runs, with the most recent information at the end of the table. If a VRF instance is specified, the statistics for the routes belonging to communities within the VRF instance are displayed.

show ip bgp [vrf *vrf-name***] statistics**

Parameters

vrf *vrf-name*	(Optional) Displays 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.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp statistics

Delta T   Phase   Upd Grp   GenId          Reason   Peer   Duration   Adds   Mods   Dels
29:33:49      3         0    2041  Fwd status chng               34    750      0    500
29:33:40      2              2042   Accept-RIB-In-               59    750      0    500
29:33:28      2              2043   Accept-RIB-In-               10      0      0    250
29:23:40      2              2044   Accept-RIB-In-               32      0      0   1000
29:13:28      3         1    2044    Phase 2 done-               48    500   2500   1750
29:02:40      1              2044      Adj-RIB-In+               21    500      0      0
29:02:01      3         0    2044     Phase 2 done               41    750      0   1250
28:33:40      2              2045     Phase 1 done                    32    500      0
28:15:00      1              2045      Adj-RIB-In+                9    250      0      0
28:14:40      2              2046     Phase 1 done                    16    250      0
```

Display Parameters

Delta T	How long since the decision process was run. hourszminuteszseconds if the elapsed time is less than 24 hours. Otherwise, days:hours.
Phase	Which phase of the decision process was run.
Upd Grp	Outbound update group ID. Only applies when phase 3 is run.
GenId	Generation ID of BGP routing table when decision process was run. The generation ID is incremented each time phase 2 of the decisi cess is run and when there is a change to the status of aggregate addresses.
Reason	The event that triggered the decision process to run.
Peer	Phase 1 of the decision process can be triggered for a specific peer when a peer's inbound routing policy changes or the peer is resrt. When phase 1 is run for a single peer, the peer's IP address is given.
Duration	How long the decision process took,in milliseconds.
Adds	The number of routes added. For phase 1, this is the number of prefixes that pass inbound policy and are added to the Accept-RIB-In. For phase 2, this is the number of routes added to the BGP routing table For phase 3, this is the number of prefixes added to the update group's Adj-RIB-Out.
Mods	The number of routes modified. Always 0 for phase 1.
Dels	The number of routes deleted. Always 0 for phase 1.

11-121 show ip bgp summary

This command displays a summary of BGP configuration and status. If a VRF instance is specified, the configuration and status for the routes in belonging to communities withing the specified VRF instance are displayed.

show ip bgp [vrf *vrf-name*] **summary**

Parameters

vrf *vrf-name*	(Optional) Displays 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.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip bgp summary

Admin Mode..................................... Enable
BGP Router ID.................................. 172.20.1.1
Local AS Number................................ 200
Traps.......................................... Disable
Maximum Paths.................................. 32
Maximum Paths iBGP............................. 16
Default Keep Alive Time........................ 30 sec
Default Hold Time.............................. 90 sec
Number of Network Entries...................... 20
Number of AS Paths............................. 5

Default Metric................................. Not configured
Default Route Advertise........................ No

Redistributing.................................
Source......................................... ospf
Metric......................................... Not configured
Match Value.................................... 'internal'
Distribute List................................ Not configured

Neighbor     ASN    MsgRcvd    MsgSent         State    Up/Down Time   Pfx Rcvd
100.16.1.1    50         48         92           EST        00:47:30         20
100.20.1.4    20          0          2    OPEN SENT                           0
```

Display Parameters

IPv4 Routing	Whether IPv4 routing is globally enabled. BGP does not include the IPv4 unicastAFI/SAFI capability in OPEN messages it sends unless routing is globally enabled.
BGP Admin Mode	Whether BGP is globally enabled.
BGP Router ID	The configured router ID.
Local AS Number	The router's AS number.
Traps	Whether BGP traps are enabled.
Maximum Paths	The maximum number of next hops in an external BGP route.
Maximum Paths iBGP	The maximum number of next hops in an internal BGP route.
Default Keep Alive Time	The configured keepalive time used by all peers that have not been configured with a peer-specific keepalive time.
Default Hold Time	The configured hold time used by all peers that have not been configured with a peer-specific hold time.
Number of Network Entries	The number of distinct prefixes in the local RIB.
Number of AS Paths	The number of AS-PATHs in the local RIB.
Default Metric	The default value for the MED for redistributed routes.
Default Route Advertise	Whether BGP is configured to advertise a default route. Corresponds to the “default-information originate” command.
Redistributing Source	A source of routes that BGP is configured to redistribute.
Metric	The metric configured with the redistribute command.
Match Value	For routes redistributed from OSPF, the types of OSPF routes being redistributed.
Distribute List	The name of the prefix list used to filter redistributed routes, if one is configured with the “distribute-list prefix out” command.
Route Map	The name of the route map used to filter redistributed routes.
Dynamic Neighbors	Shows the current number of created dynamic IPv4 BGP neighbors, high water mark and a limit of dynamic IPv4 BGP neighbors that can be created.
Neighbor	The IP address ofa neighbor. A neighbor, that is created with BGP dynamic neighbors feature, will be marked with “*”.
ASN	The neighbor's ASN.
MsgRcvd	The number of BGP messages received from this neighbor.
Msgsent	The number of BGP messages sent to this neighbor.
State	The adjacency state. One of IDLE, CONNECT, ACTIVE, QPEN SENT, OPEN CNFRM, EST.
Up/Down Time	How long the adjacency has been in the ESTABLISHED state, or if the adjacency is down, how long it has been down. In dayszhours minutes seconds.
Pfx Rcvd	The number of prefixes received from the neighbor.

11-122 show ip bgp template

Use this command to view information about all configured BGP peer templates or for the specified BGP template.

show ip bgp template *name*

Parameters

name	Displays the name of a BGP peer template.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(router)#show ip bgp template

Template Name     AF         Configuration
---------------   -----      ------------------------------
peer-grp1                    timers 5 15
                             password rivendell
                  IPv4       advertisement-interval 15
peer-grp2         IPv4       prefix-list strider in
                  IPv4       maximum-prefix 100
                  IPv6       prefix-list gandolf in
                  IPv6       maximum-prefix 200
peer-grp3         IPv6       send-community
peer-grp4                    update-source loopback 0
                  IPv4       next-hop-self
```

Display Parameters

Name	The name of a BGP peer template.
AF	The address family to which the configuration command applies This field is blankfor session parameters, which apply to all address families.
Configuration	Configuration commands that are included in the template.

11-123 show ip bgp traffic

This command reports global BGP message counters for transmitted and received messages along with BGP work queue information. If a VRF instance is specified, the counters belonging to communities within that VRF instance are displayed.

show ip bgp [vrf *vrf-name*] **traffic**

Parameters

vrf *vrf-name*	Displays the virtual router for which to display information.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(router)#show ip bgp traffic

Time Since Counters Cleared: 55223 Seconds
BGP Message Statistics
         Open     Update    Notification    Keepalive    Refresh      Total
Recd:       6         11               0         7888          0       7905
Sent:       8         56               3         8465          0       8532

Max Received UPDATE rate: 1 pps
Max Send UPDATE rate: 5 pps

BGP Queue Statistics
                   Current      Max      Drops      Limit
Events                   0        2          0        800
Keepalive Tx             0        3          0        128
Dec Proc                 0        3          0        133
Rx Data                  0        3          0        500
RTO Notifications        0        4          0       1222
MIB Queries              0        0          0          5
```

Display Parameters

The first table lists the number of BGP messages of each type that this router has sent and received. Following the table is a maximum send and receive UPDATE message rate. These rates report the busiest one-second interval.

The queue statistics table reports information for BGP work queues. Items placed on each of these work queues are as follows:

Events	Includes most timer events and configuration changes.

Keepalive Tx	Includes timer events to send a KEEPALIVE message to a peer.
Dec Proc	Includes events that cause the decision process to be run.
Rx Data	Holds incoming BGP messages.
RTO Notifications	Includes best route change and next hop resolution change notifications from the routing table.
MIB Queries	Includes pending SNMP queries for BGP status.

11-124 show ip bgp update-group

This command reports the status of outbound update groups and their members. If a VRF instance is specified, the status of the update groups for that VRF instance are displayed.

show ip bgp [vrf *vrf-name***] update-group [***ipv4-address* **|** *ipv6-address***]**

Parameters

vrf *vrf-name*	Displays the virtual router for which to display information.
ipv4-address **|** *ipv6-address*	(Optional) If specified, this option restricts the output to the update group containing the peer with the given IPv4 or IPv6 address.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command displaying information for all update groups.

```
(Routing)#show ip bgp update-group

Update Group ID.................................. 0
Peer Type........................................ External
Minimum Advertisement Interval................... 30 seconds
Remove Private ASNs.............................. No
Route Reflector Client........................... No
Neighbor AS Path Access List Out................. 1
Neighbor Prefix List Out ........................ pfxList1
Members Added.................................... 48
Members Removed.................................. 0
Update Version  ................................. 19
Number of UPDATEs Sent........................... 512
Time Since Last Update........................... 5 hrs 3 min 2 sec
Current Prefixes................................. 5500
```

```
Current Paths..................................... 22
Prefixes Advertised............................... 191250
Prefixes withdrawn................................ 186000
UPDATE Send Failures.............................. 0

Current Members: 172.20.1.100, 172.20.2.100

 Version    Delta T   Duration  UPD Built   UPD Sent    Paths Sent     Pfxs Adv    Pfxs Wd
      10   00:33:49        100          6        288             5         1250        750
      11   00:33:49          0          4        192             3          750        250
      12   00:33:49          0          2         96             1          250       1000
      13   00:33:49          0          2         96             1          250       1018
      14   00:33:49          0          1         48             0            0        482
      15   00:33:49        100          8        384             7         1750        750
      16   00:33:49          0          3        144             2          500        250
      17   00:31:49          0          4        192             3          750        750
      18   00:23:49        100          4        192             3          750       1000
      19   00:03:49        100          6        288             5         1250        500

Update Group ID................................... 1
Peer Type......................................... Internal
Minimum Advertisement Interval.................... 5 seconds
Neighbor AS Path Access List Out.................. none
Neighbor Prefix List Out ......................... noge
Members Added..................................... 3
Members Removed................................... 0
Update Version  .................................. 4
Number of UPDATEs Sent............................ 8
Time Since Last UPDATE ........................... 3 hrs 13 min 22 sec
Current Prefixes.................................. 84
Current Paths..................................... 2
Prefixes Advertised............................... 100
Prefixes Withdrawn................................ 16
UPDATE Send Failures.............................. 0

Current Members: 172.24.3.1, 172.25.8.56, 172.28.9.1

 Version    Delta TDuration UPDBuilt UPD Sent Paths     Sent Pfxs          Adv    Pfxs wd
      10   00:00:49        100          6        288             5         1250        750
```

Display Parameters

Update Group ID	Unique identifier for outbound update group.
Peer Type	Whether peers in this update group are internal or external.
Minimum Advertisement Interval	The minimum time, in seconds, between sets of UPDATE messages sent to the group.
Send Community	If the BGP communities are included in route advertisements to members of the group.

Remove Private ASNs	If BGP removes private ASNs from paths advertised to members of this update group. • Replace if BGP replaces private ASNs with the local ASN. • Remove if private ASNs are simply removed. • Otherwise No.
Route Reflector Client	If peers in this update group are route reflector clients.
Neighbor AS Path Access List Out	The AS-PATH access list used to filter UPDATE messages sent to peers in the update group.
Neighbor Prefix List Out	Name of the prefix list used to filter prefixes advertised to the peers in the update group.
Members Added	The number of peers added to the group since the group was formed.
Members Removed	The number of peers removed from the group.
Update Version	The number of times phase 3 of the BGP decision process has run for this group to determine which routes should be advertised to the group.
Number of UPDATEs Sent	The number of UPDATE messages that have been sent to this group. Incremented once for each UPDATE regardless of the number of group members.
Time Since Last UPDATE	Time since an UPDATE message was last sent to the group. If no UPDATE has been sent to the group, the status is “Never.”
Current Prefixes	The number of prefixes currently advertised to the group.
Current Paths	The number of paths currently advertised to the group.
Prefixes Advertised	The total number of prefixes advertised to the group since the group was formed.
Prefixes Withdrawn	The total number of prefixes included in the Withdrawn Routes field of UPDATE messages sent to the group since the group was formed.
UPDATE Send Failures	The number of UPDATE messages that failed to be delivered to all members of the group.
Current Members	The IPv4 address of all current members of the group.

The update send history table show statistics on as many as the ten most recent executions of the update send process for the update group. Items in the history table are as follows.

Version	Displays the update version.
Delta T	Displays the amount of time elapsed since the update send process executed. hours::minutes::seconds.
Duration	Displays the duration in milliseconds of the update send process took.
UPD Built	Displays the number of UPDATE messages built.
UPD Sent	Displays the number of UPDATE messages successfully transmitted to group members. Normally a copy of each UPDATE message built is sent to each group member.
Paths Sent	Displays the number of paths advertised
Pfxs Adv	Displays the number of prefixes advertised

Pfxs Wd	Displays the number of prefixes withdrawn

11-125 show ip bgp vpnv4

This command displays the VPNv4 address information from the BGP table. If an optional VRF is specified, the address information pertaining to that VRF is displayed.

show ip bgp vpnv4 {all | rd *route-distinguisher* **| vrf** *vrf-name***} [***ip-prefix/length***]**

Parameters

all	Displays the complete VPNv4 database.
rd *route-distinguisher*	Displays NLRI prefixes that match the named route distinguisher.
vrf *vrf-name*	Displays NLRI prefixes associated with the named VRF instance.
ip-prefix/length	(Optional) IP address (in dotted decimal format) and the length of the mask (0 to 32). The slash (/) mark must be included.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following example shows all available VPNv4 information in a BGP routing table.

```
(Routing)#show ip bgp vpnv4 all

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network                Next Hop       Metric     LocPrf       Path
Route Distinguisher : 1:10 (for VRF red)
*> 172.20.1.0/24      100.10.1.1            10        100      20 10     i
*> 24.95.16.0/24      100.10.1.1            10        100      20 10     i
*> 24.14.8.0/24       100.10.1.1            10        100      20 10     i

Route Distinguisher : 2:20 (for VRF blue)
*> 173.20.1.0/24      120.10.1.1            10        100      20 10     i
*> 25.95.16.0/24      120.10.1.1            10        100      20 10     i
*> 25.14.8.0/24       120.10.1.1            10        100      20 10     i

Route Distinguisher : 3:30 (for VRF yellow)
*> 174.20.1.0/24      130.10.1.1            10        100      20 10     i
```

```
*> 26.95.16.0/24      130.10.1.1            10        100      20 10     i
*> 26.14.8.0/24       130.10.1.1            10        100      20 10     i
```

The following example shows VPNv4 routing entries for VRF named red.

```
(Routing)#show ip bgp vpnv4 vrf red

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network                Next Hop       Metric     LocPrf       Path
Route Distinguisher : 1:10 (for VRF red)
*> 172.20.1.0/24      100.10.1.1            10        100      20 10     i
*> 24.95.16.0/24      100.10.1.1            10        100      20 10     i
*> 24.14.8.0/24       100.10.1.1            10        100      20 10     i
```

The following example shows the attributes for network 172.20.1.0 that include multi-paths and best path (Use like any of the below formats).

```
(Routing)#show ip bgp vpnv4 vrf red 172.20.1.0 255.255.255.0
(Routing)#show ip bgp vpnv4 vrf red 172.20.1.0/24

Prefix/Prefix Length.............................. 1:100:172.20.1.0/24
Generation ID..................................... 2056
Forwarding........................................ Yes
Advertised to Update Groups....................... 1, 5

Best Path:
Imported from..................................... 2:200:100.10.1.1
Local Preference.................................. 100
AS Path .......................................... 20 10
Origin............................................ IGP
Metric............................................ 10
Type.............................................. External
IGP Cost.......................................... 30
Peer (Peer ID).................................... 100.10.1.1 (32.4.1.1)
BGP Next Hop...................................... 100.10.1.1
Atomic Aggregate.................................. Included
Aggregator (AS, Router ID)........................ 300, 14.1.1.1
Communities....................................... no-export
Extended Community................................ RT:1:100
                                                   RT:2:200
Originator........................................ 10.1.1.1

Non-best Paths:
Local Preference.................................. 200
AS Path........................................... 18 50 27
Or-igin........................................... Incomplete
Type.............................................. External
IGP Cost.......................................... 10
```

```
Peer (Peer ID)..................................... 200.1.1.1 (18.24.1.3)
BGP Next Hop....................................... 200.1.1.1
Extended Community................................. RT:3:300
```

Display Parameters

BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.
Status codes	One of the following: • s: The route is aggregated into an aggregate address configured with the summary-only option. • *: D-LINK OS never displays invalid routes; so this code is always displayed (to maintain consistency with the industw standard). • >: Indicates that BGP has selected this path as the best path to the destination. • i: The route is learned from an internal peer.
Route Distinguisher	The RD associated with the VRF.
Network	Destination prefix.
Next Hop	The route's BGP next hop.
Metric	Displays the BGP metric.
LocPrf	The local preference.
Path	The AS-PATH per route.
Prefix/Prefix Length	The destination prefix and prefix length.
Generation ID	The version of the BGP routing table when this route last changed.
Forwarding	If this BGP route is used for forwarding.
Advertised To Update Groups	The outbound update groups to which this route is advertised.
Local Preference	The local preference, either as received from the peer or as set according to local policy.
AS Path	The AS-PATH. This form ofthe command displays AS-PATHs as long as allowed by bgp maxas-limit.
Origin	Value of the ORIGIN attribute.
Metric	Value of the MED attribute, if included.
Type	If the path is received from an internal or external peer.
IGP Cost	The interior gateway cost (e.g., OSPF cost) to the BGP NEXT HOP.
Peer (Peer ID)	The lP address of the peer that sent this route, and its router ID.
BGP Next Hop	The BGP NEXT HOP attribute.
Atomic Aggregate	If the ATOMIC AGGEGATE attribute is attached to the path.
Aggregator	The AS number and router ID of the speaker that aggregated the route.
Communities	The BGP communities attached to the path.

Originator	If the ORIGINATOR attribute is attached to the path, the value of this attribute.
Cluster List	If the CLUSTER_LIST attribute is attached to the path, the sequence of cluster IDs in the cluster list.
Extended Community	Route target value associated with the specified route.

11-126 show bgp ipv6

Use the **show bgp ipv6** command in Privileged EXEC mode to display IPv6 routes in the BGP routing table.

show bgp ipv6 [*ipv6-prefix* **I** *prefix-length* **[longer-prefixes | shorter-prefixes [***length***]] | filter-list** *as-path-list***]**

Parameters

ipv6-prefix **I** *prefix-length*	(Optional) Limits the output to a specific prefix.
longer-prefixes	(Optional) Display the specified prefix and any longer prefixes within the same range.
shorter-prefixes *length*	(Optional) Used with the ipv6-prefix|prefix-length option to show routes whose prefix length is shorter than prefix-length and, optionally, longer than a specified length. This option may not be given if the longer-prefixes option is given.
filter-list *as-path-list*	(Optional) Filter the output to the set of routes that match a given AS-PATH list. This option may not be given if an ipv6-prefix|prefix-length option is given.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(R1)#show bgp ipv6

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network                  Next Hop     Metric     LocPrf       Path
*> 2001:DB8::/48       3FFE:100::1         10        100     20 10     i
                       3FFE:200::4
```

```
*> 2001:DB8:4:5::/64    3FFE:100::1          10         100      20 10     i
```

Display Parameters

BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.
Status codes	• s: The route is aggregated into an aggregate address configured with the summary-only option • *: D-LINK OS BGP never displays invalid routes; so this code is always displayed • >: Indicates that BGP has selected this path as the best path to the destination • i: If the route is learned from an internal peer
Network	IPv6 destination prefix.
Next Hop	The IPv6 route's BGP NEXT HOP.
Metric	Multi Exit Discriminator.
LocPrf	The local preference.
Path	The AS-PATH.
Origin	The value of the Origin attribute.

11-127 show bgp ipv6 aggregate-address

This command lists IPv6 aggregate addresses that have been configured and indicates whether each is currently active.

show bgp ipv6 aggregate-address

Parameters

The default is None.

Default

None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show bgp ipv6 aggregate-address

Prefix/Len               AS Set    Summary Only     Active
--------------------     -------    ------------    -------
```

```
2001:DB8::/48                 N               Y          Y
3Ffe:4000:1::/48              N               Y          Y
```

Display Parameters

PrefixlLen	Destination prefix and prefix length.
AS Set	Indicates whether an empty AS-PATH is advertised with the aggregate address (N) or an AS SET is advertised with the set ofAS numbers forthe paths contributing to the aggregate (Y).
Summary Only	Indicates whether the individual networks are suppressed (Y) or advertised (N).
Active	Indicates whether the aggregate is currently being advertised.

11-128 show bgp ipv6 community

This command displays IPv6 routes that belong to a given set of communities. The output format and field descriptions are the same as for the command “show bgp ipv6”.

show bgp ipv6 community *communities* **[exact-match]**

Parameters

communities	A string of zero or more community values, which may be in either format and may contain the well-known community keywords no-advertise and no-export. The output displays routes that belong to every community specified in the command.
exact-match	(Optional) Only displays routes that are members of those and only those communities specified in the command.

Default

The default is None.

Command Mode

Privileged EXEC

11-129 show bgp ipv6 community-list

This command displays IPv6 routes that match a community list. The output format and field descriptions are the same as for the command “show bgp ipv6”.

show bgp ipv6 community-list *name* **[exact-match]**

Parameters

name	Displays a standard community list name.
exact-match	(Optional) Display only routes that are an exact match for the set of communities in the matching community list statement.

Default

The default is None.

Command Mode

Privileged EXEC

11-130 show bgp ipv6 listen range

This command displays information adout BGP listen ranges.

show bgp ipv6 listen range [*network/length***]**

Parameters

listen range	Displays all listen subnet ranges that have been created.
network/length	Displays information about specified listen range.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows an example of the command.

```
(Routing)#show bgp ipv6 listen range

Listen Range..................................... 2001::1/64
Inherited Template............................... template_2001

Member                    ASN           State
---------------    ----------    ------------
2001::10               65001     OPENCONFIRM
2001::20                   0          ACTIVE

Listen Range..................................... 2002::1/64
Inherited Template............................... template_2002
```

```
Member                  ASN          State
---------------    ----------    ------------
```

11-131 show bgp ipv6 neighbors advertised-routes

This command displays IPv6 routes advertised to a specific neighbor. The format and field descriptions are the same as for the IPv4 command "show ip bgp neighbors advertised-routes" except that the **Network** and **Next Hop** fields show IPv6 addresses and the command displays IPv4 routes advertised to a specific neighbor with RFC5549.

show bgp ipv6 neighbors {ipv6-address [interface interface-name**] | autodetect** interface interface-name | **policy}**

Parameters

ipv6-address	Displays the IP address of the peer address.
autodetect interface *interface-name*	Displays thepolicy for the given peer.
policy	Display policy for a given peer.

Default

The default is None.

Command Mode

Privileged EXEC

11-132 show bgp ipv6 neighbors route

This command displays a list of IPv6 routes received from a specific neighbor. The list includes either all routes received from the neighbor, received routes that passed inbound policy, or routes rejected by inbound policy. The output and format as the same as for the IPv4 command "show ip bgp neighbors", except that they list IPv6 routes.

show bgp ipv6 neighbors route *ipv6-address* **{adververtised-routes** | **interface** *interface* | **received-routes** | **routes** | **rejected-routes}**

Parameters

advertised-routes	Display routes advertised to a neighbor.
Interface *interface*	Specify the interface for IPv6 link local peer address.
policy	Display policy for a given peer.
received-routes	Display routes received from a neighbor.

rejected-routes	Display routes rejected by inbound policy.
routes	Display routes accepted by inbound policy.

DefaultThe default is None.

Command Mode

Privileged EXEC

11-133 show bgp ipv6 neighbors policy

This command displays the inbound and outbound IPv6 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template.

show bgp ipv6 neighbors [*ipv6-address* **[interface** *interface-name***] | autodetect interface** *interface-name* **policy**

Parameters

ipv6-address	Displays the neighbor's IP address.
interface *interface-name*	(Optional) Displays the specified local interface.
autodetect interface *interface-name*	Displays the routing interface on which the neighbor's link local IPv6 address is auto-detected.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#show bgp ipv6 neighbors Fe80::1 interface 0/1 policy

Neighbor          Policy                               Template
---------------   ----------------------------------   ----------
fe80::1%0/1
                  activate
                  prefix-list jupiter in
                  prefix-list saturn out
                  maximum-prefix 2000
                  send-community
```

11-134 show bgp ipv6 route-reflection

This command shows the configuration of the local router as a route reflector.

show bgp ipv6 route-reflection

Parameters

None.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show bgp ipv6 route-reflection

Cluster ID..................................... 0.0.0.0 (default)
Client-to-client Reflection..................... Enabled
Clients:
Non-client Internal Peers:
```

Display Parameters

Cluster ID	The cluster ID used by tlsis router. The value configured with the bgp cluster-id command is displayed. If no cluster ID is configured, the local router ID is shown and tagged as default.
Client-to-client Reflection	Displays *Enabled* when this router reflects routes received from its clients to its other clients; othenlvise *Disabled* displays.
Clients	A list of this router's internal peers that have been configured as route reflector clients.
Non-client Internal Peers	A list of this router's internal peers that are not configured as route reflector clients. Routes from nqfizstl t peers are reflected to clients and vice-versa.

11-135 show bgp ipv6 neighbors

This command displays a list of IPv6 routes received from a specific neighbor. The list includes either all routes received from the neighbor, received routes that passed inbound policy, or routes rejected by inbound policy. The output and format as the same as for the IPv4 command "show ip bgp neighbors", except:

- IPv6 routes are listed

- If the peer address (“Remote Address”) is a link local address, the next line of output indicates the scope of the address.
- No “IPv4 Outbound Update Group” is listed.
- No IPv4 prefix statistics are shown.
- RFC 5549 Support is displayed only if the BGP neighbor is peered over IPv6 network.
- If the peer is configured as “autodetect”, the “Remote Address” shows detected IPv6 address or “Unresolved” in case if the peer is not detected by the autodetect feature.
- Autodetect status” is displayed only if the peer is configured as “autodetect”. The field shows one of the following statuses: “Peer is detected”, “Peer is not detected” or “Multiple peers are detected”.

show bgp ipv6 neighbors {*ipv6-address***[advertised-routes | interface** *interface slot/port* **| policy | received-routes | rejected-routes | routes]} | autodetect interface** *interface-name* **{received-routes | routes | rejected-routes]} | [interface** *interface-name***] | policy**

Parameters

ipv6-address	(Optional) Displays information about the IPv6 neighbor. If this argument is omitted, information about all neighbors is displayed.
advertised-routes	Display routes advertised to a neighbor.
autodetect *interface-name*	(Optional) Autodetect IPv6 link local peer address.
interface *interface-name*	(Optional) Specify the interface for IPv6 link local peer address.
policy	Display policy for a given peer.
received-routes	(Optional) Display routes received from a neighbor.
rejected-routes	(Optional) Display routes rejected by inbound policy.
routes	(Optional) Display routes accepted by inbound policy.

Default

The default is None.

Command Mode

Privileged EXEC

Example

```
(Routing)#show bgp ipv6 neighbors fe80::2

Description: spine 1 router 1

Remote Address..................................... fe80::2
Autodetect status.................................. Peer is detected
Interface.......................................... 0/1
Remote AS.......................................... 100
Peer ID............................................ 14.3.0.1
Peer Admin Status.................................. START
Peer State......................................... ESTABLISHED
Peer Type.......................................... DYNAMIC
Listen Range....................................... 2061::1/64
Local Port......................................... 179
```

```
Remote Port..................................... 58265
Connection Retry Interval....................... 120 sec
Neighbor Capabilities........................... None
IPv4 Unicast Support............................ None
IPv6 Unicast Support............................ Both
RFC 5549 Support................................ Enable
Update Source................................... None
Local Interface Address......................... fe80::2
Configured Hold Time............................ 90 sec
Configured Keep Alive Time...................... 30 sec
Negotiated Hold Time............................ 30 sec
Keep Alive Time ................................ 10 sec
MD5 Password.................................... password

Last Error (Sent)............................... Hold Timer Expired
Last SubError................................... None
Time Since Last Error........................... 0 day 0 hr 4 min 27 sec
Established Transitions......................... 1
Established Time................................ 0 day 0 hr 4 min 25 sec
Time Since Last Update.......................... 0 day 0 hr 4 min 24 sec
IPv6 Outbound Update Group...................... 7

              Open  Update    Keepalive    Notification    Refresh      Total
Msgs Sent        1       0           10               0          0         11
MSgS Rcvd        1       1           11               0          0         12

Received UPDATE Queue Size: 0 bytes. High: 355. Limit 196096. Drops 0.

IPv6 Prefix Statistics:
                          Inbound        Outbound
Prefixes Advertised             1               0
Prefixes Withdrawn              0               0
Prefixes Current                1               0
Prefixes Accepted               1             N/A
Prefixes Rejected               1             N/A
Max NLRI per Update             1               0
Min NLRI per Update             1               0
```

11-136 show bgp ipv6 statistics

This command shows statistics for the IPv6 decision prooess. Output and field descriptions are the same as for the IPv4 command “show ip bgp statistics”.

show bgp ipv6 statistics

Parameters

None.

Default

The default is None.

Command Mode

Privileged EXEC

11-137 show bgp ipv6 summary

This command displays a summary of BGP IPv6 configuration and status. The output and field descriptions are the same as for the command "show ip bgp summary", except that **Number of Network Entries**, **Number of AS-PATHs**, and **Pfx Rcvd** all count IPv6 rather than IPv4 routing information. The command lists all adjacencies that are configured to carry IPv6 routes.

show bgp ipv6 summary

Parameters

None.

Default

None.

Command Mode

Privileged EXEC

11-138 show bgp ipv6 update-group

This command reports the status of IPv6 outbound update groups and their numbers. Output and format are the same as for "show ip bgp update-group".

show bgp ipv6 update-group [*group-index* **|** *ipv4-address* **|** *ipv6-address* **[interface** *interface-name***] autodetect interface** *interface-name***]**

Parameters

group-index	(Optional) If specified, this option restricts the output to a single update group.
ipv4-address	(Optional) The IPv4 address of a peer enabled for the exchange of IPv6 prefixes. If specified, this option restricts the output to the update group containing the peer with the given address.
ipv6-address	(Optional) The IPv6 address of a peer. If the peer address is a link local address, the interface that defines the scope of the address must also be given. If a peer address is specified, this option restricts the output to the update group containing the peer with the given address.

interface *interface-name*	(Optional) Specify the interface for IPv6 link local peer address.
autodetect interface *interface-name*	(Optional) The routing interface on which the neighbors link local IPv6 address is auto detected.

Default

The default is None.

Command Mode

Privileged EXEC

11-139 snapshot bgp

Use the snapshot bgp command in Support mode to dump a set of BGP debug information to capture the current state of BGP.

snapshot bgp

Parameters

None.

Default

The default is None.

Command Mode

Support mode

Routing Policy Commands

Exterior routing protocols like BGP use industry-standard routing policy to filter and modify routing information exchanged with peers. BGP makes use of the following routing policy constructs:

- AS-PATH Access Lists
- BGP Community Lists

Use the Routing Policy commands to configure routing policies such as:

- Matching on an AS-PATH
- Modifying the AS-PATH
- Setting the local preference
- Setting the route metric
- Setting an IPv6 next hop
- Setting or matching on a BGP community

11-140 ip as-path access-list

To create an AS-PATH access list, use the **ip as-path access-list** command in Global Configuration mode. An AS-PATH access list filters BGP routes on the AS-PATH attribute of a BGP route. The AS-PATH attribute is a list of the autonomous system numbers along the path to the destination. An AS-PATH access list is an ordered sequence of statements. Each statement specifies a regular expression and a permit or deny action. If the regular expression matches the AS-PATH of the route expressed as an ASCII string, the route is considered a match and the statement's action is taken. An AS-PATH list has an implicit deny statement at the end. If a path does not match any of the statements in an AS-PATH list, the action is considered to be deny.

Once you have created an AS-PATH list, you cannot delete an individual statement. If you want to remove an individual statement, you must delete the AS-PATH list and recreate it without the statement to be deleted.

Statements are applied in the order in which they are created. New statements are added to the end of the list. The statement with the first matching regular expression is applied.

D-LINK OS allows configuration of up to 128 AS-PATH access lists, with up to 64 statements each.

To enter the question mark within a regular expression, you must first enter **CTRL-V** to prevent the CLI from interpreting the question mark as a request for help.

See Table 13 for a listing of AS-PATH list regular expression syntax.

Use the **no** command to delete an AS-PATH access list.

{permit | deny} *regexp*

no ip as-path access-list *as-path-list-number*

Parameters

as-path-list-number	A number from 1 to 500 uniquely identifying the list. All AS-PATH access list commands with the same as-path-list-number are considered part of the same list.
permit	(Optional) Permit routes whose AS-PATH attribute matches the regular expression.
deny	(Optional) Deny routes whose AS-PATH attribute matches the regular expression.
regexp	A regular expression used to match the AS-PATH attribute of a BGP path where the AS-PATH is treated as an ASCII string.

Table 13: AS-PATH Regular Expression Syntax

Special Character	Symbol	Behavior
asterisk	*	Matches zero or more sequences of the pattern.
brackets	[]	Designates a range of single-character patterns.
caret	^	Matches the beginning of the input string.
dollar sign	$	Matches the end of the input string.
hyphen	–	Separates the end points of a range.
period	.	Matches any single character, including white space.

plus sign	–	Matches 1 or more sequences of the pattern.
underscore	?	Matches 0 or 1 occurrences of the pattern.
question mark	_	Matches a comma(,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.

Default

The default is None. AS-PATH lists are not configured. There are no default values for any of the parameters of this command.

Command Mode

Global Config

Example

In the following example, the router is configured to reject routes received from neighbor 172.20.1.1 with an AS-PATH that indicates the route originates in, or passes through, AS 100.

```
(Routing)(Config)#ip as-path access-list 1 deny _100_
(Routing)(Config)#ip as-path access-list 1 deny ^100$
(Routing)(Config)#router bgp 1
(Routing)(Config-router)#neighbor 172.20.1.1 remote-as 200
(Routing)(Config-router)#neighbor 172.20.1.1 filter-list 1 in
```

11-141 ip bgp-community new-format

To display BGP standard communities in AA:NN format, use the **ip bgp-community new-format** command in Global Configuration mode. RFC 1997 specifies that the first two bytes of a community number are considered to be an autonomous system number. The new format displays a community number as the ASN followed by a 16-bit AS-specific number.

Use the **no** command to display BGP standard communities as 32-bit integers.

ip bgp-community new-format

no ip bgp-community new-format

Parameters

None.

Default

The is default is as follows: standard communities displayed in AA:NN format.

Command Mode

Global Config

11-142 ip community-list

To create or configure a BGP community list, use the **ip community-list** command in Global Configuration mode. Acommunity list statement with no community values is considered a match for all routes, regardless of their community membership. So the statement **ip community-list bullseye permit** is a permit all statement.

A community number may be entered in either format, as a 32-bit integer or a pair of 16-bit integers separated by a colon, regardless of whether the "ip bgp-community new-format" command is active. Up to 16 communities, including the well-known communities, can be listed in a single command. Up to 32 statements may be configured with a given community list name. Up to 128 unique community list names may be configured.

Use the **no** command to delete a community list.

ip community-list *standard list-name* **{permit | deny} [***community-number***] [no-advertise] [no-export] [no-export subconfed] [no-export]**

no ip community-list *standard list-name*

Parameters

standard list-name	Identifies a named standard community list. The name may contain up to 32 characters.
permit	Indicates that matching routes are permitted.
deny	Indicates that matching routes are denied.
community	(Optional) From 0 to 16 community numbers formatted as a 32-bit integers or in AA:NN format, whereAA is a 2-byte autonomous system number and NN is a 16 bit integer. The range is 1 to 4,294,967,295 (any 32-bit integer other than 0). Communities are separated by spaces.
no-advertise	(Optional) The well-known standard community, NO_ADVERTISE (0xFFFFFF02).
no-export	(Optional) The well-known standard community, NO_EXPORT, (0XFFFFFF01).
no-export-subconfed	(Optional) Deny only routes that are not exported to other external peers.
no-export	(Optional) Deny only routes that are not exported to other peers.

Default

The default is Community lists are not configured.

Command Mode

Global Config

11-143 show ip as-path-access-list

This command displays the contents of AS-PATH access lists.

show ip as-path-access-list [*as-path-list-number***]**

Parameters

as-path-list-number	(Optional) When an AS-PATH list number is specified, the output is limited to the single AS-PATH list specified. The number is an integer from 1 to 500.

Default

The defaultis None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip as-path-access-list

AS path access list 1
       deny _100_
       deny ^100$

AS path access list 2
       deny _260_
       deny ^200$
```

11-144 show ip community-list

This command displays community lists. The format of community values is dictated by the command “ip bgp-community new-format”.

show ip community-list [*community-list-name***] {detail}**

Parameters

community-list-name	(Optional) A standard community list name. This option limits the output to a single list.
detail	Show statistics about community lists.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip community-list

Standard community list buzz
       permit 100:200
       permit 100:300
       permit 100:400
Standard community list woody
       permit 200:1
       permit 200:2
       permit 200:3
```

11-145 clear ip community-list

This command clears community lists.

clear ip community-list [*list-name***]**

Parameters

list-name	(Optional) A community list name.

Default

The default is None.

Command Mode

Privileged EXEC

12. Quality of Service Commands

This chapter describes the Quality of Service (QoS) commands available in the D-LINK OS CLI.

The QoS Commands chapter contains the following sections:

Note: The commands in this chapter are in one of two functional groups:

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

Class of Service Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

12-1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *userpriority* values can range from 0-7. The *trafficclass* values range from 0-6, although the actual number of available traffic classes depends on the platform.

Use the **no** command to map each 802.1 p priority to its default internal traffic class value.

classofservice dot1p-mapping *userpriority trafficclass*

no classofservice dot1p-mapping

Parameters

userpriority	User defined priority from 0-7.
trafficclass	The traffic class from 0-6.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-2 classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The *ipdscp* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23,af31, af32, af33, af41, af42, af43, be,cs0, cs1. cs2, cs3, cs4. cs5, cs6, cs7, ef.

The *trafficclass* values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Use the **no** command to map each IP DSCP value to its default internal traffic class value.

classofservice ip-dscp-mapping *ipdscp trafficclass*

no classofservice ip-dscp-mapping

Parameters

ipdscp	IP DSCP value.
trafficclass	The mapping class.

Default

The default is None.

Command Mode

Global Config

12-3 classofservice trust

This command sets the class of service trust mode of an interface or range of interfaces. You can set the mode to trust one of the Dot1p (802.1 p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the **show running config** command because Dot1p is the default.

Note: The **classofservice trust dotlp** command will not be supported in future releases of the software because Dot1p is the default value. Use the **no classofservice trust** command to set the mode to the default value.

Use the **no** command to set the interface mode to the default value.

classofservice trust {dot1p | ip-dscp | untrusted}

no classofservice trust

Parameters

dot1p	The bit of dot1p number

ip-dscp	The bit of the ip-dscp value.
untrusted	Sets the class of service trust mode for all interfaces to untrusted.

Default

The default is dot1p.

Command Mode

- Global Config
- Interface Config

12-4 cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. The total number of queues supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Use the **no** command to restore the default for each queue's minimum bandwidth value.

cos-queue min-bandwidth *bw-0 bw-1 … bw-n*

no cos-queue min-bandwidth

Parameters

bw-0 bw-1 … bw-n	Enter the minimum bandwidth percentage for the selected queue.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-5 cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the **random-detect queue-parms** and the **random-detect exponential-weighting-constant** commands.

Use the **no** command to restore WRED to the default value.

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

At least one, but no more than n queue-id values are specified with this command. Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (n-1), where n is the total number of queues supported per interface. The number n = 7 and corresponds to the number of supported queues (traffic classes).

cos-queue random-detect *queue-id-1* **[***queue-id-2 … queue-id-n***]**

no cos-queue random-detect *queue-id-1* **[***queue-id-2 … queue-id-n***]**

Parameters

queue-id-1 queue-id-n	Enter the value ranging from 0 to 7 representing the queue ID.
queue-id-2 … queue-id-n	(Optional) Enter the value where “n” is the queue ID.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-6 cos-queue strict

This command activates the strict priority scheduler mode for each specified queue for an interface queue on an interface, a range of interfaces, or all interfaces.

Use the **no** command to restore the default weighted scheduler mode for each specified queue.

cos-gueue strict *queue-id-1* **[***queue-id-2 … queue-id-n***]**

no cos-gueue strict *queue-id-1* **[***queue-id-2 … queue-id-n***]**

Parameters

queue-id-1 queue-id-n	Enter the value ranging from 0 to 7 representing the queue ID.
queue-id-2 … queue-id-n	(Optional) Enter the value where “n” is the queue ID.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-7 random-detect

This command is used to enable WRED for the interface as a whole. and is only available when per-queue WRED activation control is not supported by the device Specific WRED parameters are configured using the **random-detect queue-parms** and the **random-detect exponential-weighting-constant** commands.

Use the **no** command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

When specified in Interface Config mode, this command only affects a single interface. In contrast, in Global Config mode, it applies to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

random-detect *queue-id-0 queue-id-1*

no random-detect *queue-id-0 queue-id-1*

Parameters

queue-id-1	Enter the value ranging from 0 to 7 representing the queue ID.

Default

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-8 random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

Use the **no** command to set the WRED decay exponent back to the default.

random-detect exponential-weighting-constant *1-15*

no random-detect exponential-weighting-constant

Parameters

None.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-9 random-detect queue-parms

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the **cos-queue random-detect** command).

Use the **no** command to set the WRED configuration back to the default.

Each parameter is specified for each possible drop precedence (color of TCP traffic). The last precedence applies to all non-TCP traffic. For example, in a 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

random-detect queue-parms *queue-id-1* **[***queue-id-2 … queue-id-n***] min-thresh** *thresh-prec-1 … thresh-prec-n* **max-thresh** *thresh-prec-1 … thresh-prec-n* **drop-probability** *prob-prec-1 … prob-prec-n*

no random-detect queue-parms *queue-id-1* **[***queue-id-2 … queue-id-n***]**

Parameters

queue-id-1 queue-id-n	Enter the value ranging from 0 to 7 representing the queue ID.
queue-id-2 … queue-id-n	(Optional) Enter the value where “n” is the queue ID.
min-thresh	The minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
max-thresh	The maximum threshold is the queue depth (as a percentage) above which WRED marks/drops all traffic.
drop-probability	The percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-10 traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. You can also specify this value for a range of interfaces or all interfaces. Also known as rate shaping, traffic

shaping has the effect of smoothing temporaw traffic bursts over time so that the transmitted traffic rate is bounded.

Use the **no** command to restore the interface shaping rate to the default value.

traffic-shape *bw*

no traffic-shape

Parameters

bw	The shaping bandwidth percentage from 0 to 100 in increments of 1.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-11 show classofservice dot1p-mapping

This command displays the current Dot1 p (802.1 p) priority mapping to internal traffic classes for a specific interface. The *slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

show classofservice dot1p-mapping [*slot/port***]**

Parameters

slot/port	(Optional) Displays the interface number. This is only valid on platforms that support independent per port class of service mappings.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

The following information is repeated for each user priority.

User Priority	The 802.1p user priorilty value.
Traffic Class	The traffic class internal queue identifier to which the user priority value

	is mapped.

12-12 show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

show classofservice ip-precedence-mapping [*slot/port***]**

Parameters

slot/port	(Optional) Displays the interface number.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

12-13 show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

show classofservice ip-dscp-mapping

Parameters

None.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

IP DSCP	Displays the IP DSCP value.
Traffic Class	Displays the traffic class internal queue identifier to which the IP DSCP value is mapped.

12-14 show classofservice trust

This command displays the current trust mode setting for a specific interface. The *slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

show classofservice trust [*slot/port***]**

Parameters

slot/port	(Optional) Displays the interface number.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

12-15 show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The *slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

show interfaces cos-queue [*slot/port***]**

Parameters

slot/port	(Optional) Displays the interface number.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Queue Id	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
Minimum Bandwidth	The minimum transmission bandwidth guarantee forthe queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme.
Queue Management Type	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Interface	The slot/port of the interface.If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface.

12-16 show interfaces random-detect

This command displays the global WRED settings for each CoS queue. Ifyou specify the *slot/port*, the command displays the WRED settings for each CoS queue on the specified interface.

show interfaces random-detect [*slot/port***]**

Parameters

slot/port	(Optional) Displays the interface number.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Queue ID	An interface supports n queues numbered 0 to (n-1). The n value is platform dependent.
WRED Minimum Threshold	The configured minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
WRED Maximum Threshold	The configured maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
WRED Drop Probability	The configured percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

Differentiated Services Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

- Class
  - Creating and deleting classes.
  - Defining match criteria for a class.
- Policy
  - Creating and deleting policies
  - Associating classes with a policy
  - Defining policy statements for a policy/class combination
- Service
  - Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and recreate it.

Note: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

12-17 diffserv

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

Use the **no** command to set the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

diffserv

no diffserv

Parameters

None.

Default

The default is None.

Command Mode

Global Config

DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands

specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

Note: Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and recreate the entire class.

The CLI command root is class-map.

12-18 class-map

This command defines a DiffServ class of type match-all. When used without any match condition, this

command enters the class-map mode. The *class-map-name* is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Note: The class-map-name ‘default’ is reserved and must not be used.

The class type of **match-all** indicates all of the individual match conditions must be true for a packet to be considered a member of the class.This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

Note: The optional keywords **[{ipv4 | ipv6}]** specify the Layer 3 protocol for this class. If not specified, this parameter defaults to **ipv4**. This maintains backward compatibility for configurations defined on systems before lPv6 match items were supported.
The optional keyword appiq creates a new DiffServ appiq class. Regular expressions found in the traffic patterns in layer 7 applications can be matched to the App-IQ class using a **match signature** command.

Note: The CLI mode is changed to Class-Map Config or lpv6-Class-Map Config when this command is successfully executed depending on the **[{ipv4 | ipv6}]** keyword specified.

Use the **no** command to eliminate an existing DiffServ class. The *class-map-name* is the name of an existing DiffServ class. (The class name **default** is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

class-map match-all *class-map-name* **[{ ipv4 | ipv6}]**

no class-map *class-map-name*

Parameters

match-all	Indicates all of the individual match conditions must be true for a packet to be considered a member of the class.
class-map-name	Case sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.
ipv4 | ipv6	(Optional) Specifies the class. If not specified, this parameter defaults to IPv4.

Default

The default is None.

Command Mode

Global Config

12-19 class-map rename

This command changes the name of a DiffServ class. The *class-map-name* is the name of an existing DiffServ class. The *new-class-map-name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

class-map rename *class-map-name new-class-map-name*

Parameters

class-map-name	Enter a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class name.
new-class-map-name	Enter a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying a new class name.

Default

The default is None.

Command Mode

Global Config

12-20 match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The *ethertype* value is specified as one of the following keywords: **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, **rarp** or as a custom EtherType value in the range of 0x0600-0xFFFF. Use the [not] option to negate the match condition.

match [not] ethertype {*keyword* **| custom** *0x0600-0xFFFF***}**

Parameters

not	(Optional) Specify to negate the match condition.
keyword	Specifies appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast etc.
custom *0x0600-0xFFFF*	Specifies ethertype value.

Default

The default is None.

Command Mode

Class-Map Config

12-21 match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. Use the [not] option to negate the match condition.

match [not] any

Parameters

not	(Optional) Specify to negate the match condition.

Default

The default is None.

Command Mode

Class-Map Config

12-22 match class-map

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

Use the **no** command to remove from the specified class definition the set of match conditions defined for another class.

Note:

- The parameters refctassname and class-map-name can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the refclassname class while the class is still referenced by any class-mup-name fails.
- The combined match criteria of class-map-name and refclassname must be an allowed combination based on the class type.
- Any subsequent changes to the refclassname class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal ofa refclass rule reduces the maximum number of available rules in the class definition by one.

match class-map *refclassname*

no match class-map *refclassname*

Parameters

refclassname	Specify the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default

The default is None.

Command Mode

Class-Map Config

12-23 match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet).. Use the [not] option to negate the match condition.

match [not] cos *0-7*

Parameters

not	(Optional) Specify to negate the match condition.

Default

The default is None.

Command Mode

Class-Map Config

12-24 match secondary-cos

This command adds to the specified class definition a match condition forthe secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). Use the [**not**] option to negate the match condition.

match [not] secondary-cos *0-7*

Parameters

not	(Optional) Specify to negate the match condition.

Default

The default is None.

Command Mode

Class-Map Config

12-25 match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The *macaddr* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). Use the [**not**] option to negate the match condition.

match [not] destination-address mac *macaddr macmask*

Parameters

not	(Optional) Specify to negate the match condition.
macaddr	Specifies any layer 2 MAC address.
macmask	Specifies a layer 2 MAC address bit mask.

Default

The default is None.

Command Mode

Class-Map Config

12-26 match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the [**not**] option to negate the match condition.

match [not] dstip *ipaddr ipmask*

Parameters

not	(Optional) Specify to negate the match condition.
ipaddr	Specifies an IP address.
ipmask	Specifies an IP address bit mask; note that although similar to a standard subnet mask, this bit mask need not be contiguous.

Default

The default is None.

Command Mode

Class-Map Config

12-27 match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet. Use the [**not**] option to negate the match condition.

match [not] dstip6 *destination-ipv6-prefix/prefix-length*

Parameters

not	(Optional) Specify to negate the match condition.
destination-ipv6-prefix/prefix-length	IPv6 address and prefix length.

Default

The default is None.

Command Mode

lpv6-Class-Map Config

12-28 match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *portkey* is one of the supported port name keywords. The currently supported *portkey* values are: domain, echo, ftp, ftpdata, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [**not**] option to negate the match condition.

match [not] dstl4port {*portkey* **| 0-65535}**

Parameters

not	(Optional) Specify to negate the match condition.
portkey	To specify the match condition as a single keyword, the value for <portkey> is one of the supported port name keywords. The currently supported <portkey> values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.
<0-65535>	To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535. To specify the match condition using a numeric range notation, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

Default

The default is None.

Command Mode

Class-Map Config

12-29 match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22 af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef. Use the [**not**] option to the match condition.

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

match ip dscp *dscpval*

Parameters

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

Default

The default is None.

Command Mode

Class-Map Config

12-30 match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7. Use the [**not**] option to negate the match condition.

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

match [not] ip precedence *0-7*

Parameters

not	(Optional) Specify to negate the match condition.

Default

The default is None.

Command Mode

Class-Map Config

12-31 match ip tos

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

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation

Note: This “free form” version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

match [not] ip tos *tosbits tosmask*

Parameters

not	(Optional) Specify to negate the match condition.
tosbits	Two-digit hexadecimal number from 00 to ff.
tosmask	Two-digit hexadecimal number from 00 to ff. The <tosmask> denotes the bit positions in <tosbits> that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a <tosbits> value of a0 (hex) and a <tosmask> of a2 (hex).

Default

The default is None.

Command Mode

Class-Map Config

12-32 match ip6flowlbl

Use this command to enter an IPv6 flow label value. Use the [**not**] option to negate the match condition.

match [not] ip6flowlbl label *0-1048575*

Parameters

not	(Optional) Specify to negate the match condition.

Default

The default is None.

Command Mode

IPv6-Class-Map Config

12-33 match protocol

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

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

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Use the [**not**] option to negate the match condition.

Note: This command does not validate the protocol number value against the current list defined by IANA.

match [not] protocol {*protocol-name* **| 0-255}**

Parameters

not	(Optional) Specify to negate the match condition.
protocol-name	One of the supported protocol name keywords. The currently supported values are: icmp, igmp, ip, tcp, udp. Note that a value of ip is interpreted to match all protocol number values.
0-255	To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255.

Default

The default is None.

Command Mode

Class-Map Config

12-34 match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The *address* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal

numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). Use the **[not]** option to negate the match condition.

match [not] source-address mac *address macmask*

Parameters

not	(Optional) Specify to negate the match condition.
address	Specifies any layer 2 MAC address.
macmask	Specifies a layer 2 MAC address bit mask.

Default

The default is None.

Command Mode

Class-Map Config

12-35 match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the **[not]** option to negate the match condition.

match [not] srcip *ipaddr ipmask*

Parameters

not	(Optional) Specify to negate the match condition.
ipaddr	Specifies an IP address.
ipmask	Specifies an IP address bit mask; note that although it resembles a standard subnet mask, this bit mask need not be contiguous.

Default

The default is None.

Command Mode

Class-Map Config

12-36 match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet. Use the **[not]** option to negate the match condition.

match [not] srcip6 *source-ipv6-prefix/prefix-length*

Parameters

not	(Optional) Specify to negate the match condition.
source-ipv6-prefix/prefix-length	IPv6 address and prefix length.

Default

The default is None.

Command Mode

lpv6-Class-Map Config

12-37 match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for portkey is one of the supported port name keywords (listed below). The currently supported portkey values are: domain, echo, ftp, ftpdata, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the **[not]** option to negate the match condition.

match not srcl4port {*portkey* **| 0-65535}**

Parameters

portkey	One of the supported port name keywords (listed below). The currently supported <portkey> values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each translates into the equivalent port number, which is used as both the start and end of a port range.
0-65535	To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535. To specify the match condition as a range, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

Default

The default is None.

Command Mode

Class-Map Config

12-38 match src port

This command adds a match condition for a range of layer source 4 ports. lf an interface receives traffic that is within the configured range of layer 4 source ports, then only the appiq class is in effect. *portvalue* specifies a single source port.

match src port {*portstart-portend* **|** *portvalue***}**

Parameters

portstart-portend	Specify a match ondition for a range of layer source ports.
portvalue	Specify a single port source.

Default

The default is None.

Command Mode

Class-Map Config

12-39 match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN identifier field (the only tag in a single tagged packet or the first or outer tag ofa double VLAN tagged packet). The VLAN ID is an integer from 0 to 4095. Use the **[not]** option to negate the match condition.

match [not] vlan *0-4095*

Parameters

not	(Optional) Specify to negate the match condition.

Default

The default is None.

Command Mode

Class-Map Config

12-40 match secondary-vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN tagged packet). The secondary VLAN ID is an integer from 0 to 4095. Use the **[not]** option to negate the match condition.

match [not] secondary-vlan *0-4095*

Parameters

not	(Optional) Specify to negate the match condition.

Default

The default is None.

Command Mode

Class-Map Config

DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes.

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

Note: The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and readd it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

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

12-41 assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The *queueid* is an integer from 0 to n-1, where n is the number of egress queues supported by the device.

assign-queue *queueid*

Parameters

queueid	Enter the queue ID ranging from 0 to 7.

Default

The default is None.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop

12-42 drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

drop

Parameters

None.

Default

The default is None.

Command Mode

Policy-Class-Map Config

Incompatibilities

Assign Queue, Mark (all forms), Mirror, Police, Redirect

12-43 mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

mirror *slot/port*

Parameters

slot/port	Specifies the physical interface where of the destination mirrored packet.

Default

The default is None.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Redirect

12-44 redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

redirect *slot/port*

Parameters

slot/port	Specifies the physical interface where of the destination mirrored packet.

Default

The default is None.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mirror

12-45 conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The *class-map-name* parameter is the name of an existing DiffServ class map.

Note: This command may only be used after specifying a police command for the policy-class instance.

conform-color *class-map-name*

Parameters

class-map-name	Name of an existing Diffserv class map, where different ones must be

used for the conform colors.

Default

The default is None.

Command Mode

Policy-Class-Map Config

12-46 class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The *classname* is the name of an existing DiffServ class.

Note: This command causes the specified policy to create a reference to the class definition.

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

Use the **no** command to delete the instance of a particular class and its defined treatment from the specified policy. classname is the names of an existing DiffServ class.

Note: This command removes the reference to the class definition for the specified policy.

class *classname*

no class *classname*

Parameters

classname	The name of an existing DiffServ class. The command causes the specified policy to create a reference to the class definition.

Default

The default is None.

Command Mode

Policy-Map Config

12-47 mark cos

This command marks all packets for the associated traffic stream with the specified class of service (CoS) value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7

mark cos *0-7*

Parameters

None.

Default

The default is 1.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mark IP DSCP, IP Precedence, Police

12-48 mark secondary-cos

This command marks all packets for the associated traffic stream with the specified secondary class of service (CoS) value in the priority field of the 802.1p header (the secondary or inner 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

mark secondary-cos *0-7*

Parameters

None.

Default

The default is None.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mark IP DSCP, IP Precedence, Police

12-49 mark cos-as-sec-cos

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking Cos as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

mark-cos-as-sec-cos

Parameters

None.

Default

The default is None.

Command Mode

Policy-Class-Map Config

Example

The following shows an example of the command.

```
(Routing)(Config-policy-classmap)#mark cos-as-sec-cos
```

Incompatibilities

Drop, Mark IP DSCP, IP Precedence, Police

12-50 mark ip-dscp

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

mark ip-dscp *dscpval*

Parameters

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

Default

The default is None.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mark CoS, Mark IP Precedence, Police

12-51 mark ip-precedence

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

mark ip-precedence *0-7*

Parameters

None.

Default

The default is None.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mark CoS, Mark IP Precedence, Police

Policy Type

In

12-52 police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the **police** command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

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

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

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

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

police-simple {*1-4294967295 1-128* **conform-action {drop | set-cos-as-sec-cos | set-cos-transmit** *0-7* **| set-sec-cos-transmit** *0-7* **| set-prec-transmit** *0-7* **| set-dscp-transmit** *0-63* **| transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit** *0-7* **| set-sec-cos-transmit** *0-7* **| set-prec-transmit** *0-7* **| set-dscp-transmit** *0-63* **| transmit}]}**

Parameters

conform-action & violate-action	The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or set-cos-transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has

	been configured. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.
set-cos-transmit	Priority value is required and is specified as an integer from 0-7.
set-dscp-transmit	Required and specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.
set-prec-transmit	IP Precedence value is required and is specified as an integer from 0-7.

Default

The default is None.

Command Mode

Policy-Class-Map Config

Example

The following shows an example of the command.

```
(Routing)(Config-policy-classmap)#police-simple 1 128 conform-action transmit violate-action drop
```

Incompatibilities

Drop, Mark (all forms)

12-53 police-single-rate

This command is the single-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cost, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this single-rate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

police-single-rate {*1-4294967295 1-128 1-128* **conform-action {drop | set-cos-as-sec-cos | set-cos-transmit** *0-7* **| set-sec-cos-transmit** *0-7* **| set-prec-transmit** *0-7* **| set-dscp-transmit** *0-63* **| transmit} exceed-action {drop | set-cos-as-sec-cos | et-cos-transmit 0-7 | set-sec-cos-transmit** *0-7* **| set-prec-transmit** *0-7* **| set-dscp-transmit** *0-63* **| transmit} [violate-action {drop | set-cos-as-sec-cos-transmit | set-cos-transmit** *0-7* **| set-sec-cos-transmit** *0-7* **| set-prec-transmit** *0-7* **| set-dscp-transmit** *0-63* **| transmit}]}**

Parameters

conform-action & violate-action	The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-

	transmit, or set-cos-transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.
set-cos-transmit	Priority value is required and is specified as an integer from 0-7.
set-dscp-transmit	Required and specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.
set-prec-transmit	IP Precedence value is required and is specified as an integer from 0-7.

Default

The default is None.

Command Mode

Policy-Class-Map Config

12-54 police-two-rate

This command is the two-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

police-two-rate {*1-4294967295 1-4294967295 1-128 1-128* **conform-action {drop | set-cos-as-sec-cos | set-cos-transmit** *0-7* **| set-sec-cos-transmit** *0-7* **| set-prec-transmit** *0-7* **| set-dscp-transmit** *0-63* **| transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit** *0-7* **| set-sec-cos-transmit** *0-7* **| set-prec-transmit** *0-7* **| set-dscp-transmit** *0-63* **I transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit** *0-7* **| set-sec-cos-transmit** *0-7* **| set-prec-transmit** *0-7* **| set-dscp-transmit** *0-63* **| transmit}]}**

Parameters

conform-action & violate-action	The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or set-cos-transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.
set-cos-transmit	Priority value is required and is specified as an integer from 0-7.

set-dscp-transmit	Required and specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.
set-prec-transmit	IP Precedence value is required and is specified as an integer from 0-7.

Default

The default is None.

Command Mode

Policy-Class-Map Config

12-55 policy-map

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

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

Use the **no** command to eliminate an existing DiffServ policy. The policyname parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

policy-map *policyname* **in**

no policy-map *policyname*

Parameters

policyname	Policy name up to 31 alphanumeric characters.

Default

The default is None.

Command Mode

Global Config

12-56 policy-map rename

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

policy-map rename *policyname newpolicyname*

Parameters

policyname	Enter the policy name up to 31 alphanumeric characters.
newpolicyname	Enter the new policy name up to 31 alphanumeric characters.

Default

The default is None.

Command Mode

Global Config

DiffServ Service Commands

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

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

12-57 service-policy

This command attaches a policy to an interface in the inbound direction. The *policyname* parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

Note: This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode ' command for DiffServ.

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

Use the **no** command to detache a policy from an interface in the inbound direction. The policyname parameter is the name of an existing DiffServ policy.

Note: The **no** command causes a service to remove its reference to the policy. The **no** command effectively disables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Note: Each interface can have one policy attached.

service-policy in *policymapname*

no service-policy in *policymapname*

Parameters

policymapname	The name of an existing DiffServ policy, whose type must match the interface direction. The command causes a service to create a reference to the policy.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

12-58 show class-map

This command displays all configuration information for the specified class. The *class-name* is the name of an existing DiffServ class.

show class-map *class-name*

Parameters

class-name	Enter the name of an existing DiffServ class.

Default

The default is None.

Command Mode

- Privileged EXEC
- User EXEC

Display Parameters

If the *class-name* is specified the following fields are displayed.

Class Name	The name of this class.
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
L3 Proto	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.

Match Criteria	The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.
Values	The values of the Match Criteria.

If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed.

Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

12-59 show diffserv

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

show diffserv

Parameters

None.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show diffserv

DiffServ Admin Mode.............................. Enable
Class Table Size Current/Max..................... 0 / 32
Class Rule Table Size Current/Max................ 0 / 416
Policy Table Size Current/Max.................... 0 / 64
```

```
Policy Instance Table Size Current/Max..... 0 / 1792
Policy Attribute Table Size Current/Max..... 0 / 5376
Service Table Size Current/Max.............. 0 / 298
```

Display Parameters

DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size	The current number of entries (rows) in the Class Table.
Class Table Max	The maximum allowed entries (rows) for the Class Table.
Class Rule Table Size	The current number of entries (rows) in the Class Rule Table.
Class Rule Table Max	The maximum allowed entries (rows) for the Class Rule Table.
Policy Table Size	The current number of entries (rows) in the Policy Table.
Policy Table Max	The maximum allowed entries (rows) for the Policy Table.
Policy Instance Table Size	Current number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max	Maximum allowed entries (rows) for the Policy Instance Table.
Policy Attribute Table Size	Current number of entries (rows) in the Policy Attribute Table.
Policy Attribute Table Max	Maximum allowed entries (rows) for the Policy Attribute Table.
Service Table Size	The current number of entries (rows) in the Service Table.
Service Table Max	The maximum allowed entries (rows) for the Service Table.

12-60 show policy-map

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

show policy-map [*policy-map-name***]**

Parameters

policy-map-name>	(Optional) Displays the name of an existing DiffServ policy.
interface	Display summary service information for Diffserv interfaces.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output including the mark-cos-as-sec-cos option specified in the policy action.

```
(Routing)#show policy-map p1

Policy Name..................................... p1
Policy Type..................................... In
Class Name...................................... c1
Mark CoS as Secondary CoS....................... Yes
```

The following shows example CLI display output including the mark-cos-as-sec-cos action used in the policing (simple-police, police-single-rate, police two-rate) command.

```
(Routing)#show policy-map p2

Policy Name..................................... p2
Policy Type..................................... In
Class Name...................................... c2
Policing Style.................................. Police Two Rate
Committed Rate.................................. 1
Committed Burst Size............................ 1
Peak Rate....................................... 1
Peak Burst Size................................. 1
Conform Action.................................. Mark CoS as Secondary CoS
Exceed Action................................... Mark CoS as Secondary CoS
Non-Conform Action.............................. Mark CoS as Secondary CoS
Conform Color Mode.............................. Blind
Exceed Color Mode............................... Blind
```

Display Parameters

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

Policy Name	The name of this policy.
Policy Type	The policy type (only inbound policy definitions are supported for this platform.)

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

Class Name	The name of this class.
Policing Style	The style of policing, if any, used (simple).
Committed Rate (Kbps)	The committed rate, used in simple policing.
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Peak Rate	Guarantees a committed rate for transmission, but also transmits excess traffic bursts up to a user-specified peak rate, with the understanding that a downstream network element (such as the next hop's policer) might drop this excess traffic. Traffic is held in queue until it is

	transmitted or dropped (pertype of queue depth management.) Peak rate shaping can be configured for the outgoing transmission stream for an AF (Assured Forwarding) traffic class (although average rate shaping could also be used.)
Peak Burst Size	(PBS). The network administrator can set the PBS as a means to limit the damage expedited fonivarding traffic could inflict on other traffic (e.g., a token bucket rate limiter) Traffic that exceeds this limit is discarded.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Exceed Action	The action taken on traffic that exceeds settings that the network administrator specifies.
Non-Conform Action	The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
Conform Color Mode	The current setting for the color mode. Policing uses either color blind or color aware mode.Color blind mode ignores the coloration (marking) ofthe incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome.
Exceed Color Mode	The current setting for the color of exceeding traffic that the user may optionally specify.

12-61 show diffserv service

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

show diffserv service *slot/port* **in**

Parameters

slot/port	Displays a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing) #show diffserv service 0/1 in
```

```
DiffServ Admin Mode.......................... Enable
Interface.................................... 0/1
Direction.................................... In
No policy is attached to this interface in this direction.
```

Display Parameters

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

12-62 show diffserv service brief

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

show diffserv service brief [in]

Parameters

in	(Optional) Displays the inbound direction.
out	(Optional) Displays the outbound direction.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

DiffServ Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled

	mode.

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

Interface	Displays the slot/port interface.
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

12-63 show policy-map interface

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

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

show policy-map interface {*slot/port* **| lag** *lag-id***} [in]**

Parameters

slot/port	Displays the slot/port interface.
lag *lag-id*	Displays the interface in lag format.
in	(Optional) Displays the inbound direction.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

Interface	The port or LAG associated with the policy.
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance Within this policy.

Class Name	The name of this class instance.

In Discarded Packets	A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

12-64 show service-policy

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

show service-policy [in | out]

Parameters

In	(Optional) Displays the inbound direction.
out	(Optional) Displays the outbound direction.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

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

Interface	The interface associated with the service policy.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

MAC Access Control List Commands

This section describes the commands you use to configure MAC Access Control List (ACL) settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet ll frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- If an IP ACL is configured on an interface, you cannot configure a MAC ACL on the same interface.

12-65 mac access-list extended

This command creates a MAC Access Control List (ACL) identified by name, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

lf a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Use the **no** command to delete a MAC ACL identified by *name* from the system.

mac access-list extended *name*

no mac access-list extended *name*

Parameters

name	Enter the ACL name to identify a specific MAC ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

Default

The default is None.

Command Mode

Global Config

12-66 mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The *name* parameter is the name of an existing MAC ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name newnume already exists.

mac access-list extended rename *oldname newname*

Parameters

oldname	Enter the old name of an existing MAC ACL to be changed.
newname	Enter the new name of an existing MAC ACL to be changed.

Default

The default is None.

Command Mode

Global Config

12-67 mac access-list resequence

Use this command to renumber the sequence numbers of the entries for specified MAC access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

Note: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

mac access-list resequence {*name* **|** *id***}** *starting-sequence-number increment*

Parameters

name	Enter the ACL name which is used to identify a specific MAC ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
1-2147483647	The sequence number from which to start. The range is 1-2147483647. The default is 1.
1-2147483647	The amount to increment. The range is 1-2147483647. The default is 1.

Default

The default is 10.

Command Mode

Global Config

12-68 {deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Use the **no** command to remove the ACL rule with the specified sequence number from the ACL.

Note: An implicit deny all MAC rule always terminates the access list.

[*sequence-number***] {deny | permit} {***srcmac* **| any} {***dstmac* **| any} [***ethertypekey* **|** *0x0600-0xFFFF***] [vlan {eq** *0-4095* | **range}] [cos** *0-7***] [[log] [time-range** *time-range-name***] [assign-queue** *queue-id***]] [{mirror | redirect}** *slot/port***][rate-limit** *rate burst-size***]**

no sequence-number

Parameters

sequence-number	(Optional) The sequence number of the prefix list entry.
deny	Enter to deny the specified Ethernet layer 2 packet.
permit	Enter to permit the specified Ethernet layer 2 packet.
srcmac	Enter to identify the source MAC address of the rule.
any	Any MAC source or destination address.
dstmac	Enter to identify the destination MAC address of the rule.
ethertypekey	(Optional) Enter a keyword to specify an Ethertype (appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp).
Eq *0-4095*	Specify a VLAN value.
range	Specify a VLAN range.
cos *0-7*	Enter to c onfigure a match condition based on a COS value.
secondary-cos	Configure a match condition based on secondary COS value.
secondary-vlan	Configure a match condition based on secondary VLAN.
log	Enter to configure logging for this access list rule.
time-range *time-range-name*	(Optional) Enter a time-range parameter to impose a time limit on the MAC ACL rule.
assign-queue *queue-id*	(Optional) Enter the assign-queue parameter to specify a particular hardware queue for handling traffic that matches the rule.
mirror	(Optional) Allows the traffic matching of the rule to be copied to the specified slot/port while the redirect parameter allows the traffic matching this rule to be forwarded to the specified slot/port.
redirect	Configure the packet redirection attribute.
slot/port	(Optional) Enter the slot / port values.
rate-limit *rate burst-size*	(Optional) Set the rate-limit to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The *sequence-number* specifies the sequence number for the ACL rule. The sequence number is specified by the user or is generated by device.

If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed in the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. A rule cannot be created that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule.

For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, the user can move the ACL rule to a different position in the ACL.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported ethertypekey values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Table 14: Ethertype Keyword and 4-di it Hexadecimal Value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The **vlan** and **cos** parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The **time-range** parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see “Time Range Commands for Time-Based ACLs”.

The **assign-queue** parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The assign-queue parameter is valid only for a permit rule.

Note: The **mirror** and **redirect** parameters are not available on all 5000 SKUs.

Note: The special command form **{deny | permit} any any** is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

The **permit** command’s optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

Default

The default is None.

Command Mode

Mac-Access-List Config

Example

The following shows an example of the command.

```
(Routing)(Config)#mac access-list extended mac1
```

```
(Routing)(Config-mac access-list)#permit 00:00:00:00:aa:bb ff:ff:ff:ff:00:00 any rate-limit 32 16
(Routing)(Config-mac-ac ess-list)#exit
```

12-69 mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by name to an interface or range of interfaces, or associates it with a VLAN ID, in a given direction. The *name* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

An optional control-plane is specified to apply the MAC ACL on CPU port. The control packets like BPDU are also dropped because of the implicit deny all rule added to the end of the list. To overcome this, permit rules must be added to allow the control packets.

Note: The keyword **control-plane** is only available in Global Config mode.

Note: The availability of the **out** option is platform-dependent.

Use the **no** command to remove a MAC ACL identified by name from the interface in a given direction.

mac access-group name {{control-plane | in | out} vlan *vlan-id* **{in|out}} [sequence** *1-4294967295***]**

no mac access-group name {{ control-plane | in | out} vlan *vlan-id* **{in|out })**

Parameters

name	Enter a text string value to identify the access control list.
control-plane	Enter control-plane to apply the specified ACL on CPU port.
in	Enter the direction <in>.
out	Enter the direction <out>.
vlan *vlan-id*	Enter the VLAN ID for applying the ACL.
sequence *1-4294967295*	Enter the sequence number (greater than 0) to rank precedence for this interface and direction. A lower sequence number has higher precedence.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

12-70 remark

This command adds a new remark to the ACL rule.

Use the remark keyword to add comments (remarks) to ACL rule entries belonging to an IPv4, IPv6, MAC, or ARP ACL. Up to L7_ACL_MAX_RULES_PER_LIST*10 remarks per ACL and up to 10 remarks per ACL rule can be configured. Also, up to L7_ACL_MAX_RULES*2 remarks for all QOS ACLs(lPv4/IPv6/MAC) for device can be configured. The total length of the remark cannot exceed 100 characters. A remark can contain characters in the range A-Z, a-z, 0-9, and special characters like space, hyphen, underscore. Remarks are associated to the ACL rule that is immediately created after the remarks are created. If the ACL rule is removed, the associated remarks are also deleted. Remarks are shown only in **show running-config** and are not displayed in **show ip access-lists**.

Remarks can only be added before creating the rule. If a user creates up to 10 remarks, each of them is linked to the next created rule.

Use the **no** command remove a remark from an ACL access-list.

When the first occurrence of the remark in ACL is found, the remark is deleted. Repeated execution of this command with the same remark removes the remark from the next ACL rule that has the remark associated with it (if there is any rule configured with the same remark). If there are no more rules with this remark, an error message is displayed.

If there is no such remark associated with any rule and such remark is among not associated remarks, it is removed.

remark *remark*

no remark *remark*

Parameters

remark	Enter remark string.

Default

The default is None.

Command Mode

- IPv4-Access-List Config
- lPv6-Access-List-Config
- MAC-Access-List Config
- ARP-Access-List Config

Example

The following shows an example of the command.

```
(Config)#arp access-list new
(Config-arp-access-list)#remark "test1"
(Config-arp-access-list)#permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
(Config-arp-access-list)#remark "test1"
(Config-arp-access-list)#remark "test2"
(Config-arp-access-list)#remark "test3"
(Config-arp-access-list)#permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
```

```
(Config-arp-access-list)#permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
(Config-arp-access-list)#remark "test4"
(Config-arp-access-list)#remark "test5"
(Config-arp-access-list)#permit: ip host 2.1.1.3 mac host 00:03:04:05:06:01
```

12-71 show mac access-lists

This command displays summawy information for all Mac Access lists and ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented (for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, If an ACL rule is configured without RATE-LIMIT, the counter value is count of fonlvarded/discarded packets. (For example: For a burst of 100 packets, the Counter value is 100).

If the ACL rule is configured with RATE LIMIT, the counter value is the MATCHED packet count. If the sent traffic rate exceeds the configured limit, the counters still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) which would equal the sent rate. For example, if rate limit is set to 10 kbps and 'matching' traffic is sent at 100 kbps, counters reflect a 100 kbps value. If the sent traffic rate is less than the configured limit, counters display only the matched packet count. Either way, only the matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

Use the access list name to display detailed information of a specific MAC ACL.

Note: The command output varies based on the match criteria configured within the rules of an ACL.

show mac access-lists [*name***]**

Parameters

name	(Optional) Enter access-list name up to 31 characters in length.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show mac access-lists mac1

ACL Name: mac1

Outbound Interface(s): control-plane

Sequence Number: 10
Action..................................... permit
```

```
Source MAC Address.............................. 00:00:00:00:AA:BB
Source MAC Mask................................. FF:FF:FF:FF:00:00
Committed Rate.................................. 32
Committed Burst Size............................ 16
ACL hit count................................... 0

Sequence Number: 25
Action.......................................... permit
Source MAC Address.............................. 00:00:00:00:AA:BB
Source MAC Mask................................. FF:FF:FF:FF:00:00
Destination MAC Address......................... 01:80:C2:00:00:00
Destination MAC Mask............................ 00:00:00:FF:FF:FF
Ethertype....................................... ipv6
VLAN............................................ 36
CoS Value....................................... 7
Assign Queue.................................... 4
Redirect Interface.............................. 0/34
Committed Rate.................................. 32
Committed Burst Size............................ 16
ACL Hit Count................................... 0
```

Display Parameters

Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Source MAC Mask	The source MAC mask for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst	The committed burst size defined by the rate-limit attribute.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The unit/slot/port to which packets matching this rule are copied.
Redirect Interface	Slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the MAC ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the MAC ACL rule.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

IP Access Control List Commands

This section describes the commands you use to configure IP Access Control List (ACL) settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- D-LINK OS software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IPACL is hardware dependent.
- If an MAC ACL is configured on an interface, you cannot configure an IP ACL on the same interface.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A1 in a bit position of the ACL mask indicates the corresponding bit can be ignored.

12-72 access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs.

Note: IPv4 extended ACLs have the following limitations for egress ACLs:

- Match on port ranges is not supported.
- The rate-limit command is not supported.

Use the **no** command to delete an IP ACL that is identified by the parameter accesslistnumber from the system. The range for accesslistnumber 1-99 for standard access lists and 100-199 for extended access lists.

IP Standard ACL:

access-list *1-99* **{remark** *comment***} | {[***sequence-number***]} [rule** *1-1023***] {deny | permit} {every |** *srcip srcmask***} [log] [time-range** *time-range-name***][assign-queue** *queue-id***] [{mirror | redirect}** *slot/port***] [redirectExtAgent** *agent-id***] [rate-limit** *rate burst-size***]**

IP Extended ACL:

access-list 100-199 { remark *comment***} | {[***sequence-number***]} [rule** *1-1023***] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp |** *0-255***} {***srcip srcmask* **| any | host** *srcip***} [range {***portkey* **|** *startport***} {***portkey* **|** *endport***} {eq | neq | lt | gt} {***portkey* **|** *0-65535***} {***dstip dstmask* **| any | host** *dstip***}[{range {***portkey* **|** *startport***} {***portkey* **|** *endport***} | {eq | neq | lt | gt} {***portkey* **|** *0-65535***}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type** *icmp-type* **[icmp-code** *icmp-code***] | icmp-message** *icmp-message***] [igmp-type** *igmp-type***] [fragments] [precedence** *precedence* **| tos** *tos* **[tosmask] | dscp** *dscp***]}} [time-range** *time-range-name***] [log] [assign-queue** *queue-id***] [{mirror | redirect}** *slot/port***] [rate-limit** *rate burst-size***]**

no access-list *accesslistnumber* **[rule** *1-1023***]**

Parameters

remark *comment*	Use the remark keyword to add a comment (remark) to an IP standard or IP extended ACL. The remarks make the ACL easier to understand and scan. Each remark is limited to 100 characters. A remark can consist of characters in the range A-Z, a-z, 0-9, and special characters: space, hyphen, underscore. Remarks are displayed only in show running configuration. One remark per rule can be added for IP standard or IP extended ACL. User can remove only remarks that are not associated with a rule. Remarks associated with a rule are removed when the rule is removed.
sequence-number	(Optional) Specifies a sequence number for the ACL rule. Every rule receives a sequence number. A sequence number is specified by the user or is generated by the device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in the ACL is used and this rule is locate in the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. It is not allowed to create a rule that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule. For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, user can move the ACL rule to a different position in the ACL.
1-99 or *100-199*	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
rule *1-1023*	(Optional) Specifies the IP access list rule.
deny | permit	Specifies whether the IP ACL rule permits or denies an action. **Note:** For 5630x and 5650x-based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.
every	Match every packet.
eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0-255*	Specifies the protocol to filter for an extended IP ACL rule.
srcip srcmask **| any | host** *srcip*	Specifies a source IP address and source netmask for match condition of the IP ACL rule. Specifying any specifies srcip as 0.0.0.0 and srcmask as 255.255.255.255. Specifying host A.B.C.D specifies srcip as A.B.C.D and srcmask as 0.0.0.0.
range {*portkey* **|** *startport***}** **{***portkey* **|** *endtport***} {eq | neq | lt | gt} {***portkey* **|** *0-65535***}**	**Note:** This option is available only if the protocol is TCP or UDP. Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the *portkey*, which can be one of the following keywords: • For TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3.

	• For UDP: domain, echo, ntp, rip, snmp, tftp, time, and who. For both TCP and UDP, each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range. If **range** is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified portrange. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When **eq** is specified, the IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When **neq** is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. When **lt** is s specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number — 1>. When **gt** specified, the IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. Two rules are added in the hardware one with range equal to 0 to <specified port number _- 1> and one with range equal to <<specified port number_+ 1 to 65535>> **Note:** Port number matches only apply to unfragmented or first fragments.
dstip dstmask **| any | host** *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying dstip as 0.0.0.0 and dstmask as 255.255.255.255. Specifying host A.B.C.D implies dstip as A.B.C.D and dstmask as 0.0.0.0.
precedence *precedence* **| tos** *tos* **[***tosmask***] | dscp** *dscp*	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters dscp, precedence, tas/tasmask. **Note:** *tosmask* is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	**Note:** This option is available only if the protocol is tcp. Specifies that the IP ACL rule matches on the TCP flags. When +<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is set in the TCP header. When -<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is *NOT* set in the TCP header. When **established** is specified, a match occurs if the specified RST or ACK bits are set in the TCP header. Two rules are installed in the hardware when the established option is specified.
icmp-type *icmp-type* **[icmp-code** *icmp-code***] | icmp-message** *icmp-message*	**Note:** This option is available only if the protocol is icmp. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified,the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255.

	Specifying *icmp-message* implies that both icmp-type and icrnp-code are specified. The following icmp-messages are supported: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded and unreachable.
igmp-type *igmp-type*	This option is available only if the protocol is igmp. When *igmp-type* is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
fragments	Specifies that the IP ACL rule matches on fragmented IP packets.
Log	Specifies that this rule is to be logged.
time-range *time-range-name*	Allows imposing time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see “Time Range Commands for Time-Based ACLs”.
assign-queue *queue-id*	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
{mirror | redirect} *slot/port*	Specifies the mirror or redirect interface which is the *slot/port* to which packets matching this rule are copied or forwarded, respectively.
rate-limit *rate burst-size*	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

Default

The default is None.

Command Mode

Global Config

12-73 ip access-list

This command creates an extended IP Access Control List (ACL) identified by name, consisting of classification fields defined for the IP header of an IPv4 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

lf an lP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Note: The CLI mode changes to IPv4-Access-Lis Config mode when you successfully execute this command.

Use the **no** command to delete the IP ACL identified by name from the system.

ip access-list *name*

no ip access-list *name*

Parameters

name	Enter a text string to identify the access-list, up to 31 character length string.
rename	Renames the Access Control List.
resequence	Renumbers the ACL sequence numbers.

Default

The default is None.

Command Mode

Global Config

12-74 ip access-list rename

This command changes the name of an IP Access Control List (ACL). The *name* parameter is the names of an existing IP ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails is an IP ACL by the name *newname* already exists.

ip access-list rename *oldname newname*

Parameters

oldname	Enter the current access control list name.
newname	Enter a text string to identify the access-list, up to 31 character length string.

Default

The default is None.

Command Mode

Global Config

12-75 ip access-list resequence

Use this command to renumber the sequence numbers of the entries for specified IP access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

Note: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

ip access-list resequence {*name* **|** *id***}** *starting-sequence-number increment*

Parameters

id	Enter a numberical value for the ACL sequence number. The range is 1 – 199.
name	Enter a text string to identify the access-list, up to 31 character length string.
starting-sequence-number	The sequence number from which to start. The range is 1-2147483647. The default is 10.
increment	The amount to increment. The range is 1-2147483647. The default is 10.

Default

The default is 10.

Command Mode

Global Config

12-76 {deny | permit} (IP ACL)

This command creates a new rule for the current IP access list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Use the **no** command to remove the ACL rule with the specified sequence number from the ACL.

{deny | permit} {{every *[rule-id]* **[assign-queue <***queue-id***>]** [**log**] **[{mirror | redirect** *slot/port* **| port-channel** *port-channel-group-id***} | {redirectExtAgent** *agent-id***}] [rate-limit** *1-4294967295 1- 128***] [sequence** *1-2147483647***] [time-range** *name***]} | {{***0-255* **| icmpv6 | ipv6 | tcp | udp} {***sourceipv6-prefix/prefix-length* **| any | host** *ipv6 srcip***} [eq** *0-65535* **|** *portkey***] {***destination-ipv6- prefix/prefix-length* **| any | host** *ipv6 dstip***} [eq** *0-65535* **|** *portkey***] [flag [**+fin | -fin**] [**+syn | -syn**] [**+rst | -rst**] [**+psh | -psh**]** [+ack | -ack] [+urg | -urg] **[established]] [dscp** *value***] [flow-label** *vlaue***] [fragments] [routing] [rule-id] [assign-queue** *queue-id***] [log] [{{mirror | redirect}** *slot/port* **| port- channel** *port-channel-group-id***} | {redirectExtAgent** *agent-id***}] [rate-limit** *1-4294967295 1-128***] [sequence** *1-2147483647***] [time-range** name**] }}**

no *sequence-number*

Parameters

sequence-number	(Optional) The *sequence-number* specifies the sequence number for the ACL rule. The sequence number is specified by the user or is generated by device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed at the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. A rule cannot be created that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule. For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, the user can move the ACL rule to a different position in the ACL.
deny | permit	Specifies whether the IP ACL rule permits or denies the matching traffic.
0 -255 **| every | icmpv6 | ipv6 | tcp | udp**	Specifies the protocol to match for the IP ACL rule.
rule-id	Specifies a rule ID, the value range from 1 to 1023.
assign-queue	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned, the value range from 0 to 7.
log	Specifies that this rule is to be logged.
mirror | redirect *slot/port* | **port-channel** *port-channel-group-id*	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively.
redirectExtAgent *agent-id*	Allows matching flow packets to be sent to external applications running alongside D-LINK OS on a control CPU. agent-id is a unique identifier for the external receive client application, the value range from 1 to 100.
rate-limit *rate* | *burst-size*	Specifies the allowed rate of traffic as per the configured rate in kbps range from 1 to 4294967295, and burst-size in kbytes range from 1 to 128.
sequence *sequence-number*	Specifies a sequence number for the ACL rule. Every rule receives a sequence number. The sequence number is specified by the user or is generated by the device, the value range from 1 to 2147483647.
time-range *name*	Specifies a time limitation on the ACL rule as defined by the parameter time-range-name.
0-255	Specifies the protocol to match for the IPv6 ACL rule, the value range from 0 to 255.
source-ipv6-prefix/prefix-length	Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule.
destination-ipv6-prefix/prefix-length	Specifies a source IPv6 destination address and prefix length to match for the IPv6 ACL rule.
any	Specifying any implies specifying ::/0
host *ipv6 srcip*	Specifying host source-ipv6-address implies matching the specified IPv6 address.

host *ipv6 dstip*	Specifying host destination-ipv6-address implies matching the specified IPv6 address.
eq *0-65535* | *portkey*	Specifies the layer 4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0- 65535, or the portkey, which can be one of the following keywords: • For TCP: bgp | domain | echo | ftp | ftpdata | http | pop2 | pop3 | smtp | telnet | www.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IPv6 ACL rule matches on the tcp flags. When +<*tcpflagname*> is specified, a match occurs if specified *tcpflagname* flag is set in the TCP header. When -<*tcpflagname*> is specified, a match occurs if specified *tcpflagname* flag is not set in the TCP header. When established is specified, a match occurs if specified either RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when established option is specified. This option is visible only if protocol is TCP.
dscp	Match DSCP value.
flow-label	Match flow label field.
fragments	Match on non-initail fragmented packets.
Icp-message	Specify icmp-msg string.
icmp-type	Match icmp-type value.
routing	Match on presence of routing extention header.

Note: An implicit **deny all** IP rule always terminates the access list.

The **time-range** parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see “Time Range Commands for Time-Based ACLs”.

The **assign-queue** parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The **assign-queue** parameter is valid only for a **permit** rule.

The **permit** commands optional attribute **rate-limit** allows you to permit only the allowed rate of trafflc as per the configured rate in kbps, and burst-size in kbytes.

Default

The default is None.

Command Mode

lPv6-Access-List Config

12-77 ip access-group

This command either attaches a specific IP ACL identified by *accesslistnumber* to an interface (including VLAN routing interfaces), range of interfaces, or all interfaces; or associates it with a VLAN ID in a given direction. The parameter name is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

An optional control-plane is specified to apply the ACL on CPU port. The IPv4 control packets like RADIUS and TACACS+ are also dropped because of the implicit **deny all** rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv4 control packets.

Note: The keyword *control-plane* is only available in Global Config mode.

Note: The **out** option may or may not be available, depending on the platform.

Use the **no** command to remove a specified IP ACL from an interface.

ip access-group {*accesslistnumber* **|** *name***} { in | out} | vlan** *vlan-id* **{in | out}} [sequence** *1-4294967295***]**

no ip access-group {*accesslistnumber* **|** *name***} {{***control-plane* **| in | out} | vlan** *vlan-id* **{in | out}}**

Parameters

accesslistnumber	Enter the ACL ID in the range of 1 to 199.
name	Enter name of access control list
in	Enter the direction <in>.
out	Enter the direction <out>.
vlan *vlan-id*	Enter the VLAN ID, valid only in Global Config mode.
sequence *1-4294967295*	Enter the sequence number (greater than 0) to rank precedence for this interface and direction. A lower sequence number has higher precedence.

Default

The default is None.

Command Mode

- Interface Config
- Global Config

12-78 acl-trapflags

This command enables the ACL trap mode.

Use the **no** command to disable the ACL trap mode.

acl-trapflags

no acl-trapflags

Parameters

None

Default

The default is Disabled.

Command Mode

Global Config

12-79 show ip access-lists

Use this command to view summary information about all IP ACLs configured on the switch. To view more detailed information about a specific access list, specify the ACL number or name that is used to identify the IP ACL. For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented for example,consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, if an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/discarded packets (for example: If burst of 100 packets sent from IXIA, the Counter value is 100).

If an ACL rule is configured with RATE LIMIT, the counter value will be the MATCHED packet count. If the sent traffic rate exceeds the configured limit, counters will still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) that would equal the sent rate. For example, if rate limit is set to 10 kbps and ‘matching’ traffic is sent at 100 kbps, counters would reflect 100 kbps value. If the sent traffic rate is less than the configured limit, counters would display only matched packet count. Either way, only matched packet count is reflected in the counters, irrespective of whether they get dropped or fonivarded. ACL counters do not interact with diffserv policies.

show ip access-lists [*1-199* **|** *name***]**

Parameters

1-199	Displays the ACL ID used to identify a specific IP ACL.
name	Displays the ACL name used to identify a specific IP ACL.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ip access-lists ip1
```

```
ACL Name: ip1
Inbound Interface(s): 0/30

Sequence Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 1 (icmp)
ICMP Type.................................. 3 (Destination Unreachable)
Starting Source L4 port.................... 80
Ending Source L4 port...................... 85
Starting Destination L4 port............... 180
Ending Destination L4 port................. 185
ICMP Code.................................. 0
Fragments.................................. FALSE
Committed Rate............................. 32
Committed Burst Size....................... 16
ACL hit count.............................. 0
```

Display Parameters

ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).
red irectExtAgent	Indicates whether matching flow packets are allowed to be sent to external applications running alongside D-LINK OS on a control CPU. agent-id is a unique identifier for the external receive client application. agent-id is an integer in the range 1 to 100. The redirectExtAgent action is mutually exclusive with the redirect and mirror actions.

lf you specify an IP ACL number or name, the following information displays:
Note: Only the access list fields that you configure are displayed.

Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.

Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified lP Precedence.
IP TOS	The value specified for IP TOS.
Fragments	Specifies whether the IP ACL rule matches on fragmented IP packets is enabled.
TTL Field Value	The value specified for the TTL.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
redirectExtAgent	Indicates whether matching flow packets are allowed to be sent to external applications running alongside D-LINK OS on a control CPU. agent-id is a unique identifier for the external receive client application. agent-id is an integer in the range 1 to 100. The redirectExtAgent action is mutually exclusive with the redirect and mirror actions.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Rule Status	Status (Active/Inactive) of the IP ACL rule.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

12-80 show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction. Use the control-plane keyword to display the ACLs applied on the CPU port.

show access-lists interface {{*slot/port* **| lag** *lag-id***} in | out |** *control-plane***} | vlan** *vlan-id* **{in | out}**

Parameters

interface	Display access list information for a particular interface.
vlan	Enter the VLAN ID for showing bound ACLs.
vlan-id	Display access list information for a particular vlan ID.

slot/port	Enter an interface in slot/port format.
control-plane	Display access list information on management (CPU) port.
lag *lag-id*	Enter into interface lag mode.
lag-intf-num	Enter LAG interface number.
in	Display access list information for a particular interface and the in direction.
out	Display access list information for a particular interface and the out direction.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

ACL Type	Type of access list (IP, IPv6 or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).
in | out	• in – Display Access List information for a particular interface and the in direction. • out – Display Access List information for a particular interface and the out direction.

12-81 show access-lists vlan

This command displays Access List information for a particular VLAN ID.

show access-lists vlan *vlan-id* **{in | out}**

Parameters

vlan *vlan-id*	Display access list information for a particular vlan ID.

in	Display access list information for a particular vlan ID and the 'in' direction.
out	Display access list information for a particular vlan ID and the 'out' direction.

Default

The default is None.

Command Mode

Privileged EXEC

Display Parameters

	AVLAN ID.
in | out	• in – Display Access List information for a particular VLAN ID and the in direction. • out – Display Access List information for a particular VLAN ID and the out direction.

IPv6 Access Control List Commands

This section describes the commands you use to configure IPv6 Access Control List (ACL) settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet ll frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

12-82 ipv6 access-list

This command creates an IPv6 Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv6 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

Note: The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Use the **no** command to delete the IPv6 ACL identified by name from the system.

ipv6 access-list {rename [*oldname* | *newname***] | resequence**

no ipv6 access-list *name*

Parameters

rename *oldname* | *newname*	Rename an Access Control List.
resequence	Renumber ACL sequence numbers.

Default

The default is None.

Command Mode

Global Config

12-83 ipv6 access-list rename

This command changes the name of an IPv6 ACL. The *name* parameter is the name of an existing IPv6 ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name newname already exists.

ipv6 access-list rename *oldname newname*

Parameters

oldname	Enter the previously defined name.
newname	Enter an access-list name up to 31 characters in length.

Default

The default is None.

Command Mode

Global Config

12-84 ipv6 access-list resequence

Use this command to renumber the sequence numbers of the entries for specified IPv6 access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

Note: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

ipv6 access-list resequence {*name* **|** *id***}** *starting-sequence-number increment*

Parameters

name	Enter access-list name up to 31 characters in length.
starting-sequence-number	The sequence number from which to start. The range is 1—2147483647. The default is 10.
increment	The amount to increment. The range is 1—2147483647. The default is 10.

Default

The default is 10.

Command Mode

Global Config

12-85 {deny | permit} (IPv6)

This command creates a new rule for the current IPv6 access list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Use the **no** command to remove the ACL rule with the specified sequence number from the ACL.

{deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | *0-255***} {***source-ipv6-prefix/prefix-length* **| any | host** *source-tpv6-address***} [{range {***portkey* **|** *startport***} {***portkey* **|** *endport***} | {eq | neq | lt | gt) {***portkey* **|** *0-65535***}] {***destination-ipv6-prefix/prefix-length* **| any | host** *destination-ipv6-address***} [{range {***portkey* **|** *startport***} {***portkey* **|** *endport***} | {eq | neq | lt | gt} {**portkey | 0-65535**}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [flow-label** *value***] [icmp-type** *icmp-type* **[icmp-code** *icmp-code***] | icmp-message** *icmp-message***] [routing] [fragments] [sequence** *sequence-number***] [dscp** *dscp***]}} [log] [assign-queue** *queue-id***] [{mirror | redirect}** *unit/slot/port***] [rate-limit** *rate burst-size***]**

no *sequence-number*

Parameters

deny | permit	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.
every	Specifies to match every packet.
icmpv6 | ipv6 | tcp | udp | *0-255*	Specifies the protocol to match for the IPv6 ACL rule. The current list is: icmpv6, ipv6, tcp, and udp.
source-ipv6-prefix/prefix-length **| any | host** *source-ipv6-address*	Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying "::/0 " Specifying **host** *source-ipv6-address* implies matching the specified IPv6 address.

	This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
range {*portkey* **|** *startport***} {***portkey* **|** *endport***}	{eq	neq	lt	gt} {***portkey* **|** ***0-65535***}**	**Note:** This option is available only ifthe protocol is TCP or UDP. Specifies the layer 4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0-65535, or the portkey, which can be one of the following keywords: • For TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3 • For UDP: domain, echo, ntp, rip, snmp, tftp, time, who. Each of these keywords translates into its equivalent port number. When range is specified, IPv6 ACL rule matches only if the layer 4 port number falls within the specified poortrange. The startport and endpon parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between are part of the layer 4 port range. When **eq** is specified, IPv6 ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When **neq** is specified, IPv6 ACL rule matches only if the layer4 port number is not equal to the specified port number or portkey. When **lt** is specified, IPv6 ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number - 1>. When **gt** is specified, IPv6 ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. lt is equivalent to specifying the range as <specified port number + 1> to 65535. Two rules are added in the hardware one with range equal to 0 to <specified port number - 1> and one with range equal to <<specified port number +1 to 65535>>
destination-ipv6-prefix/prefih-length **	any	host** *destination-ipv6-address*	Specifies a destination IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying “::/0 “ Specifying host *destination-ipv6-address* implies matching the specified IPv6 address. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
sequence *sequence-number*	Specifies a sequence number for the ACL rule. Every rule receives a sequence number. The sequence number is specified by the user or is generated by the device. If a *sequence number* is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed at the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. It is not allowed to create a rule that duplicates an already existing one. A rule cannot be configured with a sequence number that is already used for another rule. For example, if a user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the

	sequence number, user can move the ACL rule to a different position in the ACL.
dscp *dscp*	Specifies the dscp value to match for for the IPv6 rule.
flag [+fin | -fin] [+syn | -syn] [+rst –rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IPv6 ACL rule matches on the tcp flags. When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header. When "-<tcpflagname>" is specified, a match occurs if specified <tcpflagname> flag is *NOT* set in the TCP header. When **established** is specified, a match occurs if specified either RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when "established" option is specified. This option is visible only if protocol is "top".
icmp-type *icmp-type* **[icmp-code** *icmp-code***] | icmp-message** *icmp-message*	**Note:** This option is available only if the protocol is icmpv6. Specifies a match condition for ICMP packets. When *icmp-type* is specified, IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, IPv6 ACL rule matches on the specified ICMP message code, a numberfrom 0 to 255. Specifying *icmp-message* implies both icmp-type and icmp-code are specified. The following icmp-messages are supported: destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mid-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, router-renumbering, time-exceeded, and unreachable. The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type.
fragments	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (packets that have the next header field set to 44).
routing	Specifies that IPv6 ACL rule matches on IPv6 packets that have the routing extension header (the next header field is set to 43).
log	Specifies that this rule is to be logged.
time- range *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with the specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
assign-queue *queue-id*	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
{mirror | redirect} *unit/slot/port*	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or fonlvarded, respectively.
rate-limit *rate burst-size*	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

Note: An implicit **deny all IPv6** rule always terminates the access list.

The **time-range** parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges. see “Time Range Commands for Time-Based ACLs”.

The **assign-queue** parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The **assign-queue** parameter is valid only for a **permit** rule.

The **permit** commands optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps. and burst-size in kbytes.

IPv6 ACLs have the following limitations:

- Port ranges are not supported for egress IPv6 ACLs.
- The lPv5 ACL routing keyword is not supported when an IPv6 address is specified.
- IPv6 ACL fragment keyword matches only on the first two IPv6 extension headers for the fragment header (next header code 44). If the fragment header appears in the third or subsequent header, it is not matched.
- IPv6 ACL fragment keyword matches only on the first IPv6 extension header (next header code 44). If the fragment header appears in the second or subsequent header, it is not matched.
- IPv6 ACL routing keyword matches only on the first IPv6 extension header (next header code 43). If the fragment header appears in the second or subsequent header, it is not matched.
- The rate-limit command not supported for egress IPv6 ACLs.

Default

The default is None.

Command Mode

IPv6-Access-List Config

Example

The following shows an example of the command.

```
(Routins)(Config)#ipv6 access-list ip61
(Routins)(Config-ipv6-acl)#per-mit udp any any rate-limit 32 16
(Routins)(Config-ipv6-acl)#exit
```

12-86 ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by name to an interface or range of interfaces, or associates it with a VLAN ID in a given direction. The name parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use forthis interface and direction, the specifiedlPv6 access list replaces the currently attached IPv6 access list using that sequence number. If

the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The vlan keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

An optional *control-plane* is specified to apply the ACL on CPU port. The IPv6 control packets like lGMPv6 are also dropped because of the implicit **deny all** rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv6 control packets.

Note: The keyword *control-plane* is only available in Global Config mode.

Note: You should be aware that the **out** option may or may not be available, depending on the platform.

Use the **no** command to remove an IPv6 ACL identified by name from the interface(s) in a given direction.

ipv6 traffic-filter name {{*control-plane* **| in | out} | vlan** *vlan-id* **{in | out}} [sequence** *1-4294967295***]**

no ipv6 traffic-filter name {{*control-plane* **| in | out} | vlan** *vlan-id* **{in | out}}**

Parameters

control-plane	Enter 'control-plane' to apply the specified ACL on CPU port.
in	Enter the direction <in>.
out	Enter the direction <out>.
vlan *vlan-id*	Enter the VLAN ID for applying the ACL.
sequence *1-4294967295*	Enter the sequence number (greater than 0) to rank precedence for this interface and direction. A lower equence number has higher precedence.

Default

The default is None.

Command Mode

- Global Config
- Interface Config

Example

The following shows an example of the command.

```
(Routing)(Config)#ipv6 traffic-filter ip61 control-plane
```

The following shows an example of the command.

```
(Routing)(ConFig)#no ipv6 traffic-filter ip61 control-plane
```

12-87 show ipv6 access-lists

This command displays summary information of all the IPv6 Access lists. Use the access list *name* to display detailed information of a specific IPv6 ACL.

This command displays information about the attributes icmp-type, icmp-code, fragments, routing, tcp flags, and source and destination L4 port ranges. It displays committed rate,committed burst size and ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented (for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, If an ACL rule is configured without RATE-LIMIT, the counter value is a count of the forwarded/discarded packets. (For example: for a burst of 100 packets, the Counter value is 100).

If an ACL rule is configured with RATE LIMIT, the counter value is that of the MATCHED packet count. If the sent traffic rate exceeds the configured limit, the counters still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) that equals the sent rate. For example, if the rate limit is set to 10 kbps and 'matching' traffic is sent at 100 kbps, counters would reflect 100 kbps value. If the sent traffic rate is less than the configured limit, the counters display only the matched packet count. Either way, only the matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

show ipv6 access-lists [*name***]**

Parameters

name	(Optional) Enter access-list name up to 31 characters in length.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show ipv6 access-lists ip61

ACL Name: ip61

Outbound Interface(s): control-plane

Rule Number: 1
Action..................................... permit
Match Every................................ FALSE
Protocol................................... 17 (udp)
Committed Rate............................. 32
Committed Burst Size....................... 16
ACL Hit Count.............................. 0
```

Display Parameters

Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IPv6 ACL rule has referenced a time range.
red irectExtAgent	Indicates whether matching flow packets are allowed to be sent to external applications running alongside D-LINK OS on a control CPU. agent-id is a unique identifier for the external receive client application. agent-id is an integer in the range 1 to 100. The redirectExtAgent action is mutually exclusive With the redirect and mirror actions.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

Management Access Control and Administration List

In order to ensure the security of the switch management features, the administrator may elect to configure a management access control list. The Management Access Control and Administration List (MACAL) feature is used to ensure that only known and trusted devices are allowed to remotely manage the switch via TCP/IP.

MACALs can be applied only to in-band ports and cannot be applied to the service port.

12-88 management access-list

Use this command to create a management access list and to enter access-list configuration mode, where you must define the denied or permitted access conditions with the deny and permit commands. If no match criteria are defined, the default is deny. If you reenter to an access-list context, the new rules would be entered at the end of the access-list. Use the **management access-class** command to choose the active access-list. The active management list cannot be updated or removed. The *name* value can be up to 32 characters.

Use the **no** command to delete the management ACAL identified by name from the system.

management access-list *name*

no management access-list *name*

Parameters

name	Enter access-list name up to 31 characters in length.

Default

The default is None.

Command Mode

Global Config

12-89 {deny | permit} (Management ACAL)

This command creates a new rule for the current management access control access list (ACAL). A rule may either deny or permit traffic according to the specified classification fields. Rules with **ethernet**, **vlan** and **port-channel** parameters will be valid only if an IP address is defined on the appropriate interface. Each rule should have a unique priority.

{deny | permit} [ethernet *interface-number* **| vlan** *vlan-id* **| port-channel** *number***] [service** *service***] [priority** *priority-value***]**

{deny | permit} ip-source *ip-address* **[mask** *mask* **|** *prefix-length***] [ethernet** *interface-number* **| vlan** *vlan-id* **| port-channel** *number***] [service** *service***] [priority** *priority-value***]**

Parameters

deny	Enter to specific traffic rule to deny.
permit	Enter to specific traffic rule to permit.
ip-source *ip-address*	Source IP address.
mask *mask*	(Optional) The network mask of the source IP address (0-32).
prefix-length	(Optional) The number of bits that comprise the source IP address

	prefix. prefix length must be preceded by a forward slash (/).
ethernet *interface-number*	(Optional) Ethernet port number.
vlan *vlan-id*	(Optional) VLAN number.
port-channel *number*	(Optional) Port-channel number.
service *service*	(Optional) Service type condition, which can be one of the following key words: • java • mp • telnet • ssh • http • https • snmp • sntp • any
priority *priority-value*	(Optional) Priority for rule.

Default

The default is None.

Command Mode

Management-ACAL Config

Example

The following example shows how to configure two management interfaces.

```
ethernet 0/1 and ethernet 0/9.
(Routing)(Config)#management access-list mlist
(Routing)(config-macal)#permit ethernet 0/1 priority 63
(Routing)(config-macal)#permit ethernet 0/9 priority 64
(Routing)(config-macal)#exit
(Routing)(Config)#management access-list mlist
```

The following example shows how to configure all the interfaces to be management interfaces except for two interfaces: ethernet 0/1 and ethernet 0/9

```
(Routing)(Config)#management access-list mlist
(Routing)(config-macal)#deny ethernet 0/1 priority 62
(Routing)(config-macal)#deny ethernet 0/9 priority 63
(Routing)(config-macal)#permit priority 64
(Routing)(config-macal)#exit
```

12-90 management access-class

Use this command to restrict management connections. The **console-only** keyword specifies that the device can be managed only from the console.

Use the **no** command to disable the management restrictions.

management accesss-class {console-only | *name***}**

no management access-class

Parameters

name	Specify the name of the access list.
console-only	Allow management through console only.

Default

The default is None.

Command Mode

Global Config

12-91 show management access-list

This command displays management access-lists.

show management access-list [*listname***]**

Parameters

listname	(Optional) Specify the name of the access list.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show management access-list

List Name..................................... mlist
List Admin Mode............................... Disabled
Packets Filtered.............................. 0

Rules:
permit ethernet 0/1 priority 63
permit ethernet 0/9 priority 64
```

```
Note: All other access is implicitly denied.
```

Display Parameters

List Name	Displays the name of the access list.
List Admin Mode	Displays the admin mode status (disabled/enabled) of the list.
Packets Filtered	Displays the number of filtered packets through the rule.

12-92 show management access-class

This command displays information about the active management access list.

show management access-class [*name***]**

Parameters

name	(Optional) Displays the name of the access list. If unspecified, defaults to an empty Access-List. (Range: 1 - 32characters)

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following shows example CLI display output for the command.

```
(Routing)#show management access-class

Management access-class is enabled, using access list mlist
```

Time Range Commands for Time-Based ACLs

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit deny all rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined with in an ACL.

12-93 time-range

Use this command to create a time range identified by name, consisting of one absolute time entry and/or one or more periodic time entries. The *name* parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries.

Note: When you successfully execute this command, ode changes to Time-Range Config mode.

Use the **no** command to delete a time-range identified by name.

time-range *name*

no time-range *name*

Parameters

name	Enter time-range name up to 31 characters in length.

Default

The default is None.

Command Mode

Global Config

12-94 absolute

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The *time* parameter is based on the currently configured time zone.

The **[***start time date***]** parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is} in effect immediately.

The **[***end time date***]** parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Use the **no** command to delete the absolute time entry in the time range.

absolute {[*start time date***] [***end time date***]}**

no absolute

Parameters

start time date	(Optional) Configure the starting time range entry parameter.
end time date	(Optional) Configure the ending time range entry parameter.

Default

The default is None.

Command Mode

Time-Range Config

12-95 periodic

Use this command to add a periodic time entry to a time range. The *time* parameter is based off of the currently configured time zone.

The first occurrence of the *days-of-the-week* argument is the starting day(s) from which the configuration that referenced the time range starts going into ettect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily – Monday through Sunday
- weekdays – Monday through Friday
- weekend – Saturday and Sunday

lf the ending days of the week are the same as the starting days of the week, they can be omitted.

The first occurrence of the time argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hourszminutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Use the **no** command to delete a periodic time entry from a time range.

periodic {*daily* | *end* | *monthly* | *start* | *weekdays* | *weekend***}{***days-of-the-week time***} to {[***days-of-the-week***]** *time***}**

no periodic {*days-of-the-week time***} to {[***days-of-the-week***]** *time***}**

Parameters

frequency	Define how often this periodic entry will be active. If the value is set to 0, the option will be disabled. The possible value is from 0 to 255
days-of-the-week	(Optional) Configure to select a day of the week.
daily	Every day of the week.
end	Configure absolute time range entry's end time.
monthly	Monthly on the specified day.
start	Configure absolute time range entry's start time.
weekdays	Monday through Friday.
weekend	Saturday and Sunday.

Default

The default is None.

Command Mode

Time-Range Config

12-96 show time-range

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range.

show time-range

Parameters

None.

Default

The default is None.

Command Mode

Privileged EXEC

Example

The following is an example of the CLI display output for the command.

```
(Routing #show time-range

Admin mode: Disabled
Current number of all Time Ranges: 1
Maximum number of all Time Ranges: 100

                                          Periodic
Time Range Name                 Status    Entry count Absolute Entry
------------------------------- --------- ----------- --------------
absolute                        Active        0       Does not exist
```

Display Parameters

Admin Mode	Status of the mode: disabled (default) / enabled.
Current Number of Time Ranges	Number of current time ranges configured in the system.
Maximum number of all time ranges	Number of time ranges configured in the system.

Time Range Name	Name of the time range.
Time Range Status	Status of the time range (active/inactive).
Absolute start	Start time and day for absolute time entry.
Absolute end	End time and day for absolute time entry.
Periodic Entries	Number of periodic entries in a time-range.
Periodic start	Start time and day for periodic entry.
Periodic end	End time and day for periodic entry.

13. D-LINK OS Log Messages

This section lists common log messages that are provided by D-LINK OS, 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 D-LINK 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 15: BSP Log Messages

Component	Message	Cause
BSP	Event (0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting D-LINK OS application.

Table 16: 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.
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An eventwas 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.

Component	Message	Cause
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 17: 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 18: System Log Messages

Component	Message	Cause
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.
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.

Utilities

Table 19: Trap Mgr Log Message

Component	Message	Cause

Component	Message	Cause
Trap Mgr	Link Up/Down: slot/port	An interface changed link state.

Table 20: 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 21: 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 components 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 22: RADIUS Log Messages

Component	Message	Cause
RADIUS	RADIUS: Invalid data length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.

Component	Message	Cause
RADIUS	RADIUS: Could not allocate accounting requestlnfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestlnfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Access-Challenge failed to validate, ID = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, ID = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Access-Accept failed to validate, ID = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, ID = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	The RADIUS Client received a server response from an unconfigured server.

Table 23: TACACS+ Log Messages

Component	Message	Cause
TACACS+	TACACS+: Authentication error, no server to contact	TACACS+ request needed, but no servers are configured.
TACACS+	TACACS+: Connectoni failed to server x.x.x.x	TACACS+ request sent to server x.x.x.x but no response was received.
TACACS+	TACACS+: No key configured to encrypt packet for server x.x.x.x	No key configured for the specified server.
TACACS+	TACACS+: Received invalid packet type from server.	Received packet type that is not supported.
TACACS+	TACACS+: Invalid major version in received packet.	Major version mismatch.
TACACS+	TACACS+: Invalid minor version in received packet.	Minor version mismatch.

Table 24: LLDP Log Message

Component	Message	Cause
LLDP	IIdpTask(): Invalid message type:xx.xxxxxx:xx	Unsupported LLDP packet received.

Table 25: 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 26: 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.

Table 27: DHCPv6 Client Log Messages

Component	Message	Cause
DHCP6 Client	ip6Map dhcp add failed	This message appears when the update of a DHCP leased IP address to lP6Map fails.
DHCP6 Client	osapiNetAddrV6Add failed on interface xxx	This message appears when the update of a DHCP leased IP address to the kernel IP Stack fails.
DHCP6 Client	Failed to add DNS Server xxx to DNS Client	This message appears when the update of a DNS6 Server address given by the DHCPv6 Server to the DNS6 Client fails.
DHCP6 Client	Failed to add Domain name xxx to DNS Client	This message appears when the update of a DNS6 Domain name info given by the

Component	Message	Cause
		DHCPv6 Server to the DNS6 Client fails.

Management

Table 28: SNMP Log Message

Component	Message	Cause
SNMP	EDB Callback: Unit Join: x	A new unit has joined the stack.

Table 29: 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 30: 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 31: 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 Ul 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 sshdlssueCmd.	Failed to send the message to the SSHD message queue.

Table 32: 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 Ul event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltlssueCmd.	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 33: 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 34: Protected Ports Log Messages

Component	Message	Cause
Protected Ports	Protected Port: failed to save configuration	This appears when the protected port configuration cannot be saved.
Protected Ports	protectedPortCnfgrlnitPhase1 Process: Unable to create r/w lock for protected Port	This appears when protectedPortCfgRWLock Fails.
Protected Ports	protectedPortCnfgrlnitPhase2 Process: Unable to register for VLAN change callback	This appears when nimRegisterIntfChange with VLAN fails.
Protected Ports	Cannot add interface xxx to group yyy	This appears when an interface could not be added to a particular group.
Protected Ports	Unable to set protected port group	This appears when a dtl call fails to add interface mask at the driver level.
Protected Ports	Cannot delete interface xxx from group yyy	This appears when a dtl call to delete an interface from a group fails.
Protected Ports	Cannot update group YYY after deleting interface XXX	This message appears when an update group for a interface deletion fails.
Protected Ports	Received an interface change callback while not ready to receive it	This appears when an interface change call back has come before the protected port component is ready.

Table 35: 802.1X Log Messages

Component	Message	Cause
802.1X	*function*: Failed calling dot1xlssueCmd	802.1X message queue is full.
802.1X	*function*: EAP message not received from server	RADIUS server did not send required EAP message.

Component	Message	Cause
802.1X	*function*: Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers.
802.1X	*function*: could not set state to *authorized/unauthorized* intf xxx	DTL call failed setting authorization state of the port.
802.1X	dot1xApplyConfigData: Unable to *enable/disable* dot1x in driver	DTL call failed enabling/disabling 802.1X.
802.1X	dothSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server.
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, iflndex = xxx	Failed sending accounting start to RADIUS server.
802.1X	function: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server.

Table 36: IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	*function*: osapiMessageSend failed	IGMP Snooping message queue is full.
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Failed to set global IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Failed to set interface IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Failed to set interface multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for VLAN yyy	Failed to set VLAN IGM Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode %d for interface xxx on VLAN yyy	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	snoopCnfgrlnitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets.
IGMP Snooping	snoopCnfgrlnitPhase1 Process Error allocating large buffers	Could not allocate buffers for large IGMP packets.

Table 37: 802.3ad Log Messages

Component	Message	Cause
8U2.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU.

Component	Message	Cause
802.3ad	dot3adNimEventCompletionCaIIback, dot3adNimEventCreateCompletion Callback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully.

Table 38: 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 39: Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantaglntflsConfigurable: 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 40: IPv6 Provisioning Log Message

Component	Message	Cause
IPv6 Provisioning	ipv6ProvlntflsConfigurable: Error accessing IPv6 Provisioning 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 preconflguration.

Table 41: MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

Table 42: 802. 1Q Log Messages

Component	Message	Cause
802.1Q	dot1qlssueCmd: Unabie 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 range	This accommodates for reserved vlan ids. i.e. 4094 - x.
802.1Q	dot1qMaplntflsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMaplntflsConfigurable.	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 – pottMask = %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.

Component	Message	Cause
8U2.1Q	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 ently 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.
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.

Component	Message	Cause
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 Undgr 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	Requester %d attempted to releasegnal VLAN %d: owned by %d	Request to release the VLAN ID.

Table 43: 802.1S Log Messages

Component	Message	Cause
802.1S	d0t1slssueCmd: Dot1s Msg Queue is fuIll!!! 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 44: Port MAC Locking Log Message

Component	Message	Cause
Port MAC Locking	pmlMaplntflsConfigurable: Error	A default configuration does not exist for

Component	Message	Cause
	accessing PML config data for interface %d in pmlMaplntflsConfigurable.	this interface. Typically a case when a new interface is created and has no preconfiguration.

QoS

Table 45: 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.

Table 46: CoS Log Message

Component	Message	Cause
COS	cosCnfgrlhitPhase3Process: Unable to apply saved config – using factory defaults	The COS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 47: DiffServ Log Messages

Component	Message	Cause
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	While attempting to clear the running configuration an error was encountered in removing the current settings. This may lead to an inconsistent state in the system and resetting is advised.

Component	Message	Cause
DiffServ	Policy invalid for service intf: policy *name*, interface *x*, direction *y*	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

Routing/IPv6 Routing

Table 48: 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 49: OSPFv2 Log Messages

Component	Message	Cause
OSPFv2	Best route client deregistration failed for OSPF Redist	OSPFv2 registers with the lPv4 routing table manager ("RTO") to be notified of best route changes. There are cases where OSPFv2 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv2	XX_Call() failure in _checkTimers for thread 0x869bcc0	An OSPFv2 timer has fired but the message queue that holds the event has filled up. This is normally a fatal error.

Component	Message	Cause
OSPFv2	Warning: OSPF LSDB is 90% full (22648 LSAs)	OSPFv2 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv2 logs this warning. The warning includes the current size of the database.
OSPFv2	The number of LSAs, 25165, in the OSPF LSDB has exceeded the LSDB memory allocation	When the OSPFv2 LSDB becomes full, OSPFv2 logs this message. OSPFv2 reoriginates its router LSAs with the metric of all non-stub links set to the maximum value to encourage other routers to not compute routes through the overloaded router.
OSPFv2	Dropping the DD packet because of MTU mismatch	OSPFv2 ignored a Database Description packet whose MTU is greater than the IP MTU on the interface where the DD was received.
OSPFv2	LSA Checksum error in LsUpdate. dropping LSID 1.2.3.4 checksum 0x1234	OSPFv2 ignored a received link state advertisement (LSA) whose checksum was incorrect.

Table 50: OSPFv3 Log Messages

Component	Message	Cause
OSPFv3	Best route client deregistration failed for OSPFv3 Redist	OSPFv3 registers with the lPv6 routing table manager (“RTO6”) to be notified of best route changes. There are cases where OSPFv3 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv3	Warning: OSPF LSDB is 90% full (15292 LSAs).	OSPFv3 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv3 logs this warning. The warning includes the current size of the database.
OSPFv3	The number of LSAs, 16992, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv3 LSDB becomes full, OSPFv3 logs this message. OSPFv3 reoriginates its router LSAs with the R-bit clear indicating that OSPFv3 is overloaded.
OSPFV3	LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.	OSPFv3 periodically verifies the checksum of each LSA in memory. OSPFv3 logs this.

Table 51: Routing Table Manager Log Messages

Component	Message	Cause
RTO	RTO is no longer full. Routing table contains xxx best routes, xxx total routes, reserved local routes.	When the number of best routes drops below full capacity, RTO logs this notice. The number of bad adds may give an indication of the number of route adds that failed while RTO was full, but a full routing table is only one reason why this count is incremented.
RTO	RTO is full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes. The routing table manager stores a limited number of best routes. The count of total routes includes alternate routes, which are not installed in hardware.	The routing table manager, also called “RTO”, stores a limited number of best routes, based on hardware capacity. When the routing table becomes full, RTO logs this alert. The count of total routes includes alternate routes, which are not installed in hardware.

Table 52: VRRP Log Messages

Component	Message	Cause
VRRP	VRRP packet of size xxx dropped. Min VRRP packet size is xxx; Max VRRP packet size is xxx.	This message appears when there is flood of VRRP messages in the network.
VRRP	VR xxx on interface xxx started as xxx.	This message appears when the Virtual router is started in the role of a Master or a Backup.
VRRP	This router is the IP address owner for virtual router xxx on interface xxx. Setting the virtual router priority to xxx.	This message appears when the address ownership status for a specific VR is updated. If this router is the address owner for the VR, set the VR's priority to MAX priority (as per RFC 3768). If the router is no longer the address owner, revert the priority.

Table 53: 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.

Multicast

Table 54: IGMP/MLD Log Messages

Component	Message	Cause
IGMP/MLD	MGMD Protocol Heap Memory lnit Failed; Family – XXX.	MGMD Heap memory initialization Failed for the specified address family. his message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD Protocol Heap Memory De-lnit Failed; Family – xxx.	MGMD Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable MGMD (IGMP/MLD) Protocol. As a result of this, the subsequent attempts to enable/ disable MGMD will also fail.
IGMP/MLD	MGMD Protocol Initialization Failed; Family – xxx.	MGMD protocol initialization sequence Failed. This could be due to the nonavailability of some resources. This message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD All Routers Address - xxx Set to the DTL Mcast List Failed; Mode – xxx, intf – xxx.	This message appears when trying to enable/disable MGMD Protocol.
IGMP/MLD	MGMD All Routers Address – xxx Add to the DTL Mcast List Failed.	MGMD All Routers Address addition to the local multicast list Failed. As a result of this, MGMD Multicast packets with this address will not be received at the application.
IGMP/MLD	MGMD All Routers Address – xxx Delete from the DTL Mcast List Failed.	MGMD All Routers Address deletion from the local multicast list Failed. As a result of this, MGMD Multicast packets are still received at the application though MGMD is disabled.
IGMP/MLD	MLDv2 GroupAddr-[FF02::16] Enable with lnterpeak Stack Failed; rtrlfNum – xxx, int f – xxx.	Registration of this Group address with the lnterpeak stack failed. As a result of this, MLDv2 packets will not be received at the application.
IGMP/MLD	MGMD Group Entry Creation Failed; grpAddr – xxx, rtrlfNum – xxx.	The specified Group Address registration on the specified router interface failed.
IGMP/MLD	MGMD Socket Creation/Initialization Failed for addrFamily – xxx.	MGMD Socket Creation/options Set Failed. As a result of this, the MGMD Control packets cannot be sent out on an interface.

Table 55: IGMP-Proxy Log Messages

Component	Message	Cause
IGMP-Proxy/MLD-Proxy	MGMD-Proxy Protocol Initialization Failed; Family – xxx.	MGMD-Proxy protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable MGMD-Proxy Protocol.
IGMP-Proxy/MLD-Proxy	MGMD-Proxy Protocol Heap Memory De-lnit Failed; Family – xxx.	MGMD-Proxy Heap memory de-initialization is Failed forthe specified address family. This message appears when trying to disable MGMD-Proxy Protocol. As a result of this, the subsequent attempts to enable/disable MGMD-Proxy will also fail.
IGMP-Proxy/MLD-Proxy	MGMD Proxy Route Entry Creation Failed; grpAddr – xxx, srcAddr – xxx, rtrlfNum – xxx.	Registration of the Multicast Forwarding entry for the specified Source and Group Address Failed when MGMD-Proxy is used.

Table 56: PIM-SM Log Messages

Component	Message	Cause
PIMSM	Non-Zero SPT/Data Threshold Rate – xxx is currently Not Supported on this platform.	This message appears when the user tries to configure the PIMSM SPT threshold value.
PIMSM	PIMSM Protocol Heap Memory lnit Failed; Family – xxx.	PIMSM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMSM Protocol.
PIMSM	PIMSM Protocol Heap Memory De-lnit Failed; Family – xxx.	PIMSM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMSM Protocol. As a result of this, the subsequent attempts to enable/disable PIMSM will also fail.
PIMSM	PIMSM Protocol Initialization Failed; Family – xxx.	PIMSM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMSM Protocol.
PIMSM	PIMSM Protocol De-lnitialization Failed; Family – xxx.	PIMSM protocol de-initialization sequence Failed. This message appears when trying to disable PIMSM Protocol.
PIMSM	PIMSM SSM Range Table is Full	PIMSM SSM Range Table is Full. This message appears when the protocol cannot accommodate new SSM registrations.

Component	Message	Cause
PIMSM	PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.
PIMSM	PIM All Routers Address – xxx Add to the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.
PIMSM	Mcast Forwarding Mode Disable Failed for intf – xxx.	Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.
PIMSM	Mcast Forwarding Mode Enable Failed for intf – xxx.	Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.
PIMSM	PIMSMv6 Socket Memb‘ship Enable Failed for rtrlfNum – xxx.	PIMSMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result ofthis, the PIM Control packets cannot be received on the interface.
PIMSM	PIMSMv6 Socket Memb'ship Disable Failed for rtrlfNum – xxx.	PIMSMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIM Control packets are still received on the interface at the application though no protocol is enabled.
PIMSM	PIMSM (S, G, RPt) Table Max Limit – xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (S, G, RPt) has reached maximum capacity and cannot accommodate new registrations anymore.
PIMSM	PIMSM (S, G) Table Max Limit – xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (S, G) has reached maximum capacity and cannot accommodate new registrations anymore.
PIMSM	PIMSM (*, G) Table Max Limit – xxx Reached; Cannot accommodate any further routes	PIMSM Multicast Route table (*, G) has reached maximum capacity and cannot accommodate new registrations anymore.

Table 57: PIM-DM Log Messages

Component	Message	Cause
PIMDM	PIMDM Protocol Heap Memory Init Failed; Family – xxx.	PIMDM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMDM Protocol.
PIMDM	PIMDM Protocol Heap Memory De-init Failed; Family – xxx.	PIMDM Heap memow de-initialization Failed for the specified address family. This message appears when trying to disable PIMDM Protocol. As a result of this, the subsequent attempts to enable/disable

Component	Message	Cause
		PIMDM will also fail.
PIMDM	PIMDM Protocol Initialization Failed; Family – xxx.	PIMDM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMDM Protocol.
PIMDM	PIMDM Protocol De-Initialization Failed; Family – xxx.	PIMDM protocol de-initialization sequence Failed. This message appears when trying to disable PIMDM Protocol.
PIMDM	PIM All Routers Address – xxx Delete from The DTL Mcast List Failed for intf – xxx.	PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.
PIMDM	PIM All Routers Address – xxx Add to the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.
PIMDM	Mcast Forwarding Mode Disable Failed for intf – xxx.	Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.
PIMDM	Mcast Forwarding Mode Enable Failed for intf – xxx	Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.
PIMDM	PlMDMv6 Socket Memb'ship Enable Failed for rtrlfNum – xxx.	PlMDMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.
PIMDM	PIMDMv6 Socket Memb'ship Disable Failed for rtrlfNum – xxx.	PlMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result ofthis, the PIM Control packets are still received on the interface at the application though no protocol is enabled.
PIMDM	PIMDM FSM Action Invoke Failed; rtrlfNum – xxx Out of Bounds for Event – xxx.	The PIMDM FSM Action invocation Failed due to invalid Routing interface number. in such cases, the FSM Action routine can never be invoked which may result in abnormal behavior. The failed FSM-name can be identified from the specified Event name.
PIMDM	PIMDM Socket initialization Failed for addrFamily – xxx.	PIMDM Socket Creation/options Set Failed. As a result of this, the PIM Control packets cannot be sent out on an interface.
PIMDM	PIMDMv6 Socket Memb'ship Enable Failed for rtrlfNum – xxx.	Socket options Set to enable the reception of PlMv6 packets Failed. As a result of this, the PlMv6 packets will not be received by the application.

Component	Message	Cause
PIMDM	PIMDMv6 Socket Memb'ship Disable Failed for rtrlfNum – xxx	PIMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIMv6 Control packets are still received on the interface at the application though no protocol is enabled.
PIMDM	PIMDM MRT Table Max Limit – xxx Reached; cannot accommodate any further routes.	PIMDM Multicast Route table (S, G) has reached maximum capacity and cannot accommodate new registrations anymore.

Table 58: DVMRP Log Messages

Component	Message	Cause
DVMRP	DVMRP Heap memory initialization is Failed for the specified address family	This message appears when trying to enable DVMRP Protocol
DVMRP	DVMRP Heap memory de-initialization is Failed for the specified address family.	This message appears when trying to disable DVMRP Protocol. As a result of this, the subsequent attempts to enable/disable DVMRP will also fail.
DVMRP	DVMRP protocol initialization sequence Failed.	This could be due to the non-availability of some resources. This message appears when trying to enable DVMRP Protocol.
DVMRP	DVMRP All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.	DMVRP All Routers Address deletion from the local multicast list Failed. As a result of this, DVMRP Multicast packets are still received at the application though DVMRP is disabled.
DVMRP	Mcast Forwarding Mode Disable Failed for intf – xxx.	The Multicast Forwarding mode Disable Failed for this routing interface.
DVMRP	DVMRP All Routers Address – xxx Add to the DTL Mcast List Failed for intf – xxx.	DMVRP All Routers Address addition to the local multicast list Failed. As a result of this, DVMRP Multicast packets with this address will not be received at the application.
DVMRP	Mcast Fon/varding Mode Enable Failed forintf – xxx.	The Multicast Forwarding mode Enable Failed for thi r ing interface. As a result of this, the ability to forward Multicast packets does not function on this interface.
DVMRP	DVMRP Probe Control message Send Failed on rtrlfNum – xxx.	DVMRP Probe control message send failed. This couId mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.

Component	Message	Cause
DVMRP	DVMRP Prune Control message Send Failed; rtrlfNum – xxx.	Neighbor - %s, SrcAddr - %s, GrpAddr - %s DVMRP Prune control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the unwanted multicast traffic is still received and forwarded.
DVMRP	DVMRP Probe Control message Send Failed on rtrlfNum – xxx.	DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.

Technologies

Table 59: Error Messages

Message	Cause
invalid USP unit = x, slot = x, port = x	A port was not able to be translated correctly during the receive.
in hapiBroadSystemMacAddress call to '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.
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.
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.
ERROR: policy x, tmpPolicy x, size x, data x x x x x x x	An issue installing the policy due to a possible dupliate hash.
ACL x not found in internal table	Attempting to delete a non-existent ACL.
ACL internal table overflow	Attempting to add an ACL to a full table.
In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it's capabilities.
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.
USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.
usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.
USL: No available entries in the	The Spanning Tree Group table is full in USL.

Message	Cause
STG table	
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.
USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn't exist.
USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
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.
USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
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 retw will be issued.
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.
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.
invalid LAG ID X	Possible synchronization issue between the BCM driver and HAPI.
invalid uport calculated from the uport x_l2_addr->lport = x	Uport not valid from BCM driver.
invalid USP calculated from the uport\nx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver
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.
Unable to Insert host H	Host H could not be inserted in hardware host table. A retry will be issued.
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.
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.
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.
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.
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.

O/S Support

Table 60: Linux BSP Log Message

Component	Message	Cause
Linux BSP	rc=10	Second message logged at bootup, right after Starting code.... Always logged.

Table 61: OSAPI Linux Log Messages

Component	Message	Cause
OSAPI Linux	osapiNetLinkNeighDump: could not open socket! – or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX	Couldn‘t open a netlink socket. Make sure “ARP Daemon support” (CONFIG_ARPD) is enabled in the Linux kernel, if the reference kernel binary is not being used.
OSAPI Linux	ipstkNdpFlush: sending delete failed	Failed when telling the kernel to delete a neighbor table entry (the message is incorrect).
OSAPI Linux	osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ	Error adding or deleting an IPv4 route (listed In hex as YY), on the interface with Linux name ZZ Error code can be looked up in errno.h.
OSAPI Linux	l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: Failed to Delete Route	Error adding or deleting a default gateway in the kernel‘s routing table (the function is really osapiRawMRouteAdd()/Delete()).
OSAPI Linux	osapiNetlfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetlPSet: ioctl on XX failed: addr:0x%YY	Failed trying to set the IP address (in hex as YY) of the interface with Linux name XX, and the interface does not exist. Sometimes this is a harmless race condition (e.g., we try to set address 0 when DHCPing on the network port (dtl0) at bootup, before it's created using TAP).
OSAPI Linux	Ping: sendto error	Trouble sending an ICMP echo request packet forthe Ul ping command. Maybe there was no route to that network.
OSAPI Linux	Failed to Create Interface	Out of memory at system initialization time.
OSAPI Linux	TAP Unable to open XX	The/dev/tap file is missing, or, if not using the reference kernel binary, the kernel is missing “Universal TUN/TAP device driver support” (CONFIG_TUN).
OSAPI Linux	Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX	Trouble reading the/dev/tap device, check the error message XX for details.
OSAPI Linux	Log_lnit: log file error – creating new log file	This pertains to the “event log” persistent file in flash. Either it did not exist, or had a bad checksum.

Component	Message	Cause
OSAPI Linux	Log_Init: Flash (event) log full; erasing	Event log file has been cleared; happens at boot time.
OSAPI Linux	Log_Init: Corrupt event log; erasing	Event log file had a non-blank entry after a blank entry; therefore, something was messed up.
OSAPI Linux	Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve interface Flags	Trouble adding VRRP IP or MAC address(es) to a Linux network interface.

14. Switch Management

This chapter describes the management functions available on the 5000 Series devices.

The series also supports ONIE for the installation of an operating system.

CAUTION: By selecting the **ONIE: Install OS** any previously installed operating systems will be automatically removed from the switch, which will require the re-installation of the new OS. See Install Other OS or D-Link OS on page 1254 for further details.

D-Link OS First Instance

When powering on the switch for the first time, the D-Link OS requires activation. See the following information for further details regarding the first instance logging in.

1. In the first logging in instance enter the command **sudo license install [activation code]** to activate the operating system. Refer to the license activation information for the required information. The switch needs to reboot to continue. After the reboot, go to step 2.

```
admin@Switch:~$ sudo license install [activation code]
sudo: unable to resolve host Switch
License successfully installed (AC: activation code)
Please reboot the device to activate the license.
Do you want to reboot now? (y/n): y
```

2. After the operating system is activated, enter the command **sudo dlink-os-cli** to enter the D-Link OS command interface.

```
Ubuntu 14.04 LTS Switch ttyS1
Switch login: admin
Password:
Last login: Mon Feb 26 19:40:30 UTC 2001 on ttyS1
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.16.0-29-generic x86_64)

* Documentation:  https://help.ubuntu.com/
admin@Switch:~$ sudo dlink-os-cli
sudo: unable to resolve host Switch
[sudo] password for admin:

Initializing console session. Press ^z to exit.

(Switch) #
```

Upgrade D-Link OS

The switch is equipped with an operating system which can be upgraded. Before starting any upgrade procedure, make sure the switch has the D-Link OS currently installed.

To upgrade the D-Link OS in Linux shell use the following guidelines:

1. Upload the D-LINK OS deb file to switch including the HW monitoring driver.

   scp –P 2233 filename.deb admin@Switch-IP:filename.deb

2. Enter the password (admin).

   The following is an example of the CLI display output for the command.

```
[tester@lhatws1 ~/upgradeboot]$ scp -P 2233 3.2-nc2x-1.00.006-rc-advance-DLink-DXS-
5000-54S.deb admin@172.20.192.70:3.2-nc2x-1.00.006-rc-advance-DLink-DXS-5000-54S.deb
admin@172.20.192.70's password:
3.2-nc2x-1.00.006-rc-advance-DLink-DXS-5000-54S.deb     100%   23MB  23.4MB/s   00:01
```

3. Make sure the file exists in the switch.
4. Upgrade the switch including the HW monitoring driver (optional), not required for upgrading.

   dpkg –I filename.deb

   The following is an example of the CLI display output for the command.

```
Switch:/home/admin# dpkg -I 3.2-nc2x-1.00.006-rc-advance-DLink-DXS-5000-54S.deb
 new debian package, version 2.0.
 size 24534688 bytes: control archive=4564 bytes.
     130 bytes,     5 lines      conffiles
     333 bytes,    10 lines      control
    7523 bytes,   119 lines      md5sums
    2872 bytes,    84 lines   *  postinst             #!/bin/sh
     664 bytes,    23 lines   *  preinst              #!/bin/sh
     662 bytes,    23 lines   *  prerm                #!/bin/sh
 Package: dlink-os-x86
 Version: 1.00.006
 Architecture: amd64
 Maintainer: D-Link Corporation
 Installed-Size: 111665
 Depends: p7zip-full, gawk, tftp-hpa, screen, psmisc, gdbserver, iptables
 Section: misc
 Priority: optional
 Description: Networking software for D-Link Corporation
              Image signature 3.2-nc2x-1.00.006-rc.img.
```

5. Validate the D-Link OS version.

   The following is an example of the CLI display output for the command.

```
(DXS-5000-54S-2011) #show version

Switch: 1

System Description.............................. DXS-5000-54S - 48 10GE + 6 40GE,
1.00.006, Linux 3.16.0-29-generic
Machine Type.................................... DXS-5000-54S - 48 10GE + 6 40GE
Machine Model................................... DXS-5000-54S
```

```
Hardware Version.............................. A1
Serial Number................................. SG1J100000001
Part Number................................... BXS500054SAB.A1
Burned In MAC Address......................... 00:05:64:2F:0F:80
Software Version.............................. 1.00.006
Operating System.............................. Linux 3.16.0-29-generic
```

Install Other OS or D-Link OS

Open Network Install Environment (ONIE) allows the installation of third-party network operating systems on the switch.

Note: When using a TFTP server, it is recommended to configure the TFTP server to be in the same subnet as the switch and to connect the server directly to the switch. The default IP of switch's management port is 192.168.3.10 with subnet mask 255.255.255.0, so the server should be configured in the 192.168.3.x subnet.

Note: Currently only D-Link and Pluribus Network operating systems are supported. For more information on how to obtain a license and installation instructions for the Pluribus Network OS, visit www.pluribusnetworks.com.

Use the following procedure for installing/upgrading the switch to install the OS on the switch. Below is an example of installing D-Link OS over TFTP.

1. In the OS selection, select **ONIE** and press **Enter**.

```
   GNU GRUB  version 2.02~beta3

+----------------------------------------------------------------------------+
|*D-Link OS                                                                  |
| ONIE                                                                       |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+

     Use the ^ and v keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
  The highlighted entry will be executed automatically in 0s.
```

2. From the ONIE interface window, select **ONIE: Install OS** and press **Enter**.

CAUTION: By selecting the **ONIE: Install OS** any previously installed operating systems will be automatically removed from the switch and will require the OS to be reinstalled. See Install Other OS or D-Link OS on page 1254 for further details.

```
                      GNU GRUB  version 2.02~beta3
```

```
 +----------------------------------------------------------------------------+
 |*ONIE: Install OS                                                           |
 | ONIE: Rescue                                                               |
 | ONIE: Uninstall OS                                                         |
 | ONIE: Update ONIE                                                          |
 | ONIE: Embed ONIE                                                           |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 +----------------------------------------------------------------------------+

      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands
      before booting or `c' for a command-line.
```

3. Enter the command *onie-discovery-stop* to stop ONIE discovery.

```
ONIE:/ #onie-discovery-stop
discover: installer mode detected.
Stopping: discover...done.
ONIE:/#
```

4. Enter the command: **onie-nos-install tftp://[IP address]/[ONIE installer file name]**

In this example, the command appears as follows:
onie-nos-install tftp://ip address/onie-installer-x86_64-nc2x_rangeley-1.00.006-rc-DLink-DXS-5000-54S.

```
ONIE:/# onie-nos-install tftp://ip address/onie-installer-x86_64-nc2x_rangeley-
1.00.006-rc-DLink-DXS-5000-54S
```

When the OS installation is successful, the switch automatically reboots. The newly installed OS appears in the OS selection menu.

SNTP Configuration for x86 D-Link OS

1. Enter Linux shell from D-LINK OS shell
   (Switch) #linuxsh
   Trying 127.0.0.1...
   Connected to 127.0.0.1
   Ubuntu 14.04 LTS
   sroot@Switch:/#
2. Synchronize with the time server by sntp program as below
   root@Switch:/# sntp x.x.x.x/SNTP server domain name
3. Add the command to rc.loal as below
   # By default this script does nothing.
   sntp x.x.x./SNTP server domain name
   exit 0

NTP Configuration for x86 D-Link OS

1. Enter Linux shell from D-LINK OS shell
   (Switch) #linuxsh
   Trying 127.0.0.1...
   Connected to 127.0.0.1
   Ubuntu 14.04 LTS
   root@Switch:/#
2. Backup the original NTP configuration file
   root@Switch:/# cp /etc/ntp.conf /etc/ntp.conf.bak
3. Configure your NTP server IP in ntp.conf. See the following example:
   root@Switch:/# vi /etc/ntp.conf
4. In the illustrated screen, delete the following entries:

   Server 0.ubuntu.pool.ntp.org

   Server 1.ubuntu.pool.ntp.org

   Server 2.ubuntu.pool.ntp.org

   Server 3.ubuntu.pool.ntp.org

   -

   Server ntp.ubuntu.com

```
#more information
Server 0.ubuntu.pool.ntp.org
Server 1.ubuntu.pool.ntp.org
Server 2.ubuntu.pool.ntp.org
Server 3.ubuntu.pool.ntp.org

#Use Ubuntu's ntpserver as a fallback.
Server ntp.ubuntu.com
```

   Once the entries are deleted, specify one or more NTP servers. The following screen lists correct setting information.

```
#more information
#server yourNTPserverIP/Domian Name
```

5. Restart the NTP service
   root@Switch:/home/admin# service ntp restart
   Stopping NTP server ntpd
   …done
   Starting NTP server ntpd
   …done
   root@Switch:/home/admin#
6. To ensure the process is complete, make sure the NTP server time is synchronized with your device.
   root@Switch:/# date
   Mon 25 19 07:59:55 UTC 2018 <=time should be synchronized with server
   root@Switch:/#