Data Center Switches

MES5448
MES7048

Operation Manual, Firmware Version 8.4.0.7

Document Version	Issue Date	Revisions
Version 4.0	30.04.2021	Synchronization with firmware version 8.4.0.7
Version 3.0	25.12.2020	Synchronization with firmware version 8.4.0.6
Version 2.0	31.07.2020	Synchronization with firmware version 8.4.0.5
Version 1.0	26.09.2019	First issue
Firmware version 8.4.0.7		

CONTENTS

SYMBOLS

Symbol	Description
[ ]	Square brackets are used to indicate optional parameters in the command line; when entered, they provide additional options.
{}	Curly brackets are used to indicate mandatory parameters in the command line. You need to choose one of them.
“,” **“-”**	In the command description, these characters are used to define ranges.
“|”	In the command description, this character means 'or'.
“/”	In the command description, this character indicates the default value.
Calibri Italic	Calibri Italic is used to indicate variables and parameters that should be replaced with an appropriate word or string.
Bold	Notes and warnings are shown in semibold.
<Bold Italic>	Keyboard keys are shown in bold italic within angle brackets.
`Consolas`	Command examples are shown in Consolas.
`Consolas`	Command execution results are shown in Consolas in a frame with a shadow border.

Notes and Warnings

Notes contain important information, tips, or recommendations on device operation and configuration.

Warnings inform the user about situations that may be harmful to the user, cause damage to the device, malfunction or data loss.

1 INTRODUCTION

Eltex MES5448 and MES7048 switches provide full Layer 2 and Layer 3 functionality allowing them to be used as aggregation switches as well as in data centers. Switch software is optimized to scale and improve data center performance.

MES5448 and MES7048 meet the data centers requirements for Top-of-Rack and End-of-Row switches and carrier requirements for aggregation and backbone networks equipment, providing high performance and cost-efficient solution.

2 PRODUCT DESCRIPTION

2.1 Purpose

MES5448 and MES7048 switches are high-performance devices equipped with 10GBASE-R/1000BASE-X and 40GBASE-R, 100GBASE-SR4/LR4 interfaces and intended to be used in data centers as Top-of-Rack or End-of-Row switches as well as in aggregation and backbone networks of carriers.

Non-blocking switching matrix allows correctly processing of packets at maximum speads, while maintaining minimal and predictable delays on all types of traffic.

The front-to-back cooling provides effective cooldown in modern data centers.

The devices allow hot swapping of power and ventilation modules providing smooth network operation.

2.2 Switch features

2.2.1 Basic features

Table 2.1 lists the basic administrable features of switches of this series.

Table 2.1 – Basic device features

Head-of-line blocking (HOL) protection	HOL blocking occurs when device output ports are overloaded with traffic coming from input ports. It may lead to data transfer delays and packet loss.
Jumbo Frames	The ability to support the transmission of super-long frames, which allows data to be transmitted by a smaller number of packets. This reduces the amount of service information and, consequently, the packets processing time.
Flow control (IEEE 802.3X)	With flow control you can interconnect low-speed and high-speed devices. For avoid buffer overrun, the low-speed device can send PAUSE packets that will force the high-speed device to pause packet transmission.
Operation in device stack	You can combine multiple switches in a stack. In this case, switches are considered as a single logic device with shared settings. There are two stack topologies — ring and chain. All ports of each stack unit must be configured from the master switch. Device stacking allows for reducing network management efforts and increasing its fault-tolerance.

2.2.2 MAC address processing features

Table 2.2 lists MAC address processing features.

Table 2.2 –MAC address processing features

Table of MAC addresses	The switch creates an in-memory look-up table which contains MAC addresses and due ports.

Learning mode	When learning is not available, the incoming data on a port will be transmitted to all other ports of the switch. Learning mode allows the switch to analyse the frame, discover sender's MAC address and add it to the routing table. Then, if the destination MAC address of an Ethernet frames is already in the routing table, that frame will be sent to the port specified in the table.
MAC Multicast support *(MAC Multicast support)*	This feature enables one-to-many and many-to-many data distribution. Thus, the frame addressed to a multicast group will be transmitted to each port of the group.
Automatic Aging for MAC Addresses *(Automatic Aging for MAC Addresses)*	If there are no packets from a device with a specific MAC address in a specific period, the entry for this address expires and will be removed. It keeps the switch table up to date.

2.2.3 Layer 2 features

Table 2.3 lists *Layer 2 (OSI Layer 2)* features and special aspects.

Table 2.3 – Layer 2 (OSI Layer 2) Features description

IGMP Snooping	IGMP implementation analyses the contents of IGMP packets and discovers network devices participating in multicast groups and forwards the traffic to the corresponding ports.
MLD Snooping	MLD protocol implementation allows the device to minimize multicast IPv6 traffic.
MVR (Multicast VLAN Registration)	This feature can redirect multicast traffic from one VLAN to another using IGMP messages and reduce uplink port load. Used in III-play solutions.
Storm Control *(Broadcast, multicast, unknown unicast Storm Control)*	«Storm» is a multiplication of broadcast, multicast and unknown unicast packets in each host causing their exponential growth that can lead to the network meltdown. The switches can restrict the transfer rate for multicast and broadcast frames received and sent by the switch.
Port Mirroring *(Port Mirroring)*	Port mirroring is used to duplicate the traffic on monitored ports by sending ingress or and/or egress packets to the controlling port. Switch users can define controlled and controlling ports and select the type of traffic (ingress or egress) that will be sent to the controlling port.
Protected ports	This feature enables the creation of isolated group of ports that can exchange traffic only with each other. Traffic can not expand beyond a group.
Support of Private VLAN	Private VLAN (PVLAN) technology enables isolation of L2 traffic between switch ports located in the same broadcast domain.
Spanning Tree Protocol	Spanning Tree Protocol is a network protocol that ensures loop-free network topology by converting networks with redundant links to a spanning tree topology. Switches exchange configuration messages using frames in a specific format and, based on which, enable or disable traffic transmission through ports.
IEEE 802.1w Rapid spanning tree protocol	Rapid STP (RSTP) is the enhanced version of the STP that enables faster convergence of a network to a spanning tree topology.
IEEE 802.1w Rapid spanning tree protocol	Multiple Spanning Tree Protocol (MSTP) is the enhanced version of the RSTP that enables configuration of a single spanning tree for certain VLANs or VLAN groups.
Per-VLAN Spanning Tree protocol Plus	Per-VLAN Spanning Tree protocol Plus (PVSTP+) is the enhanced version of the STP that enables the start of certain STP instances in certain VLANs.

VLAN	VLAN is a group of switch ports that form a single broadcast domain. The switch supports various packet classification methods to identify the VLAN they belong to.
802.1Q	IEEE 802.1Q is an open standard that describes the traffic tagging procedure for transferring VLAN inheritance information. It allows multiple VLAN groups to be used on one port.
OAM (Operation, Administration, and Maintenance, IEEE 802.3ah)	EthernetOAM (Operation, Administration, andMaintenance), IEEE 802.3ah – functions of data transmission channel level corresponds to channel status monitor protocol. The protocol uses data blocks of OAM (OAM PDU) to transmit information on the channel status between connected Ethernet devices. Both devices must support standard IEEE 802.3ah.
GARP VLAN (GVRP)	GARP VLAN registration protocol dynamically add/removes VLAN groups on the switch ports. If GVRP is enabled, the switch identifies and then distributes the VLAN inheritance data to all ports that form the active topology.
Port-Based VLAN	This feature enables assigning VLAN tag to a packet on the basis of the physical port it was received from.
LAG group creation	The device allows for link group creation. Link aggregation, trunking is a technology that enables aggregation of multiple physical links into one logical link. This leads to greater bandwidth and reliability of the backbone 'switch-switch' or 'switch-server' channels. There are options for traffic balancing based on MAC address, IP address, VLAN and TCP/UDP port. A LAG group contains ports with the same speed operating in full-duplex mode.
Link aggregation with LACP	LACP (IEEE 802.3ad) provides automatic aggregation of multiple switch physical ports to a single data transmission link. The protocol constantly monitors whether link aggregation is possible; in case one link in the aggregated channel fails, its traffic will be automatically redistributed to functioning components of the aggregated channel.
Auto Voice VLAN support	Allows you to identify voice traffic by OUI (Organizationally Unique Identifier—first 24 bits of the MAC address) or L4 port. If the MAC table of the switch contains a MAC address with VoIP gateway or IP phone OUI, this port will be automatically added to the voice VLAN (identification by SIP or the destination MAC address is not supported).
Dot1ad	QinQ tunnels implementation, according to which the traffic incoming from a user to carrier's network is tagged with two VLAN tags. Internal tag is a customer tag (C-tag) and external one is a Service VLAN tag (S-tag).

2.2.4 Layer 3 features

Table 2.4 lists Layer 3 functions (OSI Layer 3).

Table 2.4 – Layer 3 Features description (Layer 3)

BootP and DHCP clients (Dynamic Host Configuration Protocol)	The devices can obtain IP address automatically via the BootP/DHCP.
Static IP routes	The switch administrator can add or remove static entries into/from the routing table.
Address Resolution Protocol	ARP maps the IP address and the physical address of the device. The mapping is established on the basis of the network host response analysis; the host address is requested by a broadcast packet.

RIP (Routing Information Protocol)	The dynamic routing protocol that allows routers to get new routing information from the neighbour routers. This protocol detects optimum routes on the basis of hops count data.
OSPF protocol (Open Shortest Path First)	A dynamic routing protocol that is based on a link-state technology and uses Dijkstra's algorithm to find the shortest route. OSPF protocol distributes information on available routes between routers in a single autonomous system.
Virtual Router Redundancy Protocol (VRRP)	VRRP is designed for backup of routers acting as default gateways. This is achieved by joining IP interfaces of the group of routers into one virtual interface which will be used as the default gateway for the computers of the network.
BFD (Bidirectional Forwarding Detection)	BFD protocol ensures bidirectional connectivity between routers that can be more than one hop apart. BFD has a very low time (flexibly customizable) for determining the failure of the communication channel and, as a result, a quick switch to the redundant route.
BGP	BGP (Border Gateway Protocol) is a dynamic routing protocol, that belongs to the class of external gateway routing protocols. BGP is designed to exchange subnet reachability information between autonomous systems, that is, groups of routers under common technical and administrative control. It uses the intradomain routing protocol to determine the routes inside and the interdomain routing protocol to determine the packet delivery routes to other autonomous systems.

2.2.5 QoS features

Table 2.5 lists the basic quality of service features.

Table 2.5 – Basic quality of service features

Priority queues support	The switch supports egress traffic prioritization with queues for each port. Packets are distributed into queues by classifying them by various fields in packet headers.
802.1p class of service support	802.1p standard specifies the method for indicating and using frame priority to ensure on-time delivery of time-critical traffic. 802.1p standard defines 8 priority levels. The switches can use 802.1p priority value to assign frames to priority queues.

2.2.6 Security features

Table 2.6 – Security features

DHCP snooping	A switch feature designed for protection from DHCP attacks. Enable filtering of DHCP messages coming from untrusted ports by building and maintaining DHCP snooping binding database. DHCP snooping performs functions of a firewall between untrusted ports and DHCP servers.
UDP relay	Broadcast UDP traffic forwarding to the specified IP address.
DHCP server features	DHCP server performs centralised management of network addresses and corresponding configuration parameters, and automatically provides them to subscribers.
IP Source address guard	The switch feature that restricts and filters IP traffic according to the mapping table from the DHCP snooping binding database and statically configured IP addresses. This feature is used to prevent IP address spoofing.

Dynamic ARP Inspection (Protection)	A switch feature designed for protection from ARP attacks. The switch checks the message received from the untrusted port: if the IP address in the body of the received ARP packet matches the source IP address. If these addresses do not match, the switch drops this packet.
L2 – L3 – L4 ACL (Access Control List)	Using information from the level 2, 3, 4 headers, the administrator can configure politics for processing or dropping packets.
Time-Based ACL	Allow you to configure the time frame for ACL operation.
Port Security	A switch feature that allows you to specify the host MAC addresses that are allowed to transmit data through the port. After that, the port transmits packets if the sender's MAC address is not specified as allowed.
Port based authentication (802.1x)	IEEE 802.1x authentication mechanism manages access to resources through an external server. Authorized users will gain access to the network resources.

2.2.7 Switch Control features

Table 2.7 – Switch control features

Uploading and downloading the configuration file	Device parameters are saved into the configuration file that contains configuration data for the specific device ports as well as for the whole system.
Trivial File Transfer Protocol (TFTP)	The TFTP is used for file read and write operations. This protocol is based on UDP transport protocol. The devices are able to outswap and transfer configuration files and firmware images via this protocol.
Secure Copy protocol (SCP)	SCP is used for file read and write operations. This protocol is based on SSH network protocol. The devices are able to download and transfer configuration files and firmware images via this protocol.
File Transfer Protocol (FTP)	The FTP is used for file read and write operations. This protocol is based on TCP transport protocol. The devices are able to outswap and transfer configuration files and firmware images via this protocol.
SSH File Transfer Protocol (SFTP)	SFTP is an application level protocol designed to copy and perform other file operations on top of a secure and reliable connection. The devices are able to outswap and transfer configuration files and firmware images via this protocol.
Remote monitoring (RMON)	Remote network monitoring (RMON) is an extension of SNMP that enables monitoring of computer networks. Compatible devices gather diagnostics data using the network management station. RMON is a standard MIB database that contains actual and historic MAC-level statistics and control objects that provide real-time data.
Simple Network Management Protocol (SNMP)	SNMP is used for monitoring and management of network devices. It consists of a set of standards for network management, including an application protocol, a database chart, and a set of data objects.
Command Line Interface (CLI)	Switches can be managed using CLI locally via serial port RS-232, or remotely via Telnet/SSH. Console command line interface (CLI) is an industrial standard. CLI interpreter provides a list of commands and keywords that help the user and reduce the amount of input data.
Syslog	*Syslog* is a protocol designed for transmission of system event messages and error notifications to remote servers.
SNTP (Simple Network Time Protocol)	*SNTP* is a time synchronization protocol. This protocol guarantees the accuracy of time synchronization of a network device with a server up to a millisecond.

Traceroute	*Traceroute* is a service feature that allows the user to display data transfer routes in IP networks.
Privilege level controlled access management	The administrator can define privilege levels for device users and settings for each privilege level (read-only - level 1, full access - level 15).
Management interface blocking	The switch can block access to each management interface (SNMP, CLI). Each access interface can be blocked independently: Telnet (CLI over Telnet Session) Secure Shell (CLI over SSH) TFTP HTTP HTTPS SNMP SNTP
Local authentication	Passwords for local authentication can be stored in the switch database.
RADIUS client	RADIUS is used for authentication, authorization and accounting. RADIUS server uses a user database that contains authentication data for each user. The switches implement a RADIUS client.
(TACACS+) Terminal Access Controller Access Control System	The device supports client authentication with TACACS+ protocol. The TACACS+ protocol provides a centralized security system that handles user authentication and a centralized management system to ensure compatibility with RADIUS and other authentication mechanisms.
SSH server	SSH server functionality allows SSH clients to establish secure connection to the device for management purposes.
Macrocommand support	This feature allows the user to create sets of commands–macrocommands–and user them to configure the device.

2.2.8 Data Center features

Table 2.8 - Main Data Center features

FIP Snooping	Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) is a security feature intended for preventing of unauthorized access and data transmission in Fibre Channel (FC) networks. The feature filters traffic, allowing only those storage servers that are entitled to it.
LLDP DCBX	Data Center Bridging Exchange (DCBX) protocol is used by devices to exchange configuration information with directly connected nodes. It is an extension of LLDP.
PFC (Priority Flow Control)	The Priority-based flow control (PFC) feature provides the means to suspend traffic of a certain priority (802.1p) when congestion occurs in an outgoing queue.
QCN (Quantized Congestion Notification)	The 802.1Qau standard solves the problem of overflowing outgoing queues using the Quantized Congestion Notification (QCN) protocol. Switches constantly analyze the load of their outgoing queues. When the queue size exceeds a certain threshold and continues to grow, the switch sends special service messages to the traffic source at a specific frequency.
ETS (Enhanced Transmission Selection)	This protocol provides the capability to flexibly adjust the bandwidth for traffic of a certain priority.

Cut-Through	The Cut-Through mode allows the switch to begin forwarding a packet before its reception has been completed. That reduces delays when sending large and super-large packets.
Openflow	Openflow protocol allows you to manage the switch from a central Openflow controller.

2.2.9 Additional features

Table 2.9 lists additional device features.

Table 2.9 – Additional device functions

Virtual Cable Test (VCT)	The network switches are equipped with the hardware and software tools that allow them to perform the functions of a virtual cable tester (VCT). The tester check the condition of copper communication cables.
Optical transceiver diagnostics	The device can be used to test the optical transceiver (DDM). During testing, parameters such as current and supply voltage, transceiver temperature, signal power are monitored. Implementation requires support of these functions in the transceiver.

2.3 Main specifications

Table 2.10 shows main switch specifications.

Table 2.10 – Main specifications

General parameters		
Packet processor	MES5448	Broadcom BCM56846A1
	MES7048	Broadcom BCM56860 (Trident2+)
Interfaces	MES5448	1 x 10/100/1000BASE-T (OOB); 48x10GBASE-R (SFP+)/1000BASE-X (SFP) 4x40GBASE-SR4/LR4 (QSFP+) 1xUSB
	MES7048	1 x 10/100/1000BASE-T (OOB); 48 x 10GBASE-R (SFP+)/1000BASE-X (SFP); 6 x 100GBASE-SR4/LR4 (QSFP28) 1xUSB
Capacity	MES5448	1.28 Tbps
	MES7048	1.92 Tbps
Buffer memory	MES5448	9 MB
	MES7048	16 MB
MAC Address Table	MES5448	128K
	MES7048	228K
TCAM routing volume (number of ACL rules)	MES5448	2K input, 1K output
	MES7048	16K input, 1K output
ARP records number		6K

Number of IPv4 Unicast routes		16K[1]
Number of IPv6 Unicast routes		8K[2]
Number of multicasrt groups		2K
VLAN table		4094
SQinQ rules number		4094
Quality of Services (QoS)		7 queues
Total number of VRRP routers		20
Total number of L3 interfaces		256
Total number of virtual Loopback interfaces		64
LAG		64, up to 32 ports per LAG
MSTP instances quantity		64
Jumbo frames	MES5448	12270 bytes
	MES7048	9394 bytes
Stacking		Up to 8 devices
Standard compliance		IEEE 802.3ac IEEE 802.3ad – channel aggregation IEEE 802.3ae – 10 GbE IEEE 802.1ak – MRP IEEE 802.1S – Multiple Spanning Tree (MST) IEEE 802.1W – Rapid Spanning Tree (RSTP) IEEE 802.1D – Spanning Tree (STP) IEEE 802.1Qat – MSRP IEEE 802.1Qav – Time-Sensetive Streams IEEE 801.1Qbb IEEE 802.1v – VLAN classification IEEE 802.1p – traffic prioritization IEEE 802.1X IEEE 802.3x – Flow Control IEEE 802.1AB – LLDP IEEE 802.1Qbb – Priority-based Flow Control IEEE 802.1ad – Double VLAN tagging IEEE 802.1ag – Connectivity Fault Management (CFM) IEEE 802.3ah – Operations, Administration, and Maintenance (OAM) IEEE 802.1Qau – Congestion Notification IEEE 802.1Qaz – Enhanced Transmission Selection (ETS)
Control		
Local control		Console
Remote control		Telnet, SSH, SNMP, Netconf, HTTP/HTTPS, OpenFlow
Physical specifications and ambient conditions		
Power supply		AC: 176..264V, 50 Hz DC: 36..72V Power options: - Single AC or DC power supply - Two AC or DC hot-swappable power supplies

[1] Number of IPv4 Unicast routes can be increased up to 256K
[2] Number of IPv6 Unicast routes can be increased up to 128K

Power consumption	MES5448	max 150 W
	MES7048	max 400 W
Dimensions	MES5448	440 x 425 x 44
	MES7048	440 x 447 x 44
Operating temperature		From 0 to 50°C
Storage temperature		From -40 to +70°C
Relative humidity		Not more than 80% (without condensation)
Average lifetime		10 years

2.4 Design

This section describes design of MES5448 and MES7048 switches, presents front, rear and side device panel views, describes the connectors, LEDs and controls.

MES5448 and MES7048 switches have a metal-enclosed design for 1U 19" racks.

2.4.1 Layout and description of MES5448 front panel

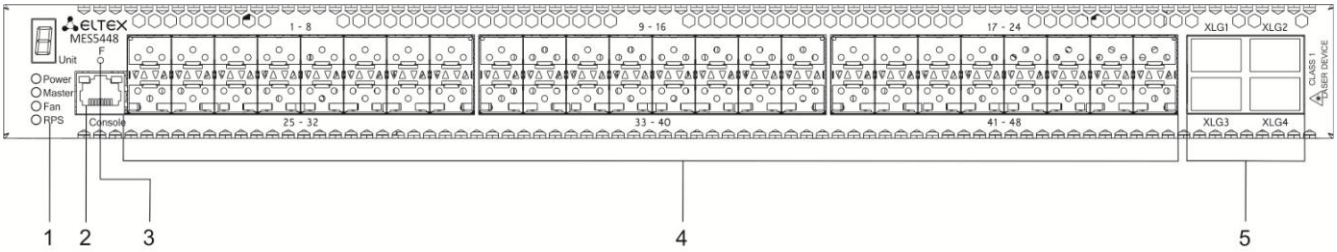

Fig. 1 – MES5448 front panel

Table 2.11 lists connectors, LEDs and controls located on the front panel of the switch.

Table 2.11 – Description of MES5448 connectors, LEDs and the controls located on the front panel

№	Front panel element	Description
1	Unit ID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Fan	Fan operation LED.
	RPS	Backup power supply LED.

2	Console	Console port for local management of the device. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used
3	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device; - pressing the key for more than 10 seconds resets the device to factory default configuration.
4	[1-48]	Slots for 10g SFP+/1G SFP transceivers.
5	XLG1, XLG2 XLG3, XLG4	Slots for XLG1-XLG4 transceivers Transceivers 40G QSFP+

2.4.2 MES5448 rear panel

The rear panel layout of MES5448 switch is depicted in - *Fig. 2*

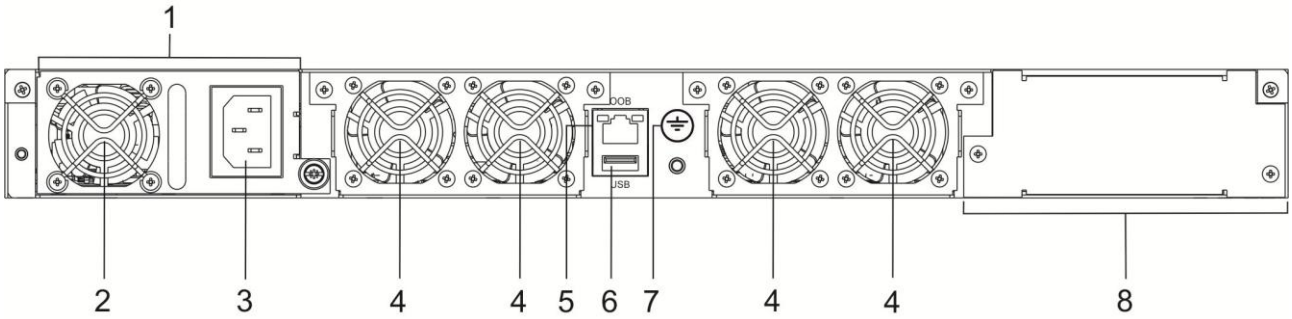

Fig. 2 – MES5448 rear panel

Table 2.12 lists rear panel connectors of the switch.

Table 2.12 – Description of the rear panel connectors of the switch

№	Rear panel elements	Description
1		PM350-220/12 power source
2		Power source fan
3	~220 VAC 50 Hz max 1A	Connector for AC power supply
4	Removable fans	Hot-swappable removable ventilation modules
5	OOB	Out-of-band 10/100/1000BASE-T (RJ-45) port for remote device management. Management is performed over network isolated from the transportation network.
6	USB	USB port

7	Earth bonding point ⏚	Earth bonding point of the device
8		Backup power supply slot

2.4.3 MES5448 side panels

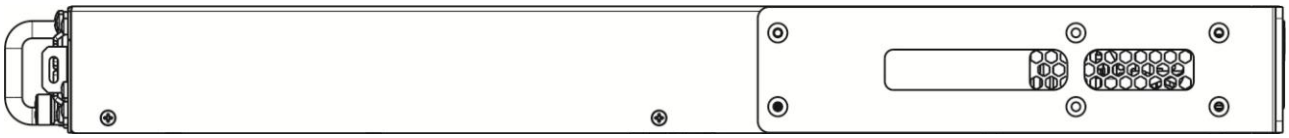

Fig. 3 - right side MES5448 panel

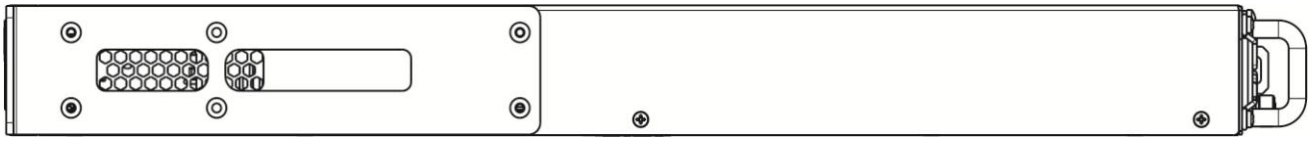

Fig. 4 - left side MES5448 panel

Side panels of the device have air vents for heat removal. Do not block air vents. This may cause overheating of the components, which may result in device malfunction. For recommendations on device installation, see section 'Installation and connection'.

2.4.4 Layout and description of MES7048 front panel

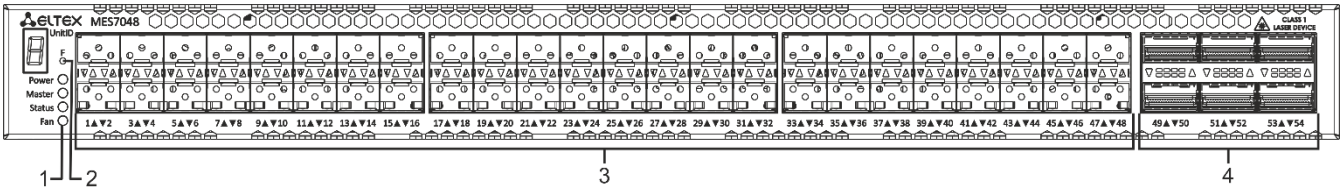

Fig. 5 – MES7048 front panel

Table 2.13 lists connectors, LEDs and controls located on the front panel of the switch.

Table 2.13 – Description of MES7048 connectors, LEDs and the controls located on the front panel

№	Front panel element	Description
1	Unit ID	Indicator of the stack unit number.
	Power	Device power LED
	Master	Device operation mode LED (master/slave).
	Status	Device status LED
	Fan	Fan operation LED.
2	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device; - pressing the key for more than 10 seconds resets the device to factory default configuration.
3	[1-48]	Slots for 10g SFP+/1G SFP transceivers.
4	[49-54]	Slots for 40G (QSFP+)/100G (QSFP28) transceivers.

2.4.5 MES7048 rear panel

The rear panel layout of MES7048 switch is depicted in - *Fig. 6*.

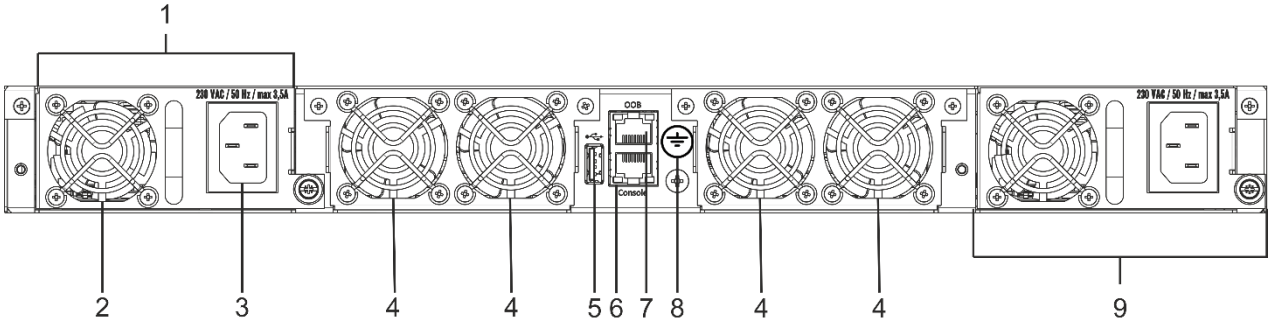

Fig. 6 – MES7048 rear panel

Table 2.14 lists rear panel connectors of the switch.

Table 2.14 – Description of the rear panel connectors of the switch

№	Rear panel elements	Description
1		PM350-220/12 power source
2		Power source fan
3	~220 VAC 50 Hz max 1A	Connector for AC power supply
4	Removable fans	Hot-swappable removable ventilation modules
5	USB	USB port
6	Console	Console port for local management of the device. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used
7	OOB	Out-of-band 10/100/1000BASE-T (RJ-45) port for remote device management. Management is performed over network isolated from the transportation network.
8	Earth bonding point ⏚	Earth bonding point of the device
9		Backup PM350-220/12 power source

2.4.6 MES7048 side panels

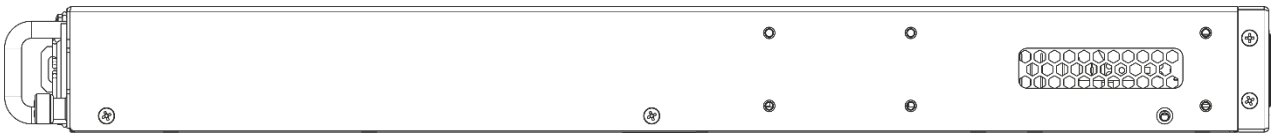

Fig. 7 - right side MES7048 panel

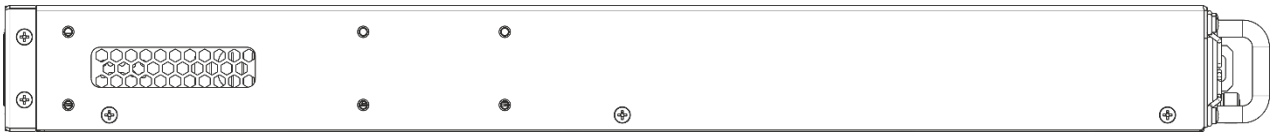

Fig. 8 - left side MES7048 panel

Side panels of the device have air vents for heat removal. Do not block air vents. This may cause overheat of the components, which may result in device malfunction. For recommendations on device installation, see section 'Installation and connection'.

2.4.7 Light indication

Ethernet interface status is represented by two LEDs: green *LINK/ACT* and amber *SPEED*. Location of LEDs is shown in figures ***9*** and 14.

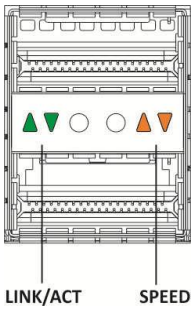

Fig. 9 – QSFP+ transceiver socket layout

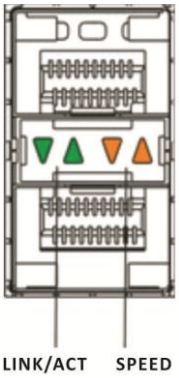

Fig. 10 – SFP/SFP+ socket layout

Table 2.15 – XLG ports status LED

SPEED indicator is lit	*LINK/ACT indicator is lit*	*Ethernet interface state*
Off	Off	Port is disabled or connection is not established
Always on	Always on	40/100 Gbps connection is established
Always on	Flashes	Data transfer is in progress

Table 2.16 – XG ports state LED

SPEED indicator is lit	*LINK/ACT indicator is lit*	*Ethernet interface state*
Off	Off	Port is disabled or connection is not established
Off	Always on	1 Gbps connection is established
Always on	Always on	10 Gbps connection is established
X	Flashes	Data transfer is in progress

Unit ID (1-8) LED indicates the stack unit number.

System indicators (Power, Master, Fan, RPS) are designed to display the operational status of the switch modules.

Table 2.17 – System indicator LED

LED name	LED function	LED State	Device State
Power	Power supply status	Off	Power is off
		Solid green	Power is on, normal device operation
		Solid red	Device power system malfunction
Master	Indicates master stack unit	Solid green	The device is a stack master
		Off	The device is not a stack master or stacking mode is not set
Status	Device temperature LED	Solid green	Temperature is below 80°C
		Solid orange	Temperature is from 80°C to 90°C
		Solid red	Temperature is above 90°C
		Off	Power is off
Fan	Cooling fan status	Solid green	All fans are operational
		Solid red	One or more fans are failed
RPS	Backup power supply operation mode	Solid green	Backup power supply is connected and operates correctly
		solid red	There is no backup source primary power supply or its failure or fan failure.
		Off	Backup power supply is not connected

2.5 Delivery package

The standard delivery package includes:

- Ethernet switch;
- Rack mounting set;
- Information leaflet;
- Certificate of conformity;
- Passport.

At the customer's request, the delivery package can be optionally included:

- User manual on CD;
- Console cable;
- PM350-220/12 power module;
- Power cord Europlug-C13 1.8m (in case of supplying with PM350-220/12 power module);
- PM350-48/12 power module;
- Power cord PVS 2x1.5 2m (in case of supplying with PM350-48/12 power module);
- SFP/SFP+/QSFP+/QSFP28 transceivers.

3 INSTALLATION AND CONFIGURATION

This section describes installation of the equipment into a rack and connection to a power supply.

3.1 Support brackets mounting

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets. To install the support brackets:

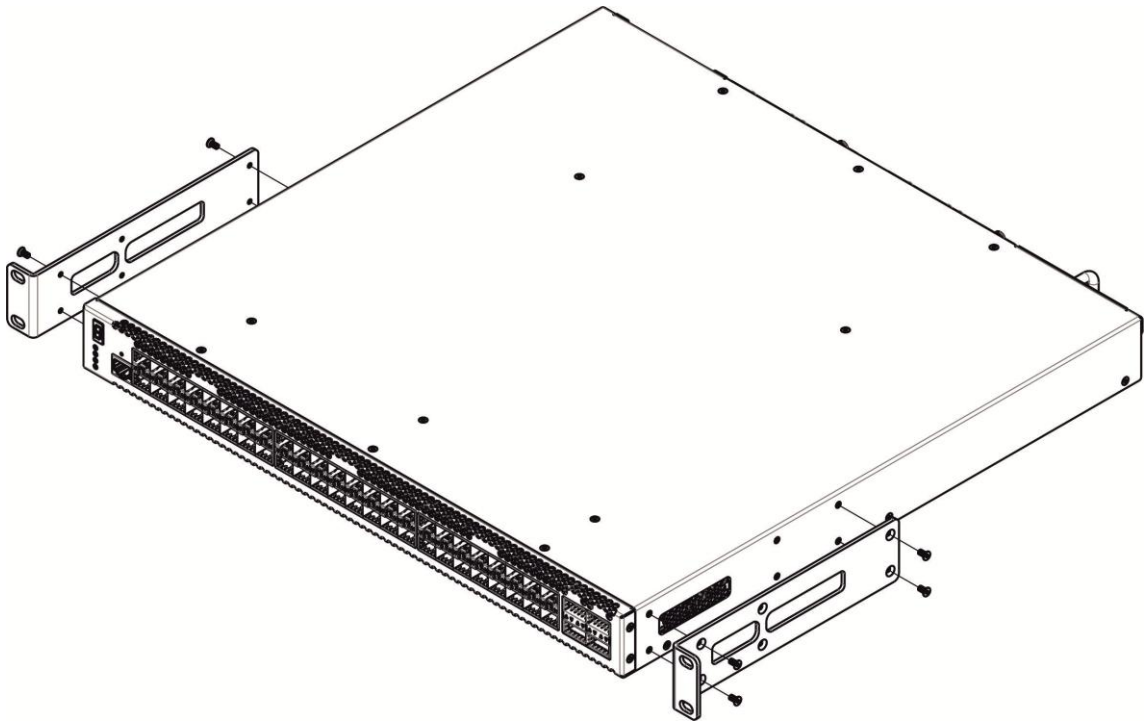

Fig. 11 – Support brackets mounting

1. Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device.
2. Use a screwdriver to screw the support bracket to the case.
3. Repeat steps 1 and 2 for the second support bracket.

3.2 Device rack installation

To install the device to the rack:

1. Attach the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guides. Use the holes of the same level on both sides of the guides to ensure horizontal installation of the device.
3. Use a screwdriver to screw the switch to the rack.

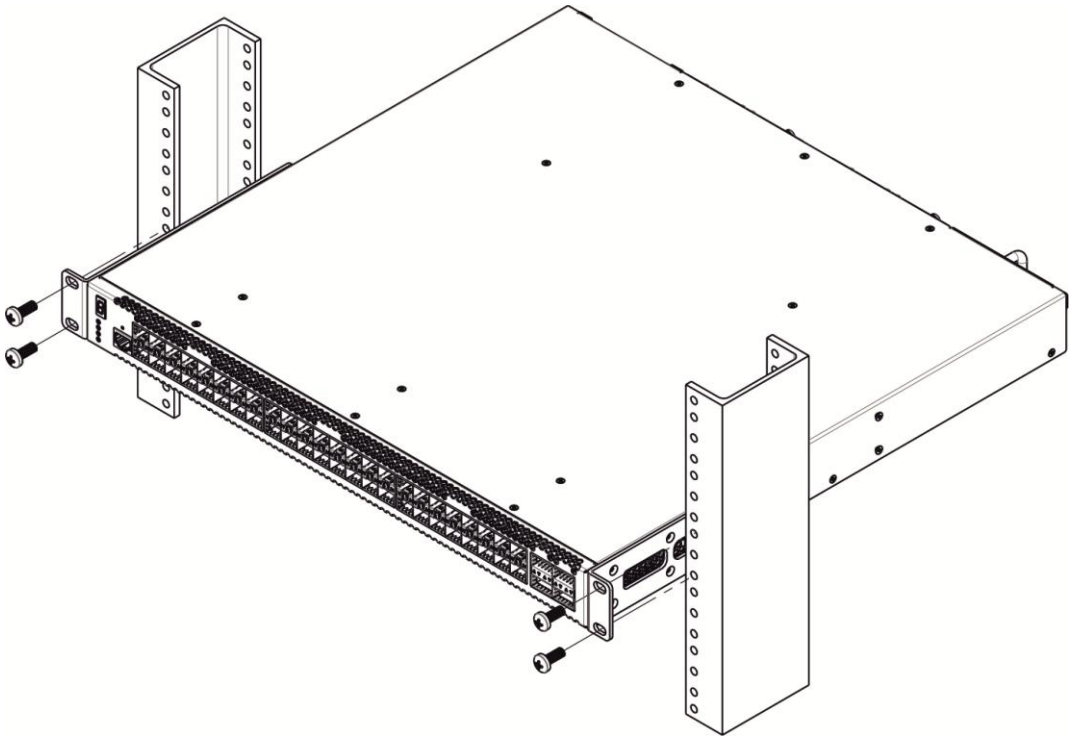

Fig. 12 - Device rack installation

Fig. *13* shows an example of MES5448 rack installation.

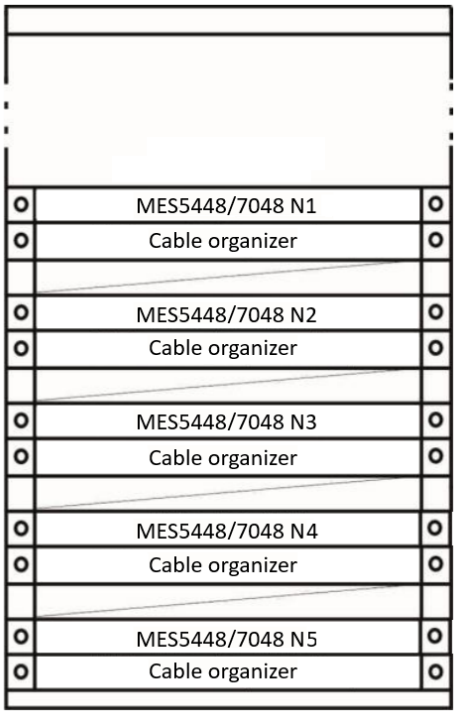

Fig. 13 – MES5448/MES7048 switch rack location

Do not block air vents and fans located on the rear panel to avoid components overheating and subsequent switch malfunction.

3.3 Power module installation

Switch can operate with one or two power modules. The second power module installation is necessary when greater reliability is required.

From the electric point of view, both places for power module installation are equivalent. From the point of view of the device, the power module located on the left (if you look at the back wall of the switch) is considered the main one, on the right - the backup one. Power modules can be inserted and removed without powering the device off. When an additional power module is inserted or removed, the switch continues to operate without reboot.

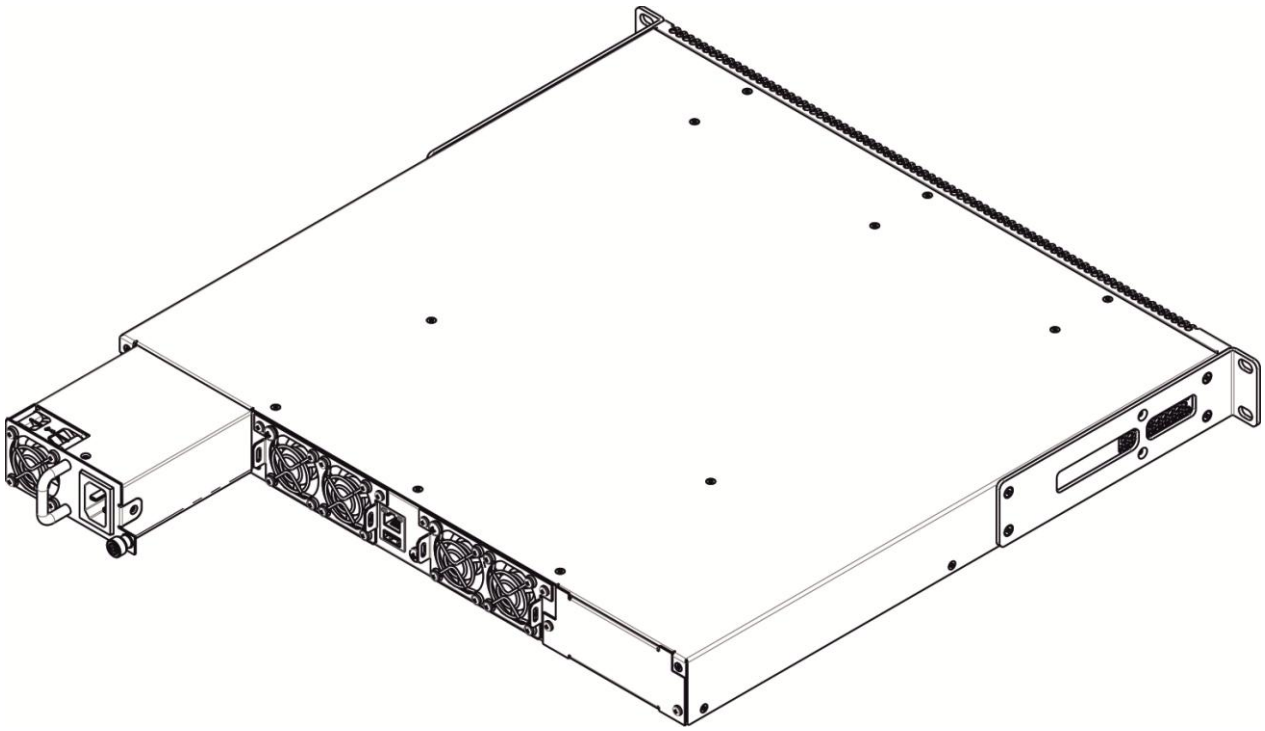

Fig. 14 – Power module installation

You can check the state of power modules by viewing the indication on the front panel of the switch (see Section 2.4.7) or by checking diagnostics available through the switch management interfaces.

Power module fault indication may be caused not only by the module failure, but also by the absence of the primary power supply.

3.4 Connection to power supply

1. Prior to connecting the power supply, the device case must be grounded. Use an insulated stranded wire to ground the case. The grounding device and the ground wire cross-section must comply with Electric Installation Code.

Connection should be performed by a qualified specialist.

2. If you intend to connect a PC or another device to the switch console port, the device must be properly grounded as well.
3. Connect the power supply cable to the device. Depending on the delivery package, the device can be powered by AC or DC electrical network. To connect the device to AC power supply, use the cable from the delivery package. To connect the device to DC power supply, use wires with a minimum cross-section of 1 mm^2.

In order to avoid short-circuits when connecting to the DC network, it is recommended that the wire be stripped to a length of 9 mm.

The DC power supply circuit should contain a power disconnect device with physical separation of the connection (switch, connector, contactor, circuit breaker, etc.).

4. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

3.5 SFP transceiver installation and removal

Optical modules can be installed when the terminal is turned on or off.

1. Insert the top SFP module into a slot with its open side down, and the bottom SFP module with its open side up.

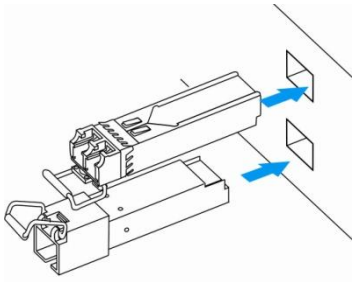

Fig. 15 – SFP transceiver installation

2. Push the module. When it is in place, you should hear a distinctive 'click'.

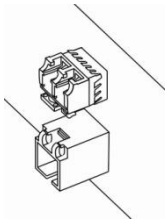

Fig. 16 – Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

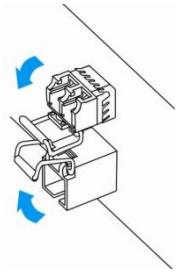

Fig. 17 – Opening SFP transceiver latch

2. Remove the module from the slot.

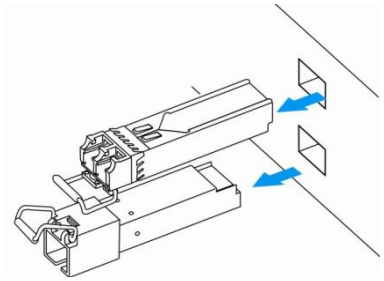

Fig. 18 – SFP transceiver removal

4 INITIAL SWITCH CONFIGURATION

4.1 Terminal configuration

Run the terminal emulation application on PC (HyperTerminal, TeraTerm, Minicom) and perform the following actions:

- Select the corresponding serial port.
- Set the data transfer rate to 115200 baud.
- Specify the data format: 8 data bits, 1 stop bit, non-parity.
- Disable hardware and software data flow control.
- Specify VT100 terminal emulation mode (many terminal applications use this emulation mode by default).

4.2 Device start-up

Establish connection between the switch console ('console' port) and the serial interface port on PC that runs the terminal emulation application.

Turn on the device. Upon every startup, the switch performs a power-on self-test which checks operational capability of the device before the executable program is loaded into RAM.

The process of the «system test» on the MES5448/MES7048 switches:

```
Stopping network: OK
Saving random seed... done.
Unloading kernel modules: OK
Stopping logging: OK
umount: /: not mounted.
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
[78648.185579] reboot: Restarting system

Booting Eltex MES5448/MES7048 BIOS version 3.5...


U-Boot 2016.07-MES5448/MES7048 (Mar 31 2021 - 12:59:35 +0700)

CPU: x86_64, vendor Intel, device 406d8h
DRAM:  4 GiB
SF: Detected MX25L12805 with page size 256 Bytes, erase size 64 KiB, total 16
MiB
Model: Eltex MES5448/MES7048
SF: Detected MX25L12805 with page size 256 Bytes, erase size 64 KiB, total 16
MiB
Loading FPGA image: ............................OK.
SF: Detected MX25L12805 with page size 256 Bytes, erase size 64 KiB, total 16
MiB
SCSI:  scanning bus for devices...
  Device 0: (1:0) Vendor: ATA Prod.: 8GB SATA Flash D Rev: SFPS
            Type: Hard Disk
            Capacity: 7641.2 MB = 7.4 GB (15649200 x 512)
Found 1 device(s).
Net:   eth0: e1000#0
Autoboot in 5 seconds
```

The switch firmware will be automatically loaded five seconds after testing is completed.

After successful startup, you will see the CLI interface prompt.

```
 Applying Global configuration, please wait ...

Applying Interface configuration, please wait ...



User Name:admin
Password:
console>enable

console#
```

The default user name is «admin», password is empty. The password for «admin» can be configured, but this user cannot be deleted. There is no password for privileged mode by default.

To quickly get help for available commands, use key combination *SHIFT+?*.

5 COMMAND LINE INTERFACE (CLI) USAGE

Command Line Interface, CLI – is a tool for managing and monitoring the system, based on text commands. You can access the CLI using a direct connection via a serial interface, or using a remote logical connection using Telnet or SSH.

This section describes CLI syntax, symbols and modes.

5.1 Command syntax

A command is one or several words that can be accompanied by one or several parameters. Parameters can be mandatory and optional.

Some commands, such as `show network` or `clear vlan` require no parameters. Another commands, such as `network parms`, require input values after the command. Parameter values should be entered in a certain order: mandatory first, then optional parameters. So, following example shows `network params` command syntax:

`network parms ipaddr netmask` *`[gateway]`*

`network parms` – command name.

`ipaddr and netmask` – mandatory parameters, which are the values that must be entered after entering the command keywords.

`[gateway]` – optional parameter, which is not mandatory for command execution.

The *CLI Command Reference* contains a list of commands (sorted by command name) and provides a brief description of each command. Command description also contains following information:

- 'Format' – command keywords, the required and optional parameters.
- 'Command entry mode' – a command entry mode in which access to this command appears.
- 'Default value' – default configuring settings value (if exist) on this device.

Description of `show` commands also contains an indication of the information displayed by each such command.

5.2 Symbols in command description

Command parameters can include required and optional values, as well as a list of keywords. Parameters are entered in a specific order. Table 5.1 describes the conventions used in this document to distinguish between types of values.

Table 5.1 - Parameter symbols

Symbol	*Example*	*Description*
[] square brackets	`[value]`	Optional parameter.
parameter written in italic.	`value or [value]`	Variable value. Instead of the text in italics and brackets, you must enter the corresponding value (name or number).
{} braces	`{choice1 | choice2}`	`You need to select` a parameter from the list of options.
| Vertical bar	`choice1 | choice2`	Mutually exclusive options.
[{}] Braces in the square brackets	`[{choice1 | choice2}]`	Selection of an optional element from the proposed.

5.3 General parameter values

Parameter values can be names (sequences of letters) or numbers. When using a space as part of a parameter, enclose the value in double quotes. For example, the system will consider spaces if you use the 'System Name with Spaces' expression. The user may not specify empty sequences (''). Table 5.2 describes the general values of parameters and rules for setting the format of values.

Table 5.2 - Parameter description

Parameter	*Description*
ipaddr	Permissible IP address. IP address can be specified in the following ways: a (32 bit) a.b (8.24 bit) a.b.c (8.8.16 bit) a.b.c.d (8.8.8.8) In addition to the above formats, CLI allows decimal, hexadecimal and octal input formats (where n is any real hexadecimal, octal or decimal number), implemented as follows: 0xn (CLI assumes hexadecimal format.) 0n (CLI assumes octal format with leading zeros.) n (CLI assumes decimal format.)
ipv6-address	FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or FE80:0:0:0:20F:24FF:FEBF:DBCB,or FE80::20F24FF:FEBF:DBCB,or FE80:0:0:0:20F:24FF:128:141:49:32
Interface or unit/slot/port	Permissible slot and port numbers, divided by slash. For example 0/1 means slot number 0 and port number 1.
Logical interface	Slot and port logical number. Applicable for an aggregated interface (LAG). Logical unit/slot/port can be used to configure an aggregated interface.
Symbol sequences	Double quotes are used to form a sequence of characters, for example, “System Name with Spaces”. An empty sequence (“”) is not allowed.

5.4 Unit/slot/port, naming rules

The software accesses physical objects (maps and ports) using the `unit/slot/port` naming rule. The software also uses this abbreviation to identify certain logical objects, such as an aggregate-type logical interface.

The slot number can be used in two ways. When accessing a physical port, it identifies the map containing the ports. When accessing a logical port and CPU port, it also identifies the type of interface or port.

Table 5.3 - Slot types

Slot type	*Description*
Numbers of physical slots	Numbers of physical slots start from zero and are assigned before reaching the maximum number of physical slots.
Numbers of logical slots	Logical slots follow the physical slots and identify the logical aggregate interface (LAG) or router interfaces. The value of the logical slot number depends on the type of logical interface and may vary depending on the platform.
Numbers of CPU slots	CPU slots immediately follow the logical slots.

The port defines either the physical port of the device or the logical interface that is controlled in this slot.

Table 5.4 - Port types

Port type	*Description*
Physical ports	The physical ports for each slot are sequentially numbered, starting from one. This way, port 1 on slot 0 (internal port) for a switch in offline mode (out of stack) is 1/0/1, port 2 is 1/0/2, port 3 is 1/0/3, etc.
Logical interfaces	Link Aggregation Group (LAG) interfaces are logical interfaces that are used only for traffic switching functions. VLAN routing interfaces are used only for routing functions. Loopback interfaces - logical interfaces that are always enabled. Tunnel interfaces are logical point-to-point (p2p) connections that pass encapsulated packets.
CPU ports	The CPU ports are processed by the driver as one or more physical objects located on the physical slots.

The CLI does not use the unit/slot/port format for loopback and tunnel interfaces. Use loopback identifier to set the loopback interface. Use tunnel identifier to set the tunnel interface.

5.5 The use of a negative form of commands

The `no` keyword is a negative form of an existing command and is not an independent command. Almost every configuration command has a negative form. It is mainly used to cancel the command or return to the default value. For example, the `no shutdown` configuration command cancels interface shutdown. Use the command without the `no` keyword to re-enable the disabled option or activate the option disabled by default. The negative form is available only for configuration commands.

5.6 The use of the show command

All commands for viewing the operational state of the device (show commands) are executed in any configuration mode (global configuration modes, interface configuration, VLAN configuration, etc.). Show commands provide information about the system and features of a particular configuration, its state and statistics. Previously, show commands were available only in user or privileged modes.

5.7 CLI output filtering

Many CLI Show commands display significant amounts of data, which can make it difficult to find the information you want. The 'CLI output filtering' feature allows the user to additionally specify output filtering parameters when executing the 'show display' CLI commands in order to output only the necessary information. The point is to reduce the amount of data displayed on the display and simplify the search for information of interest to the user.

The main CLI output filtering features:

- Pagination management
  - Pagination enabling/disabling for all CLI viewer commands support. When the feature is disabled, the entire data set is output. When the function is enabled, the data is displayed on a page-by-page basis, in order to view further information, it is necessary to press a key. At the end of each page, --More-- (Next) or (q)uit (Q, exit) is displayed.
  - When paginated output is enabled: press Enter to advance one line; press 'q' or 'Q' to cancel paginated output; press any other key to go to the next page. You cannot change these keys.

Some show commands already support the paging function, some do not, and it does not apply to all commands.

- Data output filtering
  - Control the data display on the grep principle to display the desired information.
    - Filter the displayed data by including only rows containing the specified sequence.
    - Filter the displayed data by excluding rows containing the specified sequence.
    - Filter the displayed data by including only the lines that include the specified sequence, and all following them.
    - Filter the displayed data by including the specified output content section (for example, 'interface 0/1') with a configurable delimiter.
    - When finding a sequence, the register is not considered.
    - The enabled pagination also applies to output filtering.

5.8 Software modules

The software consists of many independent modules that can be combined in an arbitrary combination to develop advanced 2/3/4+ products. Commands and command entry modes available on your switch depend on the installed modules. In addition, for some show commands, the output fields may vary depending on the modules included in a particular assembly.

The software package includes the following modules:

- Commutation (level 2)
- Routing (level 3)
- IPv6 routing
- Multicast
- BGP-4
- Quality of Services (QoS)
- Management (CLI, Web UI and SNMP)
- IPv6 management — allows you to control the device via the IPv6 protocol (does not require an IPv6 routing module in the system). The IPv6 management address can be associated with a network port (front panel ports of the switch), a VLAN interface, and a service port.
- Metro
- Stacking
- Data processing and storage center (DataCenter)
- Secure Management

Some modules are not available for some platforms or software versions.

5.9 Command mode

CLI commands are grouped by input mode according to the command function. Each of the command entry modes supports specific software commands. Commands of one mode or another will not be available until you switch to this mode, except user mode commands. You can execute the User mode commands in the Privileged mode.

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

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

Table 5.5 - CLI Command Modes

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

Interface Config	`Switch (Interface` *`unit/slot/ port`*`)#`
	`Switch (Interface Loopback id)# Switch (Interface Tunnel id)#`
	`Switch (Interface unit/slot/port (startrange)-unit/slot/ port(endrange)#`
	`Switch (Interface lag` *`lag-intf-num`*`)#`
	`Switch (Interface vlan` *`vlan-id`*`)#`
		Manages the operation of an interface and provides access to the router interface configuration commands.
		Use this mode to set up a physical port for a specific logical connection operation.
		You can also use this mode to manage the operation of a range of interfaces. For example the prompt may display as follows:
		Switch (Interface 1/0/1-1/0/4) #
		Enters LAG Interface Config for the specified LAG.
		Enters VLAN routing Interface Config for the specified VLAN ID.

Line Console	`Switch (config-line)#`	Contains commands to configure outbound telnet settings and console interface settings, as well as to configure console login/enable authentication.
Line SSH	`Switch (config-ssh)#`	Contains commands to configure SSH login/enable authentication.
Line Telnet	`Switch (config-telnet)#`	Contains commands to configure telnet login/enable authentication.
IAS AAA user configuration	`Switch (Config-IAS-User)#`	Allows password configuration for a user in the IAS database.
Mail server configuration	`Switch (Mail-Server)#`	Allows configuration of the email server.
Policy Map configuration	`Switch (Config-policy-map)#`	Contains the QoS Policy-Map configuration commands.
Policy Class configuration	`Switch (Config-policy-class-map)#`	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map configuration	`Switch (Config-class-map)#`	Contains the QoS class map configuration commands

		for IPv4.
Ipv6_Class-Map configuration	`Switch (Config-class-map)#`	Contains the QoS class map configuration commands for IPv6.
OSPF router configuration	`Switch (Config-router)#`	Contains the OSPF configuration commands.
OSPFv3 router configuration	`Switch (Config rtr)#`	Contains the OSPFv3 configuration commands.
Router RIP Config	`Switch (Config-router)#`	Contains the RIP configuration commands.
BGP Router Config	`Switch (Config-router)#`	Contains the BGP4 configuration commands.
Route map configuration	`Switch (config-route-map)#`	Contains the route map configuration commands.
IPv6 VRF Address Family Config	`Switch (Config-router-af)#`	Contains the IPv6 address family configuration commands.
Peer Template Config	`(Config-rtr-tmplt)#`	Contains the BGP peer template configuration commands.
RADIUS Dynamic Authorization Config	`(Config-radius-da)`	Contains the Radius Dynamic Authorization commands.
MAC Access-list Config	`Switch (Config-mac-access-list)#`	Allows you to create a MAC ACL and to enter the mode containing MAC ACL configuration commands.
IPv4 Access-list Config	`Switch (Config-ipv4-acl)#`	Allows you to create an IPv4 named or extended Access-List and to enter the mode containing IPv4 Access-List configuration commands.
IPv6Access-list Config	`Switch (Config-ipv6-acl)#`	Allows you to create an IPv6 Access-List and to enter the mode containing IPv6 Access-List configuration commands.
Management Access-list Config	`Switch (config-macal)#`	Allows you to create an Management Access-List and to enter the mode containing Management Access-List configuration commands.
TACACS Config	`Switch (Tacacs)#`	Contains commands to configure properties for the TACACS servers
User-Group Configuration Mode	`Switch (config-usergroup)`	Contains user group commands
Task-Group Configuration Mode	`Switch (config-taskgroup)`	Contains task group commands
DHCP Pool Config	`Switch (Config dhcp-pool)#`	Contains the DHCP server IP address pool configuration commands.
DHCPv6 Pool Config	`Switch (Config dhcp6-pool)#`	Contains the DHCPv6 server IPv6 address pool configuration commands.

Stack Global Config Mode	`Switch (Config stack)#`	Allows you to access the Stack Global Config Mode.
ARP Access-List Config Mode	`Switch (Config-arp-access-list)#`	Contains commands to add ARP ACL rules in an ARP Access List.
Support Mode	`Switch (Support)#`	Allows access to the support commands, which should only be used by the manufacturer's technical support personnel as improper use could cause unexpected system behavior and/or invalidate product warranty.

Table 5.6 explains how to enter or exit each mode. To exit a mode and return to the previous mode, enter exit. To exit to Privileged mode, press Ctrl+z.

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

Table 5.6 - CLI Mode Access and Exit

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

Interface Config	From the Global Config mode, enter:
	`interface unit/slot/port or`
	`interface loopback id or`
	`interface tunnel id`
	`interface unit/slot/port(startrange)-unit/slot/port(endrange)`
	`interface lag lag-intf-num`
	`interface vlan vlan-id`

Line Console	From the Global Config mode, enter `line console.`
Line SSH	From the Global Config mode, enter `line ssh.`
Line Telnet	From the Global Config mode, enter `line telnet.`
AAA IAS User Config	From the Global Config mode, enter `aaa ias-user username name`
Mail Server Config	From the Global Config mode, enter `mail-server address`
Policy-Map Config	From the Global Config mode, enter `policy-map`
Policy-Class-Map Config	From the Global Config mode, enter `class-map`, and specify the optional keyword

	ipv4 to specify the Layer 3 protocol for this class.
VPC	From the Global Config mode, enter vpc
IPv6-Class-Map Config	From the Global Config mode, enter class-map, and specify the optional keyword **ipv6** to specify the Layer 3 protocol for this class.
Router OSPF Config	From the Global Config mode, enter router ospf
Router OSPFv3 Config	From the Global Config mode, enter ipv6 router ospf
Router RIP Config	From the Global Config mode, enter router rip
BGP Router Config	From the Global Config mode, enter router bgp
Route Map Config	From the Global Config mode, enter route-map map-tag
IPv6 Address Family Config	BGP Router Config mode, enter address-family ipv6
Peer Template Config	From the BGP Router Config mode, enter template peer name to create a BGP peer template and enter Peer Template Configuration mode
MAC Access-list Config	From the Global Config mode, enter mac access-list extended name
IPv4 Access-list Config	From the Global Config mode, enter ip access-list *name*
IPv6 Access-list Config	From the Global Config mode, enter ipv6 access-list *name*
Management Access-list Config	From the Global Config mode, enter management access-list name
TACACS Config	From the Global Config mode, enter tacacs-server host ip-addr, where ip-addr is the IP address of the TACACS server on your network.
User-Group Configuration Mode	From the Global Config mode, enter the usergroup <usergroup-name> command.
Task-Group Configuration Mode	From the Global Config mode, enter the taskgroup <taskgroup-name> command.
DHCP Pool Config	From the Global Config mode, enter the ip dhcp pool pool-name command.
DHCPv6 Pool Config	From the Global Config mode, enter the ipv6 dhcpv6 pool pool-name command.
Stack Global Config Mode	From the Global Config mode, enter the stack command.
ARP Access-List Config Mode	From the Global Config mode, enter the arp access-list command.
Support Mode	From the Privileged mode, enter support The **support** command is available only if the **techsupport enable** command has been issued.

5.10 Command completion and abbreviation

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

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

5.11 CLI error messages

If you enter a command and the system is unable to execute it, an error message appears. Table 5.7 describes the most common CLI error messages.

Table 5.7 - CLI Error Messages

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

5.12 CLI Line-Editing conventions

Table **5.8** describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering `help` from the User or Privileged modes.

Table 5.8 - CLI Editing Conventions

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

Exit	Go to next lower command prompt.
?	List available commands, keywords, or parameters.

5.13 Using CLI \help

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

```
(switch) >?

enable                        Enter into user privilege mode.
help                          Display help for various special keys.
logout                        Exit this session. Any unsaved changes are lost.
password                      Change an existing user’s password.
ping                          Send ICMP echo packets to a specified IP address.
quit                          Exit this session. Any unsaved changes are lost.
show                          Display Switch Options and Settings.
telnet                        Telnet to a remote host.
```

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

```
(switch) #network ?

ipv6                          Configure IPv6 parameters for system network.
javamode                      Enable/Disable.
mac-address                   Configure MAC Address.
mac-type                      Select the locally administered or burnedin MAC address.
mgmt_vlan                     Configure the Management VLAN ID of the switch.
parms                         Configure Network Parameters of the device.
protocol                      Select DHCP, BootP, or None as the network config protocol.
```

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

```
(Routing) #network parms ?

<ipaddr>                      Enter the IP Address.
none                          Reset IP address and gateway on management interface
```

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

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

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

```
(switch) #show m?

mac                       mac-addr-table            mac-address-table
mail-server               mbuf                      monitor
```

5.14 Accessing the CLI

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

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP or DHCP server on your network. For more information, see section 'Remote control interface configuration commands'.

5.15 F button software management

reset-button enable

F Button Software Activation By holding the F button for 10 seconds, you can reset the device configuration to the factory settings.

Default: Enabled

Format `reset-button enable`

Command Mode: Global Config Mode

reset-button disable

Software deactivation of the F button.

Default: Disabled

Format `reset-button disable`

Command Mode: Global Config Mode

no reset-button

Software activate the F button.

Format `no reset-button`

Command Mode Privileged Mode

reset-button reload-only

Software deactivation of the F button. After releasing the button, or after 10 seconds, a reboot will occur. The configuration will remain unchanged.

Default: Disabled

Format `reset-button reload-only`

Command Mode: Global Config Mode

no reset-button

Software activate the F button.

Format `no reset-button`

Command Mode Privileged Mode

6 BASIC SYSTEM OPERATION COMMANDS

This chapter describes the commands for operating with the system and monitoring settings available in the CLI.

The commands in this section can be divided into 2 functional groups:

- **Operational status commands (show commands) display switch settings, statistics, and other information.**
- **Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.**

6.1 AutoInstall commands

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

AutoInstall includes the following support:

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

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

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

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

boot autoinstall

Use this command to operationally start or stop the AutoInstall process on the switch. The command is non-persistent and is not saved in the startup or running configuration file.

Default: stopped

Format: `boot autoinstall {start | stop}`

Command mode: Privileged

boot host retrycount

Use this command to set the number of attempts to download a configuration file from the TFTP server.

Default: 3

Format: `boot host retrycount` *1-3*

Command mode: Privileged

no boot host retrycount

Use this command to set the number of attempts to download a configuration file to the default value.

Format: `no boot host retrycount`

Command mode: Privileged

boot host dhcp

Use this command to enable AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM.

Default: enabled

Format: `boot host dhcp`

Command mode: Privileged

no boot host dhcp

Use this command to disable AutoInstall for the next reboot cycle.

Format: `no boot host dhcp`

Command mode: Privileged

boot host autosave

Use this command to automatically save the downloaded configuration file to the startup-config file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to non-volatile memory by using the `write memory` or `copy system:running-config nvram:startup-config` command. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.

Default: disabled

Format: `boot host autosave`

Command mode: Privileged

no boot host autosave

Use this command to disable automatically saving the downloaded configuration on the switch.

Format: `no boot host autosave`

Command mode: Privileged

boot host autoreboot

Use this command to allow the switch to automatically reboot after successfully downloading an image. When auto reboot is enabled, no administrative action is required to activate the image and reload the switch.

Default: enabled

Format: `boot host autoreboot`

Command mode: Privileged

no boot host autoreboot

Use this command to prevent the switch from automatically rebooting after the image is downloaded by using the AutoInstall feature.

Format: `no boot host autoreboot`

Command mode: Privileged

erase startup-config

Use this command to erase the text-based configuration file stored in non-volatile memory. If the switch boots and no startup-config file is found, the AutoInstall process automatically begins.

Format: `erase startup-config`

Command mode: Privileged

erase factory-defaults

Use this command to erase the text-based factory-defaults file stored in non-volatile memory.

Default: disabled

Format: `erase factory-defaults`

Command mode: Privileged

show autoinstall

This command displays the current status of the AutoInstall process.

Format: `show autoinstall`

Command mode: Privileged

copy <url> backup

Upload a new backup software image. The device is loaded from a file of system software, which is stored in flash memory. When updating a new system software file is stored in a dedicated memory area.

Default: Disabled

Format `copy<tftp|ftp|scp|sftp|usb://<ipaddr>/<filepath>/<filename>> |xmodem | ymodem | zmodem | backup`

Command Mode: Privileged Mode

boot system backup

Switch to backup image after reboot**.** When booting, the device launches the active system software file.

Default: Disabled

Format `boot system backup`

Command Mode: Privileged Mode

exception protocol

Use this command to specify the protocol used to store the coredump file. Only up to 4 coredump files can be stored locally.

Default: Disabled

Format `exception protocol {nfs| tftp | ftp | local | usb | none}`

Command Mode: Global Config Mode

no exception protocol

Disable the coredump file save.

Default: Disabled

Format `exception protocol {nfs| tftp | ftp | local | usb | none}`

Command Mode: Global Config Mode

exception switch-chip-register

Enables saving when the switch registers dump crashes. The dump is saved separately to the reg_core_ <timestamp> .x. {Bz2, bin} file. The registration of the dump is taken only for the master device, not for backup.

Default: Disabled

Format `exception switch-chip-register {enable | disable}`

Command Mode: Global Config Mode

exception dump stack-ip-address protocol

This command configures the protocol (dhcp or static) that will be used to configure the service port when the device crashes. If it is configured as dhcp, then the device receives an IP address from the dhcp server available on the network.

Default: Disabled

Format `exception dump stack-ip-address protocol {dhcp | static}`

Command Mode: Global Config Mode

no debug crashlog verbose

Disable the generation of file about threads and system.

Default value	Disabled
Format	`copy nvram:errorlog <tftp|ftp|scp|sftp|usb://<ipaddr>/<filepath>/<filename>> |xmodem | ymodem | zmodem`
Command Mode:	Global Config Mode

6.2 CLI Output Filtering

show xxx|include "string"

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

show xxx|include "string" exclude "string2"

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

show xxx|exclude "string"

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

show xxx|begin "string"

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

show xxx|section "string"

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

show xxx|section "string" "string2"

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

show xxx|section "string" include "string2"

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

show xxx|no-more

The command ***xxx*** is executed and the output results are displayed in the console not in portions, but in full, without the need to press additional keys to fully display the necessary information.

6.3 Firmware operation commands

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

delete

This command deletes the backup image file from the permanent storage or the core dump file from the local file system. The optional unit parameter is valid only on Stacks. Error will be returned, if this parameter is provided, on Standalone systems. In a stack, the unit parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format: `delete [unit] backup`
`delete core-dump-file file-name | all`

Command mode: Privileged

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. If the specified image doesn't exist on the system, this command returns an error message. The optional *unit* parameter is valid only in Stacking, where the *unit* parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format: `boot system [unit] {active | backup}`

Command mode: Privileged

show bootvar

This command displays the version information and the activation status for the current active and backup images on the supplied unit (node) of the Stack. If you do not specify a unit number, the command displays image details for all nodes on the Stack. The command also displays any text description associated with an image. This command, when used on a Standalone system, displays the switch activation status. For a standalone system, the *unit* parameter is not valid.

Format: `show bootvar [unit]`

Command mode: Privileged

filedescr

This command associates a given text description with an image. Any existing description will be replaced. The command is executed on all nodes in a Stack.

Format: `filedescr {active | backup} text-description`

Command mode: Privileged

6.4 System information and statistics output

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

load-interval

This command changes the length of time for which data is used to compute load statistics. The value is given in seconds, and must be a multiple of 30. The allowable range for *interval* is from 30 to 600 seconds. The smaller the value of the load interval is, the more accurate is the instantaneous rate given by load statistics. Smaller values may affect system performance.

Default: 300 seconds

Format: `load-interval` *interval*

Command mode: Interface Config

no load-interval

This command resets the load interval on the interface to the default value.

Format: `no load-interval`

Command mode: Interface Config

show arp switch

This command displays the contents of the IP stack's Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces - network or service ports. ARP entries associated with routing interfaces are not listed.

Format: `show arp switch`
Command mode: Privileged

Term	*Value*
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is *Management*. For a network port, the output is the *unit/slot/port* of the physical interface.

show eventlog

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

Format: `show eventlog [`*unit*`]`

Command mode: Privileged

Term	*Value*
File	The file in which the event originated

Line	The line number of the event
Task ID	The task ID of the event.
Code	The event code
Time	The time this event occurred
Unit	The unit for the event

Event log information is retained across a switch reset.

show hardware

This command displays switch inventory information.

The show version command and the show hardware command display the same information. In future releases of the software, the show hardware command will not be available.

Format: `show hardware`

Command mode: Privileged

show version

This command displays switch inventory information.

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

Format: `show version`

Command mode: Privileged

Term	*Value*
System Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data
Machine Model	The machine model as defined by the Vital Product Data.
Serial Number	The unique box serial number for this switch.
FRU Number	The field replaceable unit number.
Part Number	Manufacturing part number.
Maintenance Level	Hardware changes that are significant to software.
Manufacturer	Manufacturer descriptor field.

Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.
Operating System	The operating system currently running on the switch.
Network Processing Device	The type of the processor microcode.
Additional Packages	The additional packages incorporated into this system.

show platform vpd

This command displays Vital Product Data (VPD) for the switch.

Format: `show platform vpd`

Command mode: User Privileged

The information presented below is displayed.

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

show interface

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

Format: `show interface {`*`unit/slot/port`* `| switchport | lag` *`lag-id`*`}`

Command mode: Privileged

Display parameters, when the argument is `unit/slot/port` or `lag`*`lag-id`*, are as follows:

Term	*Value*
Interface index	System interface identifier
Hardware	Interface type
Interface MTU	Maximum MTU supported on this interface
Link type	Interface bandwidth and duplex status. If the argument is lag the following information will be displayed: • Link aggregation type • No. of members in this port-channel • No. of active members in this port-channel • Active LAG bandwidth • Member list

Media type	The media type of the interface. Not displayed for the LAG interface.
Link downs	The number of transitions to the Down state. Does not take into account the transitions by the shutdown command. Not displayed for the LAG interface.
Time since counters last cleared	The time since the statistics for this interface were last cleared.
Flow control	The status of the Flow Control on the interface. Not displayed for the LAG interface.
Input rate	The average rate of incoming flow for a specified time interval (Load Interval)
Output rate	The average rate of outgoing flow for a specified time interval (Load Interval)
Packets input	The number of incoming packets
Bytes received	The number of received data, in bytes
Oversize errors	The number of packets received by the interface, exceeding the maximum allowable MTU
Internal MAC errors	The number of packets received with errors
Broadcast frames	The total number of broadcast packets received and transmitted by this interface
Multicast frames	The total number of multicast packets received and transmitted by this interface
Total input errors	The total number of packets received with errors
FCS errors	The number of received packets with checksum errors and an integer number of octets
Alignment errors	The number of received packets with checksum errors and a decimal number of octets
Pause frames received	The number of received requests to stop streaming
Snmp input frames discarded	The number of dropped incoming SNMP packets
Packets output	The number of outgoing packets
Bytes sent	The number of transmitted data, in bytes
Broadcast errors	The total number of broadcast packets received and transmitted with errors by this interface
Multicast errors	The total number of multicast packets received and transmitted with errors by this interface
Output errors	The total number of packets transmitted with errors
Total collisions	The total number of collisions
Excessive collisions	The total number of characters transmitted with collisions
Late collisions	The number of packets transmitted with collisions on the final stages of transmission

Pause frames transmitted	The number of sent requests to stop streaming
Snmp out frames discarded	The number of dropped outgoing SNMP packets
Output queues	QoS statistics for outgoing interface queues (forwarded/dropped). Not displayed for the LAG interface.

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

Term	*Value*
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because oferrors.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interfaces status

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

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

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

Command mode: Privileged

Field	*Description*
Port	The interface associated with the rest of the data in the row.
Name	The descriptive user-configured name for the interface.
Admin Mode	Port Administration status
Link State	Port Operation status

Physical Mode	The speed and duplex settings on the interface.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. The physical status for LAGs is not reported. When a port is down, the physical status is unknown.
Media type	The media type of the interface.
Flow Control Status	The 802.3x flow control status.
Flow control	The configured 802.3x flow control mode.

show interfaces traffic

Use this command to display interface traffic information.

Format: `show interfaces traffic [`*`unit/slot/port`*`]`
Command mode: Privileged

Field	*Description*
Interface Name	The interface associated with the rest of the data in the row
Queue	Number of queue
Total Pass (Pkts)	The total number of packets transmitted for the specified queue
Congestion Drops	The number of packets that have been dropped on the interface due to congestion.
TX Queue	The number of cells in the transmit queue.
RX Queue	The number of cells in the receive queue
Color Drops: Yellow	The number of yellow (conformed) packets that were dropped.
Color Drops: Red	The number of red (exceeded) packets that were dropped
WRED TX Queue	The number of packets in the WRED transmit queue.

show interface counters

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

Format: `show interface counters`
Command mode: Privileged

Field	*Description*
Port	The interface associated with the rest of the data in the row.
InOctects	The total number of octets received on the interface.
InUcastPkts	The total number of unicast packets received on the in-

	terface.
InMcastPkts	The total number of multicast packets received on the interface.
InBcastPkts	The total number of broadcast packets received on the interface.
OutOctects	The total number of octets transmitted by the interface.
OutUcastPkts	The total number of unicast octets transmitted by the interface.
OutMcastPkts	The total number of multicast octets transmitted by the interface.
OutBcastPkts	The total number of broadcast octets transmitted by the interface.

show interfaces description

This command displays the description of the interfaces, their administrative and current status.

Format: `show interfaces description {unit/slot/port | all | lag | vlan}`

Command mode: Privileged

show interface ethernet

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

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

Command mode: Privileged

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

Term	*Value*
Packets Received	**Total Packets Received (Octets).** The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. **Packets Received 64 Octets.** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). **Packets Received 65–127 Octets.** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding

	framing bits but including FCS octets). **Packets Received 128–255 Octets.** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Received 256–511 Octets.** The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Received 512–1023 Octets.** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Received 1024–1518 Octets.** The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Received > 1518 Octets.** The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. **Packets RX and TX 64 Octets.** The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). **Packets RX and TX 65–127 Octets.** The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). **Packets RX and TX 128–255 Octets.** The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). **Packets RX and TX 256–511 Octets.** The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). **Packets RX and TX 512–1023 Octets.** The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). **Packets RX and TX 1024–1518 Octets**. The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). **Packets RX and TX 1519–2047 Octets.** The total number of packets received and transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. **Packets RX and TX 1523–2047 Octets.** The total number

	of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. **Packets RX and TX 2048–4095 Octets**. Number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	**Packets RX and TX 4096–9216 Octets.** The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. **Total Packets Received Without Error.** The total number of packets received that were without errors. **Unicast Packets Received.** The number of subnetwork-unicast packets delivered to a higher-layer protocol. **Multicast Packets Received.** The total number of good packets received that were directed to a multicast address. Note. This number does not include packets directed to the broadcast address. **Broadcast Packets Received.** The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets
Receive Packets Discarded	Note that this does not include multicast packets. The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Received with MAC Errors	**Total Packets Received with MAC Errors.** The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. **Jabbers Received.** The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). **Note** This definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. **Fragments/Undersize Received.** The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). **Alignment Errors.** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-

	integral number of octets. **FCS Errors.** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. **Overruns.** The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Received Packets Not Forwarded	**Total Received Packets Not Forwarded.** A count of valid frames received which were discarded (in other words, filtered) by the forwarding process. 802.3x Pause Frames Received. A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode Unacceptable Frame Type. The number of frames discarded from this port due to being an unacceptable frame type.
Packets Transmitted Octets	**Total Packets Transmitted (Octets).** The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. **Packets Transmitted 64 Octets.** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). **Packets Transmitted 65–127 Octets.** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Transmitted 128–255 Octets.** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Transmitted 256–511 Octets.** The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Transmitted 512–1023 Octets.** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Transmitted 1024–1518 Octets.** The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Transmitted > 1518 Octets.** The total number of packets transmitted that were longer than 1522 oc-

	tets (excluding framing bits, but including FCS octets) and were otherwise well formed. **Max Frame Size.** The maximum size of the Info (non-MAC) field that this port will receive or transmit. **Maximum Transmit Unit.** The maximum Ethernet payload type.
Packets Transmitted Successfully	**Total Packets Transmitted Successfully.** The number of frames that have been transmitted by this port to its segment. Unicast Packets Transmitted. The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. **Multicast Packets Transmitted.** The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent. **Broadcast Packets Transmitted.** The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Errors	**Total Transmit Errors.** The sum of Single, Multiple, and Excessive Collisions. FCS Errors. The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets Underrun Errors. The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission
Transmit Discards	**Total Transmit Packets Discards.** The total number of frames rejected due to single and multiple collisions, as well as redundant packets. **Single Collision Frames.** The counter of the number of frames successfully transmitted via a specific interface, the transmission of which was suspended due to a single collision. **Multiple Collision Frames.** The counter of the number of frames successfully transmitted via a specific interface, the transmission of which was suspended due to a several collisions. **Excessive Collisions.** The counter of the number of frames that can not be transmitted through a specific interface due to frequent collisions. **Port Membership Discards.** The number of frames re-

	jected at the output of this port due to filtering enabled. **Total Transmit Packets Discards.** The total number of frames rejected due to single and multiple collisions, as well as redundant packets. **Single Collision Frames.** The counter of the number of frames successfully transmitted via a specific interface, the transmission of which was suspended due to a single collision. **Multiple Collision Frames.** The counter of the number of frames successfully transmitted via a specific interface, the transmission of which was suspended due to a several collisions. **Excessive Collisions.** The counter of the number of frames that can not be transmitted through a specific interface due to frequent collisions. **Port Membership Discards.** The number of frames rejected at the output of this port due to filtering enabled.
Protocol Statistics	**802.3x Pause Frames Transmitted.** A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode **GVRP PDUs Received.** The count of GVRP PDUs received in the GARP layer. **GVRP PDUs Transmitted.** The count of GVRP PDUs transmitted from the GARP layer. **GVRP Failed Registrations.** The number of times attempted GVRP registrations could not be completed. **GMRP PDUs Received.** The count of GMRP PDUs received in the GARP layer. **GMRP PDUs Transmitted.** The count of GMRP PDUs transmitted from the GARP layer. **GMRP Failed Registrations.** The number of times attempted GMRP registrations could not be completed. **STP BPDUs Transmitted.** Spanning Tree Protocol Bridge Protocol Data Units sent. **STP BPDUs Received.** Spanning Tree Protocol Bridge Protocol Data Units received. **RST BPDUs Transmitted.** Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. **RSTP BPDUs Received.** Rapid Spanning Tree Protocol Bridge Protocol Data Units received. **MSTP BPDUs Transmitted.** Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. **MSTP BPDUs Received.** Multiple Spanning Tree Protocol Bridge Protocol Data Units received. **SSTP BPDUs Transmitted.** Shared Spanning Tree Protocol Bridge Protocol Data Units sent. **SSTP BPDUs Received.** Shared Spanning Tree Protocol Bridge Protocol Data Units received.

Dot1x Statistics	**EAPOL Frames Transmitted.** The number of EAPOL frames of any type that have been transmitted by this authenticator. **EAPOL Start Frames Received.** The number of valid EAPOL start frames that have been received by this authenticator.
Traffic Load Statistics	**Load Interval.** The length of time for which data is used to compute load statistics. The value is given in seconds, and must be a multiple of 30. The allowable range is from 30 to 600 seconds. **Bits Per Second Received.** Approximate number of bits per second received. This value is an exponentially weighted average and is affected by the configured load- interval. This value is an exponentially weighted average and is affected by the configured load-interval. **Bits Per Second Transmitted.** Approximate number of bits per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval. **Packets Per Second Received.** Approximate number of packets per second received. This value is an exponentially weighted average and is affected by the configured load-interval. **Packets Per Second Transmitted.** Approximate number of packets per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval. **Percent Utilization Received.** Value of link utilization in percentage representation for the RX line. **Percent Utilization Transmitted.** Value of link utilization in percentage representation for the TX line.
Time since counters last cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

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

Term	*Value*
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets
Packets Received With Error	The total number of packets with errors (including broadcast packets and multicast packets) received by the processor.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent

Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Time since counters last cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared

If you use the `all` keyword, the following information appears for all interfaces on the switch.

Term	*Value*
Port	The Interface ID.
Bytes Tx	The total number of bytes transmitted by the interface.
Bytes Rx	The total number of bytes received by the interface.
Packets Tx	The total number of packets transmitted by the interface.
Packets Rx	The total number of packets received by the interface.
Utilization Tx (%)	Total load of transfer interface for the `load interval`
Utilization Rx (%)	Total load of receiving interface for the `load interval`

show interface ethernet switchport

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

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

Command mode: Privileged

The command displays the following information

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

show fiber-ports optical-transceiver

This command displays the diagnostics information of the SFP like: Temp, Voltage, Current, Input Power, Output Power, Tx Fault, and LOS. The values are derived from the SFP's A2 (Diagnostics) table using the I2C interface.

Format: `show fiber-ports optical-transceiver {all |` *`unit/slot/port`*`}`

Command mode: Privileged

Field	*Description*
Temp	Internally measured transceiver temperature
Voltage	Internally measured supply voltage

Current	Measured TX bias current.
Output Power	Measured optical output power relative to 1mW.
Input Power	Measured optical power received relative to 1mW.
TX Fault	Transmitter fault
LOS	Loss of signal.

show fiber-ports optical-transceiver-info

This command displays the SFP vendor related information like Vendor Name, Serial Number of the SFP, Part Number of the SFP. The values are derived from the SFP's A0 table using the I2C interface.

Format: `show fiber-ports optical-transceiver-info {all | slot/port}`

Command mode: Privileged

Field	*Description*
Vendor Name	The vendor name is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h). The vendor name shall be the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.
Length (50um, OM2)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 50 micron multimode OM2 [500MHz*km at 850nm] fiber. A value of zero means that the transceiver does not support 50 micron multimode fiber or that the length information must be determined from the transceiver technology.
Length (62.5um, OM1)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 62.5 micron multimode OM1 [200 MHz*km at 850nm, 500 MHz*km at 1310nm] fiber. A value of zero means that the transceiver does not support 62.5 micron multimode fiber or that the length information must determined from the transceiver technology
Vendor SN	The vendor serial number (vendor SN) is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h), defining the vendor's serial number for the transceiver. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified.
Vendor PN	The vendor part number (vendor PN) is a 16-byte field that contains ASCII characters, left aligned and added on the right with ASCII spaces (20h), defining the vendor part number or product name. A value of all zero in the 16- byte field indicates that the vendor PN is unspecified.

BR, nominal	The nominal bit (signaling) rate (BR, nominal) is specified in units of 100 MBd, rounded off to the nearest 100 MBd. The bit rate includes those bits necessary to encode and delimit the signal as well as those bits carrying data information. A value of 0 indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate will depend on the encoding of the data, as defined by the encoding value.
Vendor Rev	The vendor revision number (vendor rev) contains ASCII characters, left aligned and padded on the right with ASCII spaces (20h), defining the vendor's product revision number. A value of all zero in this field indicates that the vendor revision is unspecified.

show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter `all` or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the `count` parameter to view summary information about the forwarding database table. Use the `interface unit/slot/port` parameter to view MAC addresses on a specific interface.

Instead of `unit/slot/port`, `lag`*`lag-intf-num`* can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number. Use the `vlan`*`vlan_id`* parameter to display information about MAC addresses on a specified VLAN.

Format: `show mac-addr-table [{`*`macaddr vlan_id`* `| all | count | interface {`*`unit/slot/port`* `| lag` *`lag-id`* `| vlan` *`vlan_id`*`} }]`

Command mode: Privileged

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

Field	*Description*
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Interface	The port through which this address was learned.
Interface index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: **Static** — The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. **Learned** — The value of the corresponding instance was

	learned by observing the source MAC addresses of incoming traffic, and is currently in use. **Management** — The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface and is currently used when enabling VLANs for routing. **Self** — The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address). **GMRP Learned** — The value of the corresponding was learned via GMRP and applies to Multicast. **Other** — The value of the corresponding instance does not fall into one of the other categories.

If you enter vlan vlan_id, only the MAC Address, Interface, and Status fields appear. If you enter the `interface`

unit/slot/port parameter, in addition to the MAC Address and Status fields, the VLAN ID field also appears. The following information displays if you enter the count parameter:

Fields	*Description*
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle

process cpu threshold

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

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

Command mode: Global Config

Field	*Description*
rising threshold	The percentage of CPU resources that, when exceeded for the configured rising interval, triggers a notification. From 1 to 100%. Default value — 0 (disabled).
rising interval	The duration of the CPU rising threshold violation, in seconds, that must be met to trigger a notification. From 5 to 86400 seconds. Default value — 0 (disabled).

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

show process app-list

This command displays the user and system applications.

Format: `show process app-list`

Command mode: Privileged

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

show process app-resource-list

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

Format: `show process app-resource-list`

Command mode: Privileged

Parameter	*Description*
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.

Memory Limit	The maximum amount of memory the process can consume.
CPU Share	The maximum percentage of CPU utilization the process can consume
Memory Usage	The amount of memory the process is currently using.
Max Mem Usage	The maximum amount of memory the process has used at any given time since it started.

show process cpu

This command provides the percentage utilization of the CPU by different tasks.

It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

Format: `show process cpu [1-n | all]`

Command mode: Privileged

Keyword	*Description*
Free	System wide free memory.
Alloc	System wide allocated memory (excluding cache, file system used space).
Pid	Process or Thread Id.
Name	Process or Thread Name.
5Secs	CPU utilization sampling in 5Secs interval.
60Secs	CPU utilization sampling in 60Secs interval.
300Secs	CPU utilization sampling in 300Secs interval.
Total CPU Utilization	Total CPU utilization % within the specified window of 5Secs, 60Secs and 300Secs.

show process proc-list

This application displays the processes started by applications created by the Process Manager.

Format: `show process proc-list`

Command mode: Privileged

Parameter	*Description*
PID	The number the software uses to identify the process.
Process Name	The name that identifies the process.
Application ID- Name	The application identifier and its associated name.

Child	Indicates whether the process has spawned a child process.
VM Size	Virtual memory size.
VM Peak	The maximum amount of virtual memory the process has used at a given time.
FD Count	The file descriptors count for the process.

show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the `all` option.

Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional scriptname is provided with a file name extension of .scr, the output is redirected to a script file.

If you issue the show running-config command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

If you use a text-based configuration file, the show running-config command only displays configured physical interfaces (i.e. if any interface only contains the default configuration, that interface will be skipped from the show running-config command output). This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its exit command, are both omitted from the show running-config command output (and hence from the startup-config file when the system settings are saving).

Use the following keys to navigate the command output.

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

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

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

Command mode: Privileged

show running-config interface

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

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

Command mode: Privileged

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

The following information is displayed for the command.

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

show

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

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

Command mode: Privileged

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

dir

Use this command to list the files saved in the flash.

Format: `dir`

Command mode: Privileged

show sysinfo

This command displays switch information.

Format: `show sysinfo`

Command mode: Privileged

Term	*Value*
System Description	Text used to identify this switch.
System Name	Name used to identify the switch. The factory default is blank.
System Location	Text used to identify the location of the switch. The factory default is blank.
System Contact	Text used to identify a contact person for this switch. The factory default is blank.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
Current SNTP Synchronized Time	The system time acquired from a network SNTP server.
MIBs Supported	A list of MIBs supported by this agent.

show tech-support

Use the `show tech-support` command to display system and configuration information when you contact technical support. The output of the `show tech-support` command combines the output of the following commands and includes log history files from previous runs:

If one of the optional parameters [bgp|dot1q|dot1s|dot3ad|file|isdp|layer3|link_dependency| |lldp|log|routing|sim|stacking|switching|system] is specified in the command, then the output displays some information from the full output of show tech-support only for the specified parameter.

- `show version`
- `show version`
- `show bootvar`
- `show switch`
- `show environment`
- `show running-config`
- `show serviceport`
- `show process cpu`
- `show process proc-list`
- `show process memory`
- `show mbuf total`
- `show port all`
- `show interface ethernet all`
- `show fiber-ports optical-transceiver-info all`
- `show fiber-ports optical-transceiver all`
- `show interface all`

- show interfaces hardware profile
- show interfaces status err-disabled
- show interface debounce
- show mac-addr-table
- show mac-addr-table count
- show vlan brief
- show port-channel all
- show ip interface brief
- show ipv6 interface brief
- show arp
- show ip stats
- show ip route
- show routing heap summary
- show ip bgp summary
- show ip bgp neighbors
- show ip bgp statistics
- show ip bgp update-group
- show bgp ipv6 summary
- show bgp ipv6 neighbors
- show bgp ipv6 statistics
- show bgp ipv6 update-group
- show spanning-tree active
- show stack-port
- show stack-port counters all
- show stack-port diag all
- show logging
- show logging buffered
- show logging traplogs
- show lldp remote-device all
- show isdp neighbors
- show link state group

Format: show tech-support [bgp|dot1q|dot1s|dot3ad|file|isdp|layer3|
|link_dependency|lldp|log|routing|sim|stacking|switching|system]

Command mode: Privileged

length value

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

Default: 24

Format: length value

Command mode: Line configuration

no length value

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

Format: `no length value`

Command mode: Line configuration

terminal length

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

Default: 24 lines per page

Format: `terminal length value`

Command mode: Privileged

no terminal length

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

Format: `no terminal length value`

Command mode: Privileged

show terminal length

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

Format: `show terminal length`

Command mode: Privileged

memory free low-watermark processor

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

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

Command mode: Global Config

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

clear mac-addr-table

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

Default: none

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

Command mode: Privileged

Parameter	*Description*
all	Clears dynamically learned forwarding database entries in the forwarding database table.
vlan vlanId	Clears dynamically learned forwarding database entries for this vlanId.
interface unit/slot/port	Clears forwarding database entries learned on for the specified interface
macAddr **macMask**	Clears dynamically learned forwarding database entries that match the range specified by MAC address and MAC mask. When MAC mask is not entered, only specified MAC is removed from the forwarding database table.

6.5 Box Services commands

This section describes the Box Services commands. Box services are services that provide support for features such as temperature, power supply status, fan control, and others.

environment temprange

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

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

Command mode: Global Config

Parameter	*Value*
min	Sets the minimum allowed temperature for normal operation. Range of values: from –100°C to 100°C. Default: 0°C
max	Sets the maximum allowed temperature for normal operation. Range of values: from –100°C to 100°C. Default: 0°C

environment trap

Use this command to configure environment status traps.

Format: `environment trap {fan | powersupply | temperature}`
Command mode: Global Config

Parameter	*Value*
fan	Enables or disables the sending of traps for fan status events. Default: enabled
powersupply	Enables or disables the sending of traps for power supply status events. Default: enabled
temperature	Enables or disables the sending of traps for temperature status events. Default: enabled

show environment

This command displays information about system disk space and usage, temperature sensor readings, fan and power supply statuses.

Format: `show environment`
Command mode: Privileged

6.6 System Log configuration

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

logging buffered

This command enables logging to an in-memory log.

Default: enabled; notice level
Format: `logging buffered`
Command mode: Global Config

no logging buffered

This command disables logging to in-memory log.

Format: `no logging buffered`
Command mode: Global Config

logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default: enabled
Format: `logging buffered wrap`
Command mode: Privileged

no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format: `no logging buffered wrap`

Command mode: Privileged

logging cli-command

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

Default: disabled

Format: `logging cli-command`

Command mode: Global Config

no logging cli-command

This command disables the CLI command Logging feature.

Format: `no logging cli-command`

Command mode: Global Config

logging console

This command enables logging to the console. You can specify the severitylevel value as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

Default: enabled; info level

Format: `logging console [severitylevel]`

Command mode: Global Config

no logging console

This command disables logging to the console.

Format: `no logging console`

Command mode: Global Config

logging host

This command configures the logging host parameters. You can configure up to 8 hosts.

Default: port: 514 (for UDP) and 6514 (for TLS)

authentication mode: anonymous

certificate index: 0

level: critical (2)

Format: logging host {hostaddress | hostname} addresstype tls [anon|x509name] certificate-index {port severitylevel}

Command mode: Global Config

Parameter	*Description*
hostaddress| hostname	Syslog server IP address
address-type	Specifies the type of specified address: DNS or IPv4.
tls	Enables secured TLS protocol
anon|x509name	Authentication mode type: anonymous or x509name
certificate-index	The certificate number to be used for authentication. Valid value range: 0–8. Index 0 is used to the default file.
port	A port number from 1 to 65535
severitylevel	Specify this value as either an integer from 0 to 7, or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6) or debug (7)

logging host reconfigure

This command enables logging host reconfiguration.

Format: logging host reconfigure *hostindex*

Command mode: Global Config

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

logging host remove

This command disables logging to host. See the show logging hosts command for a list of host indexes.

Format: logging host remove *hostindex*

Command mode: Global Config

logging protocol

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

Default: Version 0 (RFC 3164).

Format: logging protocol {0|1}

Command mode: Global Config

logging syslog

This command enables syslog logging. Use the optional facility parameter to set the default facility used in syslog messages for components that do not have an internally assigned facility. The facility value can be 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. Default facility: local7.

Default: disabled

Format: `logging syslog [facility` *`facility`*`]`

Command mode: Global Config

no logging syslog

This command disables syslog logging.

Format: `no logging syslog [facility]`

Command mode: Global Config

logging syslog port

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

Default: disabled

Format: `logging syslog port` *`portid`*

Command mode: Global Config

no logging syslog port

This command disables syslog logging.

Format: `no logging syslog port`

Command mode: Global Config

logging syslog source-interface

This command configures the syslog source-interface (source IP address) for syslog server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

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

Command mode: Global Config

Parameter	*Description*
unit/slot/port	VLAN or port-based routing interface

loopback-id	Configures the loopback interface to use as the source IP address. The range of the loopback ID: from 0 to 7.
tunnel-id	Configures the tunnel interface to use as the source IP address. The range of the tunnel ID: from 0 to 7.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID: 1–4094

no logging syslog source-interface

This command disables syslog logging.

Format: `no logging syslog`

Command mode: Global Config

show logging

This command displays logging configuration information.

Format: `show logging`

Command mode: Privileged

Term	*Value*
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
Logging Client USB File Name	The name of the file on the USB-drive, to store the log
Logging Client Source Interface	Shows the configured syslog source-interface (source IP address).
CLI Command Logging	Shows whether CLI Command logging is enabled.
logging protocol	The logging protocol version number. 0: RFC 3164 1: RFC 5424
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity at which the logging entries are retained after a system reboot.
Syslog Logging	Shows whether syslog logging is enabled.

Syslog Logging Facility	Shows the value set for the facility in syslog messages.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

show logging buffered

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

Format: `show logging buffered`

Command mode: Privileged

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

show logging hosts

This command displays all configured logging hosts.

Format: `show logging hosts`

Command mode: Privileged

Term	*Value*
Host Index	Used for deleting hosts
IP Address/Hostname	IP address or hostname of the logging host.
Severity Level	The minimum severity to log to the specified address. Possible values are: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Status	Status field provides the current status. (Active, Not in Service, Not Ready).
Mode	The type of security: UDP or TLS.
Auth	The type of authentication mode: anonymous or x509name
Cert #	The certificate number to be used for authentication. Valid value range: 0–8. Index 0 is used to the default file.

show logging persistent

Use this command to display persistent log entries. If log-files is specified, the system persistent log files are displayed.

Format: `show logging persistent [log-files]`

Command mode: Privileged

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

show logging traplogs

This command displays SNMP trap events and statistics.

Format: `show logging traplogs`

Command mode: Privileged

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

clear logging buffered

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

Format: `clear logging buffered`

Command mode: Privileged

6.7 Email Alerting and Mail Server Configuration

logging email

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires. You can specify the severitylevel value as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

Default: disabled; when enabled, log messages at or above severity Warning (4) are emailed

Format: `logging email [severitylevel]`

Command mode: Global Config

no logging email

This command disables email alerting.

Format: `no logging email`

Command mode: Global Config

logging email urgent

This command sets the lowest severity level at which log messages are emailed immediately in a single email message. The value of `severitylevel` can be set as integers from 0 to 7, and descriptively, using the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7). Specify none to indicate that log messages are collected and sent in a batch email at a specified interval.

Default: Alert (1) and emergency (0) messages are sent immediately.

Format: `logging email urgent {severitylevel | none}`

Command mode: Global Config

no logging email urgent

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

Format: `no logging email urgent`

Command mode: Global Config

logging email message-type to-addr

This command configures the email address to which messages are sent. The message types supported are *urgent*, *non-urgent*, and *both*. For each supported severity level, multiple email addresses can be configured. The *to-email-addr* variable is a standard email address, for example admin@yourcompany.com.

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

Command mode: Global Config

no logging email message-type to-addr

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

Format: `no logging email message-type {urgent |non-urgent |both} to-addr` *`to-email-addr`*

Command mode: Global Config

logging email from-addr

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

Default: switch@eltex-co.ru

Format: `logging email from-addr` *`from-email-addr`*

Command mode: Global Config

no logging email from-addr

This command removes the configured email source address.

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

Command mode: Global Config

logging email message-type subject

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

Default: For urgent messages: Urgent Log Messages

For non-urgent messages: Non Urgent Log Messages

Format: `logging email message-type {urgent |non-urgent |both} subject` *`subject`*

Command mode: Global Config

no logging email message-type subject

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

Format: `no logging email message-type {urgent |non-urgent |both} subject`

Command mode: Global Config

logging email logtime

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

Default: 30 minutes

Format: `logging email logtime` *`minutes`*

Command mode: Global Config

no logging email logtime

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

Format: `no logging email logtime`

Command mode: Global Config

logging traps

This command sets the severity at which SNMP traps are logged and sent in an email. The value of *`severitylevel`* can be set as integers from 0 to 7, and descriptively, using the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

Default: Info (6) messages and higher are logged.

Format: `logging traps` *`severitylevel`*

Command mode: Global Config

no logging traps

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

Format: `no logging traps`

Command mode: Global Config

logging email test message-type

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

Format: `logging email test message-type {urgent |non-urgent |both} message-body` *`message-body`*

Command mode: Global Config

show logging email config

This command displays information about the email alert configuration.

Format: `show logging email config`

Command mode: Privileged

Term	*Value*

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

show logging email statistics

This command displays email alerting statistics.

Format: `show logging email statistics`

Command mode: Privileged

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

clear logging email statistics

This command resets the email alerting statistics.

Format: `clear logging email statistics`

Command mode: Privileged

mail-server

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

Format: `mail-server {ip-address | ipv6-address | hostname}`

Command mode: Global Config

no mail-server

This command removes the specified SMTP server from the configuration.

Format: `no mail-server {ip-address | ipv6-address | hostname}`

Command mode: Global Config

security

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

Default: none

Format: `security {tlsv1 | none}`

Command mode: mail server configuration

port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, and for no security (i.e. none) it is 25. However, any nonstandard port in the range 1 to 65535 is also allowed.

Default: 25

Format: `port {465 | 25 | 1–65535}`

Command mode: mail server configuration

username (Mail Server Config)

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

Default: admin

Format: `username name`

Command mode: mail server configuration

password

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

Default: admin

Format: password *password*

Command mode: mail server configuration

show mail-server config

This command displays information about the email alert configuration.

Format: show mail-server {*ip-address* | *hostname* | all} config
Command mode: Privileged

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

6.8 System utility and clear commands

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

traceroute

Use the traceroute command to discover the routes that IPv4 or IPv6 packets actually take when traveling to their destination through the network on a hop-by-hop basis. This command continues to provide a synchronous response when initiated from the CLI.

The user may specify the source IP address or the virtual router of the traceroute attempts. Recall that traceroute works by sending packets that are expected not to reach their final destination, but instead trigger ICMP error messages back to the source address from each hop along the forward path to the destination. By specifying the source address, the user can determine where along the forward path there is no route back to the source address. Note that this is only useful if the route from source to destination and destination to source is symmetric). It would be common, for example, to send a traceroute from an edge router to a target higher in the network using a source address from a host subnet on the edge router. This would test reachability from within the network back to hosts attached to the edge router. Alternatively, one might send a traceroute with an address on a loopback interface as a source to test reachability back to the loopback interface address.

In the CLI, the user may specify the source as an IPv4 address, IPv6 address, a virtual router, or as a routing interface. When the source is specified as a routing interface, the traceroute is sent using the pri-

mary IPv4 address on the source interface. With SNMP, the source must be specified as an address. The source cannot be specified in the web interface.

Software will not accept an incoming packet, such as a traceroute response, that arrives on a routing interface if the packet's destination address is on one of the out-of-band management interfaces (service port or network port). Similarly, software will not accept a packet that arrives on a management interface if the packet's destination is an address on a routing interface. Thus, it would be futile to send a traceroute on a management interface using a routing interface address as source, or to send a traceroute on a routing interface using a management interface as source. When sending a traceroute on a routing interface, the source must be that routing interface or another routing interface. When sending a traceroute on a management interface, the source must be on that management interface. For this reason, the user cannot specify the source as a management interface or management interface address. When sending a traceroute on a management interface, the user should not specify a source address, but instead let the system select the source address from the outgoing interface.

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

Format: `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}]`

Command mode: Privileged

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of attempts sent for each TTL, and the size of each probe.

Parameter	*Description*
vrf-name	The name of the VRF instance from which to initiate traceroute. Only hosts reachable from within the VRF instance can be tracerouted. If a source parameter is specified in conjunction with a vrf parameter, it must be a member of the VRF. The ipv6 parameter cannot be used in conjunction with the vrf parameter.
ipaddress	The ipaddress value should be a valid IP address
ipv6-address	The ipv6-address value should be a valid IPv6 address
hostname	The hostname value should be a valid hostname
ipv6	The optional ipv6 keyword can be used before ipv6-address or hostname. Giving the ipv6 keyword before the hostname tries it to resolve to an IPv6 address.
initTtl	Specifies the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255. Valid values: from 0 to 255.
maxTtl	Specifies the maximum TTL. Valid values: from 1 to 255
maxFail	Use maxFail to terminate the traceroute after failing to

	receive a response for this number of consecutive attempts. Range is from 0 to 255.
interval	Use the optional interval parameter to specify the time between attempts, in seconds. If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Valid values: from 1 to 60 seconds.
count	Use the optional count parameter to specify the number of attempts to send for each TTL value. Valid values: from 1 to 10 attempts
port	Use the optional port parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Valid values: from 1 to 65535.
size	Use the optional size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 13000 bytes.
source	Use the optional source parameter to specify the source IP address or interface for the traceroute.

clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter y, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Format: `clear config`

Command mode: Privileged

clear counters

This command clears the statistics for a specified unit/slot/port, for all the ports, or for an interface on a VLAN based on the argument, including the loop protection counters. If a virtual router is specified, the statistics for the ports on the virtual router are cleared. If no router is specified, the information for the default router will be displayed.

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

Command mode: Privileged

clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format: `clear igmpsnooping`

Command mode: Privileged

clear ip access-list counters

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

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

Command mode: Privileged

clear ipv6 access-list counters

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

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

Command mode: Privileged

clear mac access-list counters

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

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

Command mode: Privileged

clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format: `clear pass`

Command mode: Privileged

clear traplog

This command clears the trap log.

Format: `clear traplog`

Command mode: Privileged

clear vlan

This command resets VLAN configuration parameters to the factory defaults. When the VLAN configuration is reset to the factory defaults, there are some scenarios regarding GVRP and MVRP that happen due to this:

1. Static VLANs are deleted.
2. GVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Since GVRP is disabled by default, this means that GVRP should be disabled and all of its dynamic VLANs should be deleted.

Format: `clear vlan`

Command mode: Privileged

logout

This command closes the current Telnet connection or resets the current serial connection.

Save configuration changes before logging out.

Format: `logout`

Command mode: Privileged
User

ping

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

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

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

Command mode: Privileged
User

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

Parameter	*Description*
vrf-name	The name of the virtual router in which to initiate the ping. If no virtual router is specified, the ping is initiated in the default router instance.
address	IPv4 or IPv6 addresses to ping
count	Use the count parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the ip-address field. Range of values: from 1 to 15 requests.
interval	Use the interval parameter to specify the time between Echo Requests, in seconds. Valid values: from 1 to 60 seconds.
size	Use the size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to

	13000 bytes.
source	Use the source parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.
hostname	Use the hostname parameter to resolve to an IPv4 or IPv6 address. The ipv6 keyword is specified to resolve the hostname to IPv6 address. The IPv4 address is resolved if no keyword is specified.
ipv6	The optional keyword ipv6 can be used before the ipv6-address or hostname argument. Using the ipv6 optional keyword before hostname tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.
interface	Use the interface keyword to ping a link-local IPv6 address over an interface.
link-local- address	The link-local IPv6 address to ping over an interface.
outgoing- interface	Use the outgoing-interface parameter to specify the outgoing interface for multicast IP/IPv6 ping.

quit

This command closes the current Telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format: `quit`

Command mode: Privileged
User

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed.

Format: `reload [configuration [`*`scriptname`*`]]`
Command mode: Privileged

Parameter	*Description*
configuration	Gracefully reloads the configuration. If no configuration file is specified, the startup-config file is loaded.
scriptname	The configuration file to load. The scriptname must include the extension.

copy

The copy command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (active and backup) on the file system. Upload and download files from a server using FTP, TFTP, Xmodem, Ymodem, or Zmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

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

Command mode: Privileged

Replace the *source* and *destination* parameters with the options in the following table. For the url source or destination, use one of the following values:

{xmodem | ymodem | zmodem |

tftp://<ipaddress|hostname>/<filepath>/<filename>|

ftp://<*username*>@<ipaddr|hostname>/< filepath>/<filename> |

scp://<*username*>@<ipaddr|hostname>/< filepath>/<filename> |

sftp://<*username* >@<ipaddr|hostname>/< filepath>/<filename>

| usb://<filepath>/<filename>}

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

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

{ tftp://<ipaddress|hostname>/<filepath>/<filename>|

ftp://<username >@<ipaddr|hostname>/<filepath>/<filename> |

scp://<username >@<ipaddr|hostname>/<filepath>/<filename> |

sftp://<username >@<ipaddr|hostname>/<filepath>/<filename> |

usb://<filepath>/<filename>}

The maximum length for the file path is 160 characters, and the maximum length for the file name is 128 characters.

For FTP, TFTP, SFTP and SCP, the ipaddr|hostname parameter is the IP address or host name of the server, filepath is the path to the file, and filename is the name of the file you want to upload or download. For SFTP and SCP, the username parameter is the username for logging into the remote server via SSH.

For platforms that include stacking, use the optional [unit unit id] parameter (when available) to specify the stack member to use as the source for the item to copy. If no unit is specified, the item is copied from the stack master.

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

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

Command mode: Privileged

Remember to upload the existing fastpath.cfg file off the switch prior to loading a new release image in order to make a backup.

Source	*Destination*	*Description*
nvram:application:*sourcefilename*	url	Filename of source application file
nvram:backup-config	nvram:startup-config	Copies the backup configuration to the startup configuration
nvram:clibanner	url	Copies the CLI banner to a server.
nvram: core-dump [unit *unit id*]	tftp:// <ipaddress|hostname>/ <filepath>/<filename>| ftp:// <user>@<ipaddr|hostnam e>/<path>/<filename> | scp:// <user>@<ipaddr|hostnam e>/<path>/<filename> | sftp:// <user>@<ipaddr|hostnam e>/<path>/<filename>}	Uploads the core dump file on the local system to an external TFTP/FTP/SCP/SFTP server
nvram:cpupktcapture.pcap [unit *unit id*]	url	Uploads CPU packets capture file
nvram:crash-log	url	Copies the crash log to a server.
nvram:errorlog	url	Copies the error log file to a server
nvram:factory-defaults	url	Uploads factory defaults file
nvram:fastpath.cfg	url	Uploads the binary config file to a server
nvram:log	url	Copies the log file to a server.
nvram:operational-log [unit unit id]	url	Copies the operational log file to a server
nvram:script scriptname	url	Copies a specified configuration script file to a server
nvram:startup-config	nvram:backup-config	Copies the startup configuration to the backup configuration

nvram:startup-config	url	Copies the startup configuration to a server
nvram:startup-log [unit unit id]	url	Uploads the startup log file
nvram: tech-support [unit *unit id*]	url	Uploads the system and configuration information for technical support
nvram:traplog	url	Copies the trap log file to a server
system:running-config	nvram:startup-config	Saves the running configuration to NVRAM
system:running-config	nvram:factory-defaults	Saves the running configuration to NVRAM to the factory-defaults file.
system:image	url	Saves the system image to a server.
tftp:// <ipaddress>/ <filename>	system:packet.pcap	Copies a PCAP file into RAM. The PCAP file is used to inject packets into the silicon for tracing the packets
url	nvram:application destfilename	Destination file name for the application file
url	nvram:backup-config	Downloads backup configuration file
url	nvram:ca-root index	Downloads the CA certificate file to the flash memory and uses the index number name the downloaded file to CAindex.pem.
url	nvram:clibanner	Downloads the CLI banner to the system.
url	nvram:client-key index	Downloads the client key file to the flash memory and uses the index number name the downloaded file to CAindex.key.
url	nvram:client-ssl-cert *1-8*	Downloads the client certificate to the flash memory and uses the index number to name the downloaded file
url	nvram:factory-defaults	Downloads the factory settings file
url	nvram:fastpath.cfg	Downloads the binary config file to the system
url	nvram:license-key	Downloads the license file
url	nvram:openflow-ssl-ca-cert	Downloads OpenFlow SSL certificates
url	nvram:openflow-ssl-cert	Downloads OpenFlow SSL certificates
url	nvram:openflow-ssl-priv-key	Downloads OpenFlow SSL certificates
url	nvram:publickey-config	Downloads the Public Key for Con-

		figuration Script validation.
url	nvram:publickey-image	Downloads Public Key for Image validation
url	nvram:script destfilename	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
url	nvram:script *destfilename* noval	When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows: (Routing) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval
url	nvram:sshkey-dsa	Downloads an SSH key file
url	nvram:sshkey-rsa1	Downloads an SSH key file
url	nvram:sshkey-rsa2	Downloads an SSH key file
url	nvram:sslpem-dhweak	Downloads an HTTP secure-server certificate
url	nvram:sslpem-dhstrong	Downloads an HTTP secure-server certificate
url	nvram:sslpem-root	Downloads an HTTP secure-server certificate
url	nvram:sslpem-server	Downloads an HTTP secure-server certificate
url	nvram:startup-config	Downloads the startup configuration file to the system
url	ias-users	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and their attributes available in the downloaded file.
url	nvram:tech-support-cmds	Downloads the file containing list of commands to be displayed using the show tech-support command.
url	{active | backup}	Download an image from the remote server to either image. In a stacking environment, the downloaded image is distributed to the stack nodes.
{active | backup}	url	Upload either image to the remote server.

active	backup	Copy the active image to the backup image
backup	active	Copy the backup image to the active image
{active | backup}	unit://unit/{active | backup}	Copy an image from the management node to a given node in a Stack. Use the unit parameter to specify the node to which the image should be copied.
{active | backup}	unit://unit/{active | backup}	Copy an image from the management node to all of the nodes in a Stack

file verify

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

Format: `file verify {all | image | none | script}`

Command mode: Global Config

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

no file verify

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

Format: `no file verify`

Command mode: Global Config

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running-config nvram:startup-config`. Use the confirm keyword to directly save the configuration to NVRAM without prompting for a confirmation.

Format: `write memory [confirm]`

Command mode: Privileged

6.9 Licensing for advanced features

This section describes the commands you use to enter the license key to access advanced features. You cannot access the advanced features without a valid license key. Licensing of the following components is possible: OSPF, OSPFV3, RIP, VRRP, BGP, DCBX, FIP SNOOPING, QCN, DOT1AD, DOT3AH/EFM-OAM, DOT1AG/CFM-OAM, TR069. You cannot use this features without a valid license key.

copy <url> nvram:license-key

Download the license file to the device**.**

Default: None

Format `copy <tftp|ftp|scp|sftp|usb://<ipaddr>/<filepath>/<filename>> |xmodem|ymodem|zmodem nvram:license-key`

Command Mode: Privileged Mode

delete license-key

This command deletes the license file

Default: Disabled

Format `delete license-key`

Command Mode: Global Config Mode

show license

View the current status of the license

Format `show license`

Command Mode: Privileged Mode

show license features

View list of licensed components

Format `show license features`

Command Mode: Privileged Mode

6.10 SNTP configuration

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

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds. The interval is equal to 2 to the power poll-interval, where poll-interval can be a value from 6 to 10.

Default: 6

Format: `sntp broadcast client poll-interval` *`poll-interval`*

Command mode: Global Config

no sntp broadcast client poll-interval

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

Format: `no sntp broadcast client poll-interval`

Command mode: Global Config

sntp client mode

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

Default: disabled

Format: `sntp client mode [broadcast | unicast]`

Command mode: Global Config

no sntp client mode

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

Format: `no sntp client mode`

Command mode: Global Config

sntp client port

This command sets the SNTP client port ID to 0, 123 or a value between 1025 and 65535. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying OS.

Default: 0

Format: `sntp client port portid`

Command mode: Global Config

no sntp client port

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

Format: `no sntp client port`

Command mode: Global Config

sntp unicast client poll-interval

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

Default: 6

Format: `sntp unicast client poll-interval poll-interval`

Command mode: Global Config

no sntp unicast client poll-interval

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

Format: `no sntp unicast client poll-interval`

Command mode: Global Config

sntp unicast client poll-timeout

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

Default: 5

Format: `sntp unicast client poll-timeout poll-timeout`

Command mode: Global Config

no sntp unicast client poll-timeout

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

Format: `no sntp unicast client poll-timeout`

Command mode: Global Config

sntp unicast client poll-retry

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

Default: 1

Format: `sntp unicast client poll-retry poll-retry`

Command mode: Global Config

no sntp unicast client poll-retry

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

Format: `no sntp unicast client poll-retry`

Command mode: Global Config

sntp server

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

Format: `sntp server {ipaddress | ipv6address | hostname} [priority [version [portid]]]`

Command mode: Global Config

no sntp server

This command deletes server from the configured SNTP servers.

Format: `no sntp server remove {ipaddress | ipv6address | hostname}`

Command mode: Global Config

sntp source-interface

Use this command to specify the physical or logical interface to use as the source interface (source IP address) for SNTP unicast server configuration. If configured, the address of source Interface is used for all SNTP communications between the SNTP server and the SNTP client. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If the interface is not specified, the source IP address of the initiating (outgoing) interface is used as the source address. If the configured interface is down, the SNTP client falls back to its default behavior.

Format: `sntp source-interface {unit/slot/port | loopback loopback-id | vlan vlan-id}`

Command mode: Global Config

Parameter	*Description*
unit/slot/port	The unit identifier assigned to the switch
loopback-id	Configures the loopback interface. The range of the loopback ID is 0 to 7.
tunnel-id	Configures the IPv6 tunnel interface. The range of the tunnel ID is 0 to 7.
vlan-id	Configures the VLAN interface to use as the source IP address. ID VLAN range: 1-4093

no sntp source-interface

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

Format: `no sntp source-interface`

Command mode: Global Config

show sntp

This command is used to display SNTP settings and status.

Format: `show sntp`

Command mode: Privileged

Term	*Value*

Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

show sntp client

Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

Format: `show sntp client`

Command mode: Privileged

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

show sntp server

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

Format: `show sntp server`

Command mode: Privileged

Term	*Value*
Server Host Address	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4, IPv6, or DNS).
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed
Server Current Entries	Total number of SNTP configured.

For each configured server:

Term	Value
IP Address/Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server (IPv4, IPv6, or DNS).
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

show sntp source-interface

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

Format: `show sntp source-interface`

Command mode: Privileged

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

6.11 Time Zone configuration

Use the Time Zone commands to configure system time and date, Time Zone and Summer Time (that is, Daylight Saving Time). Daylight saving time can be made periodically or not.

clock set

This command sets the system time and date.

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

Command mode: Global Config

Parameter	Description
hh:mm:ss	Enter the current system time in 24-hour format in hours, minutes, and seconds. The range is hours: from 0 to 23, for minutes: from 0 to 59, seconds: from 0 to 59
mm/dd/yyyy	Enter the current system date the format month, day,

	year. The range for month is 1 to 12. The range for the day of the month is 1 to 31. The range for year is 2010 to 2079.

clock summer-time date

Use the clock summer-time date command to set the summer-time offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they are read as either 0 or \0, as appropriate.

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

Command mode: Global Config

Parameter	*Description*
date	Day of the month. Valid values: 1 to 31.
month	Month. The range is the first three letters by name (for example, Jan).
year	Year. The range is 2000 to 2097.
hh:mm	Time in 24 hour format (hh:mm). Time range: from 0 to 23, for minutes: from 0 to 59
offset	The number of additional minutes by daylight saving time. Valid values: from 1 to 1440
acronym	The designation of summer time to display during the period of daylight saving time. Length: up to 4 characters

clock summer-time recurring

This command sets the daylight saving recurring parameters.

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

Command mode: Global Config

Parameter	*Description*
EU	The system clock uses the standard recurring daylight saving time settings used in countries in the European Union
USA	The system clock uses the standard recurring daylight saving time settings used in the United States
week	Week of the month. Range of values: 1–5, first, last.
day	Day of the week. Symbol: first three letters by name; sun, for example.
month	Month. Symbol: first three letters by name; jan, for example.

hh:mm	Time in 24 hour format (hh:mm). Time range: from 0 to 23, for minutes: from 0 to 59
offset	The number of additional minutes by daylight saving time. Valid values: from 1 to 1440
acronym	The designation of summer time to display during the period of daylight saving time. Length: up to 4 characters

no clock summer-time

This command disables the daylight saving time settings.

Format: `no clock summer-time`

Command mode: Global Config

clock timezone

Use this command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either 0 or \0 as appropriate.

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

Command mode: Global Config

no clock timezone

Use this command to reset the time zone settings.

Format: `no clock timezone`

Command mode: Global Config

show clock

Use this command to display the time and date from the system clock.

Format: `show clock`

Command mode: Privileged

show clock detail

Use this command to display the detailed system time along with the time zone and the daylight saving time configuration.

Format: `show clock detail`

Command mode: Privileged

6.12 DHCP Server configuration

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

ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode. The maximum number of address pools is 32.

Default: none

Format: `ip dhcp pool` *name*

Command mode: Global Config

no ip dhcp pool

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

Format: `no ip dhcp pool` *name*

Command mode: Global Config

client-identifier

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

Default: none

Format: `client-identifier` *uniqueidentifier*

Command mode: DHCP Pool Config

no client-identifier

This command deletes the client identifier.

Format: `no client-identifier`

Command mode: DHCP Pool Config

client-name

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

Default: none

Format: `client-name` *name*

Command mode: DHCP Pool Config

no client-name

This command removes the client name.

Format: `no client-name`

Command mode: DHCP Pool Config

default-router

This command specifies the default router list for a DHCP client. {address1, address2… address8} are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is not valid.

Default: none

Format: `default-router` *address1 [address2....address8]*

Command mode: DHCP Pool Config

no default-router

This command removes the default router list.

Format: `no default-router`

Command mode: DHCP Pool Config

dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is not valid.

Default: none

Format: `dns-server` *address1 [address2....address8]*

Command mode: DHCP Pool Config

no dns-server

This command removes the DNS Server list.

Format: `no dns-server`

Command mode: DHCP Pool Config

hardware-address

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

Default: Ethernet

Format: `hardware-address` *hardwareaddress type*

Command mode: DHCP Pool Config

no hardware-address

This command removes the hardware address of the DHCP client.

Format: `no hardware-address`

Command mode: DHCP Pool Config

host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is not valid. Prefix — integer from 0 to 32.

Default: none

Format: `host` *`address`* `[{`*`mask`* `|` *`prefix-length`*`}]`

Command mode: DHCP Pool Config

no host

This command removes the IP address of the DHCP client.

Format: `no host`

Command mode: DHCP Pool Config

lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If you specify infinite, the lease is set for 60 days. You can also specify a lease duration. Days is an integer from 0 to 59. Hours is an integer from 0 to 23. Minutes is an integer from 0 to 59.

Default: 1 (day)

Format: `lease [{`*`days`* `[`*`hours`*`] [`*`minutes`*`] | infinite}]`

Command mode: DHCP Pool Config

no lease

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

Format: `no lease`

Command mode: DHCP Pool Config

network (DHCP Pool Config)

Use this command to configure the subnet number and mask for a DHCP address pool on the server. Network- number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is not valid. Mask is the IP subnet mask for the specified address pool. Prefix — integer from 0 to 32.

Default: none

Format: `network networknumber [{mask | prefixlength}]`

Command mode: DHCP Pool Config

no network

This command removes the subnet number and mask.

Format: `no network`

Command mode: DHCP Pool Config

bootfile

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

Format: `bootfile filename`

Command mode: DHCP Pool Config

no bootfile

This command deletes the boot image name.

Format: `no bootfile`

Command mode: DHCP Pool Config

domain-name

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

Default: none

Format: `domain-name domain`

Command mode: DHCP Pool Config

no domain-name

This command removes the domain name.

Format: `no domain-name`

Command mode: DHCP Pool Config

domain-name enable

This command enables the domain name functionality.

Format: `domain-name enable [name name]`

Command mode: Global Config

no domain-name enable

This command disables the domain name functionality.

Format: `no domain-name enable`

Command mode: Global Config

netbios-name-server

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

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

Default: none

Format: `netbios-name-server address [address2...address8]`

Command mode: DHCP Pool Config

no netbios-name-server

This command removes the NetBIOS name server list.

Format: `no netbios-name-server`

Command mode: DHCP Pool Config

netbios-node-type

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

- b-node — broadcast
- p-node — peer-to-peer
- m-node — mixed
- h-node — hybrid (recommended)

Default: none

Format: `netbios-node-type type`

Command mode: DHCP Pool Config

no netbios-node-type

This command removes the NetBIOS node Type.

Format: `no netbios-node-type`

Command mode: DHCP Pool Config

next-server

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

Default: inbound interface helper addresses

Format: `next-server` *`address`*

Command mode: DHCP Pool Config

no next-server

This command removes the boot server list.

Format: `no next-server`

Command mode: DHCP Pool Config

option

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

Default: none

Format: `option` *`code`* {*`ascii string`* | *`hex string1`* [*`string2...string8`*] | `ip` *`address1`*[*`address2...address8`*]}

Command mode: DHCP Pool Config

no option

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

Format: `no option` *`code`*

Command mode: DHCP Pool Config

ip dhcp excluded-address

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

Default: none

Format: `ip dhcp excluded-address` *`lowaddress [highaddress]`*

Command mode: Global Config

no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. `Low-address` and `high-address` are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is not valid.

Format: `no ip dhcp excluded-address` *`lowaddress [highaddress]`*

Command mode: Global Config

ip dhcp ping packets

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

Default: 2

Format: `ip dhcp ping packets` *`0,2-10`*

Command mode: Global Config

no ip dhcp ping packets

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

Format: `no ip dhcp ping packets`

Command mode: Global Config

service dhcp

This command enables the DHCP server.

Default: disabled

Format: `service dhcp`

Command mode: Global Config

no service dhcp

This command disables the DHCP server.

Format: `no service dhcp`

Command mode: Global Config

ip dhcp bootp automatic

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

Default: disabled

Format: `ip dhcp bootp automatic`

Command mode: Global Config

no ip dhcp bootp automatic

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

Format: `no ip dhcp bootp automatic`

Command mode: Global Config

ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default: enabled

Format: `ip dhcp conflict logging`

Command mode: Global Config

no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format: `no ip dhcp conflict logging`

Command mode: Global Config

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If '*' is specified, the bindings corresponding to all the addresses are deleted. address is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is not valid.

Format: `clear ip dhcp binding {`*`address`*` | *}`

Command mode: Privileged

clear ip dhcp server statistics

This command clears DHCP server statistics timers.

Format: `clear ip dhcp server statistics`

Command mode: Privileged

clear ip dhcp conflict

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

Default: none

Format: `clear ip dhcp conflict {address | *}`

Command mode: Privileged

show ip dhcp binding

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

Format: `show ip dhcp binding [address]`

Command mode: Privileged
User

Term	*Value*
IP Address	The IP address of the client
Hardware Address	Client MAC address or identifier
Lease expiration	The leasing time of the IP address assigned to the client
Type	The manner in which IP address was assigned to the client

show ip dhcp global configuration

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

Format: `show ip dhcp global configuration`

Command mode: Privileged
User

Term	*Value*
Service DHCP	The field to display the status of dhcp
Number of Ping Packets	The maximum number of Ping Packets that will be sent to verify that an ip address identifier not already assigned.
Conflict Logging	Shows whether conflict logging is enabled or disabled.
BootP Automatic	Shows whether BootP for dynamic pools is enabled or disabled

show ip dhcp pool configuration

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

Format: `show ip dhcp pool configuration {name | all}`

Command mode: Privileged
User

Field	*Value*
Pool Name	The name of the configured pool

Pool Type	The pool type
Lease Time	The leasing time of the IP address assigned to the client
DNS Servers	The list of DNS servers available to the DHCP client
Default Routers	The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

Field	*Value*
Network	The network number and the mask for the DHCP address pool

The following additional fields are displayed for Manual pool type:

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

show ip dhcp server statistics

This command displays DHCP server statistics.

Format: `show ip dhcp server statistics`

Command mode: Privileged
User

Field	*Value*
Automatic Bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server.

Message Received:

Message	*Value*
DHCP DISCOVER	The number of DHCPDISCOVER messages the server has received.
DHCP REQUEST	The number of DHCPREQUEST messages the server has received.
DHCP DECLINE	The number of DHCPDECLINE messages the server has received.
DHCP RELEASE	The number of DHCPRELEASE messages the server has

	received.
DHCP INFORM	The number of DHCPINFORM messages the server has received.
DHCP OFFER	The number of DHCPOFFER messages the server has received.
DHCP ACK	The number of DHCPACK messages the server has received.
DHCP NACK	The number of DHCPNACK messages the server has received.

show ip dhcp conflict

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

Format: `show ip dhcp conflict [ip-address]`

Command mode: Privileged
User

Term	*Value*
IP Address	The IP address of the host as recorded on the DHCP server
Detection Method	The manner in which the IP address of the hosts were found on the DHCP Server
Detection time	The time when the conflict was found

6.13 DNS Client configuration

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

ip domain lookup

Use this command to enable the DNS client.

Default: enabled

Format: `ip domain lookup`

Command mode: Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format: `no ip domain lookup`

Command mode: Global Config

ip domain name

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

Default: none

Format: `ip domain name` *name*

Command mode: Global Config

Example

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

no ip domain name

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

Format: `no ip domain name`

Command mode: Global Config

ip domain list

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

Default: none

Format: `ip domain list` *name*

Command mode: Global Config

no ip domain list

Use this command to delete a name from a list.

Format: `no ip domain list` *name*

Command mode: Global Config

ip name server

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

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

Command mode: Global Config

no ip name server

Use this command to remove a name server.

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

Command mode: Global Config

ip name source-interface

Use this command to specify the physical or logical interface to use as the DNS client (IP name) source interface (source IP address) for the DNS client management application. If configured, the address of source Interface is used for all DNS communications between the DNS server and the DNS client. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If the interface is not specified, the source IP address of the initiating (outgoing) interface is used as the source address. If the configured interface is down, the DNS client falls back to its default behavior.

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

Command mode: Global Config

no ip name source-interface

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

Format: `no ip name source-interface`

Command mode: Global Config

ip host

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

Default: none

Format: `ip host name ipaddress`

Command mode: Global Config

no ip host

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

Format: `no ip host name`

Command mode: Global Config

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. Use this command to define static host name-to-IPv6 address mapping in the host cache. The parameter name is host name and v6 address is the IPv6 address of the host. The hostname can include 1–255 alphanumeric characters, periods, hyphens, and spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example 'lab-pc 45'.

Default: none

Format: `ipv6 host` *`name v6 address`*

Command mode: Global Config

no ipv6 host

Use this command to remove the static host name-to-IPv6 address mapping in the host cache.

Format: `no ipv6 host` *`name`*

Command mode: Global Config

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The parameter number indicates the number of times to retry sending a DNS query to the DNS server. Range of values: from 0 to 100.

Default: 2

Format: `ip domain retry` *`number`*

Command mode: Global Config

no ip domain retry

Use this command to return to the default.

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

Command mode: Global Config

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter seconds specifies the time, in seconds, to wait for a response to a DNS query. The parameter seconds ranges from 0 to 3600.

Default: 3

Format: `ip domain timeout` *seconds*

Command mode: Global Config

no ip domain timeout

Use this command to return to the default setting.

Format: `no ip domain timeout` *seconds*

Command mode: Global Config

clear host

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

Format: `clear host {`*name* `|` `all}`
Command mode: Privileged

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

show hosts

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

Format: `show hosts` *[name]*

Command mode: privileged, user

Field	*Description*
Host Name	Domain host name.
Default Domain	Default domain name
Default Domain List	Default domain list
Domain Name Lookup	DNS client enabled/disabled.
Number of Retries	Number of time to retry sending Domain Name System (DNS) queries
Retry Timeout Period	Amount of time to wait for a response to a DNS query
Name Servers	Configured name servers

ADNS Client Source Interface	Shows the configured source interface (source IP address) used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server

show ip name source-interface

Use this command to display the configured source interface details used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.

Format: `show ip name source-interface`

Command mode: Privileged

6.14 IP Address Conflict management

The commands in this section help troubleshoot IP address conflicts.

ip address-conflict-detect run

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

Format: `ip address-conflict-detect run`

Command mode: Global Config
Virtual Router Config

show ip address-conflict

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

Format: `show ip address-conflict`

Command mode: Privileged

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

clear ip address-conflict-detect

This command clears the detected address conflict status information for the specified virtual router. If no router is specified, the command is executed for the default router.

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

Command mode: Privileged

6.15 Serviceability Packet Tracing commands

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

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

capture start

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

The packet capture operates in three modes:

- capture file;
- remote capture;
- capture line.

The command is not persistent across a reboot cycle.

Format: `capture start [{all | receive | transmit}]`

Command mode: Privileged

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

capture stop

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

Format: `capture stop`

Command mode: Privileged

capture file | remote | line

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

Format: `capture {file|remote|line|usb}`

Command mode: Global Config

Parameter	*Description*
file	In the capture file mode, the captured packets are stored in a file on NVRAM. The maximum file size defaults to 524288 bytes. The switch can transfer the file to a TFTP server via TFTP, SFTP, SCP via CLI, and SNMP. The file is formatted in pcap format, is named

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

capture remote port

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

Format: `capture remote port` *`id`*

Command mode: Global Config

capture file size

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

Format: `capture file size` *`max file size`*

Command mode: Global Config

capture line wrap

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

Format: `capture line wrap`

Command mode: Global Config

no capture line wrap

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

Format: `no capture line wrap`

Command mode: Global Config

capture usb

This command sets capture options on USB media. The command is persistent across a reboot cycle. The <file-name> parameter specifies the name of the file on the USB media in which captured packets are written.

Format: `capture usb <file-name>`

Command mode: Global Config

show capture packets

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

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

Format: `show capture packets`

Command mode: Privileged

cpu-traffic direction interface

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

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

Default: none

Format: `cpu-traffic direction {tx|rx|both} interface` *`interface-range`*

Command mode: Global Config

no cpu-traffic direction interface

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

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

Command mode: Global Config

cpu-traffic direction match cust-filter

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

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

Default: none

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

Command mode: Global Config

no cpu-traffic direction match cust-filter

Use this command to remove the configured custom filter.

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

Command mode: Global Config

cpu-traffic direction match srcip

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

Default: none

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

Command mode: Global Config

no cpu-traffic direction match srcip

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

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

Command mode: Global Config

cpu-traffic direction match dstip

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

Default: none

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

Command mode: Global Config

no cpu-traffic direction match dstip

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

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

Command mode: Global Config

cpu-traffic direction match tcp

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

Default: none

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

Command mode: Global Config

no cpu-traffic direction match tcp

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

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

Command mode: Global Config

cpu-traffic direction match udp

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

Default: none

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

Command mode: Global Config

no cpu-traffic direction match udp

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

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

Command mode: Global Config

cpu-traffic mode

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

Default: disabled

Format: `cpu-traffic mode`

Command mode: Global Config

no cpu-traffic mode

Use this command to disable CPU-traffic mode.

Format: `no cpu-traffic mode`

Command mode: Global Config

cpu-traffic trace

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

Default: disabled

Format: `cpu-traffic trace {dump-pkt}`

Command mode: Global Config

no cpu-traffic trace

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

Format: `no cpu-traffic trace {dump-pkt}`

Command mode: Global Config

show cpu-traffic

Use this command to display the current configuration parameters.

Default: none

Format: `show cpu-traffic`

Command mode: Privileged

show cpu-traffic interface

Use this command to display per interface statistics for configured filters. The statistics can be displayed for a specific filter (e.g., stp, udld, arp etc). If no filter is specified, statistics are displayed for all configured filters.

Similarly, source/destination IP, TCP, UDP or MAC along with custom filter can be used as command option to get statistics.

Default: none

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

Command mode: Privileged

show cpu-traffic summary

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

Default: none

Format: `show cpu-traffic summary`

Command mode: Privileged

show cpu-traffic trace

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

Default: none

Format: `show cpu-traffic trace filter`

Command mode: Privileged

clear cpu-traffic

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

Default: none

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

Command mode: Global Config

debug aaa accounting

This command is useful to debug accounting configuration and functionality in User Manager.

Format: `debug aaa accounting`

Command mode: Privileged

no debug aaa accounting

Use this command to turn off debugging of User Manager accounting functionality.

Format: `no debug aaa accounting`

Command mode: Privileged

debug arp

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

Default: disabled

Format: `debug arp [vrf` *`vrf-name`*`]`

Command mode: Privileged

no debug arp

Use this command to disable ARP debug protocol messages.

Format: `no debug arp`

Command mode: Privileged

debug authentication

This command displays either the debug trace for either a single event or all events for an interface

Default: none

Format: `debug authentication packet {all | event}` *`interface`*

Command mode: Privileged

debug auto-voip

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

Default: disabled

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

Command mode: Privileged

no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format: `no debug auto-voip`

Command mode: Privileged

debug clear

This command disables all previously enabled debug traces.

Default: disabled

Format: `debug clear`

Command mode: Privileged

debug aaa authorization

Use this command to enable the tracing for AAA in User Manager. This is useful to debug authorization configuration and functionality in the User Manager. Each of the parameters are used to configure authorization debug flags.

Format: `debug aaa authorization commands|exec`

Command mode: Privileged

no debug aaa authorization

Use this command to turn off debugging of the User Manager authorization functionality.

Format: `no debug aaa authorization`

Command mode: Privileged

Parameter	*Description*
kernel	View the crash log file for the kernel
crashlog-number	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4
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 Valid value range: 0–2
download url	To download a crash dump to the switch, use the download keyword and specify the required TFTP server information.
component-id	The ID of the component that caused the crash.
item-number	The item number
additional-parameter	Additional parameters to include

debug console

This command enables the display of 'debug' trace output on the login session in which it is executed. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default: disabled

Format: `debug console`

Command mode: Privileged

no debug console

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

Format: `no debug console`

Command mode: Privileged

debug crashlog

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

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

Default: disabled

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

Command mode: Privileged

debug dcbx packet

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

Default: disabled

Format: `debug dcbx packet {receive | transmit}`

Command mode: Privileged

debug debug-config

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

Default: disabled

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

Command mode: Privileged

debug dhcp packet

This command displays 'debug information about DHCPv4 client activities and traces DHCPv4 packets to and from the local DHCPv4 client.

Default: disabled

Format: `debug dhcp packet [transmit | receive]`

Command mode: Privileged

no debug dhcp

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

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

Command mode: Privileged

debug dot1ag

Use this command to enable debugging of the messages sent between MPs and MEPs.

Default: disabled

Format: `debug dot1ag {all | ccm | events | lbm | lbr | ltm | ltr | pdu}`

Command mode: Privileged

Parameter	*Description*
all	Debug all dot1ag message types
ccm	Configure debug flags for Continuity Check Message information. A multicast CFM PDU transmitted periodically by a MEP in order to ensure continuity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to receiving a CCM.
ltm	Configure debug flags for Linktrace Message information. A CFM PDU initiated by a MEP to trace a path to a target MAC address, forwarded from MIP to MIP, up to the point at which the LTM reaches its target, a MEP, or can no longer be forwarded. Each MP along the path to the target generates an LTR.
ltr	Configure debug flags for Linktrace Reply information. A unicast CFM PDU sent by an MP to a MEP, in response to receiving an LTM from that MEP.

lbm	Configure debug flags for Loopback Message information. A unicast CFM PDU transmitted by a MEP, addressed to a specific MP, in the expectation of receiving an LBR
lbr	Configure debug flags for Loopback Reply information. A unicast CFM PDU transmitted by an MP to a MEP, in response to an LBM received from that MEP.
pdu	Configure debug flags for CFM PDU information.

debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default: disabled

Format: `debug dot1x`

Command mode: Privileged

no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format: `no debug dot1x`

Command mode: Privileged

debug fip-snooping packet

Use the `debug fip-snooping packet` command in Privileged mode to enable FIP packet debug trace on transmit or receive path with different filter options configured.

Default: disabled

Format: `debug fip-snooping packet [{transmit | receive | filter {dst-mac` *`mac-addr`* `| fip-proto-code` *`1-15`* `| src-intf` *`unit/slot/port`* `| src-mac` *`mac-addr`* `| vlan` *`1-4093`*`}]`

Command mode: User

Privileged

Parameter	*Description*
dst-mac	If the dst-mac filter option is given, trace output is filtered on matching the given Destination MAC Address.
fip-proto-code	If the fip-proto-code filter option is given, trace output is filtered on matching the supported types
src-intf	If the src-intf filter option is given, trace output is filtered on matching the incoming source interface
src-mac	If the src-mac filter option is given, trace output is filtered on matching the given Source MAC Address
vlan	If the vlan filter option is given, trace output is filtered on matching the given VLAN ID

no debug fip-snooping packet

Use the no debug fip-snooping packet command in Privileged mode to disable FIP packet debug trace on transmit or receive path with different filter options configured.

Format: `no debug fip-snooping packet [{transmit | receive | filter {dst-mac` *`mac-addr`* `| fip- proto-code` *`1-15`* `| src-intf` *`unit/slot/port`* `| src-mac` *`mac-addr`* `| vlan` *`1-4093`*`}]`

Command mode: User

Privileged

debug igmpsnooping packet

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

Default: disabled

Format: `debug igmpsnooping packet`

Command mode: Privileged

no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format: `no debug igmpsnooping packet`

Command mode: Privileged

debug igmpsnooping packet transmit

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

Default: disabled

Format: `debug igmpsnooping packet transmit`

Command mode: Privileged

Parameter	*Value*
TX	The packet sent by the device.
Intf	The interface from which the packet came out. Used format — unit/slot/port (inner interface number). For device interfaces outside the stack, the unit is always displayed as 1.
Src_Mac	MAC address of the packet source.
Dest_Mac	Group destination MAC address of the packet
Src_IP	The source IP address in the IP header of the packet.
Dest_IP	Group destination IP address of the packet
Type	IGMP packet type. The type can take one of the following values: • Membership Query – IGMP Membership Query • V1_Membership_Report – IGMP Membership Report, version 1 • V2_Membership_Report – IGMP Membership Report, version 2 • V3_Membership_Report – IGMP Membership Report, version 3 • V2_Leave_Group – IGMP Leave Group, version 2
Group	Group multicast address in IGMP header

no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format: `no debug igmpsnooping transmit`

Command mode: Privileged

debug igmpsnooping packet receive

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

Default: disabled

Format: `debug igmpsnooping packet receive`

Command mode: Privileged

Parameters displayed in the trace message

Parameter	*Value*
TX	The packet sent by the device.
Intf	The interface from which the packet came out. Used format — unit/slot/port (inner interface number). For device interfaces outside the stack, the unit is always displayed as 1.
Src_Mac	MAC address of the packet source.
Dest_Mac	Group destination MAC address of the packet
Src_IP	The source IP address in the IP header of the packet.
Dest_IP	Group destination IP address of the packet
Type	IGMP packet type. The type can take one of the following values: • Membership Query – IGMP Membership Query • V1_Membership_Report – IGMP Membership Report, version 1 • V2_Membership_Report – IGMP Membership Report, version 2 • V3_Membership_Report – IGMP Membership Report, version 3 • V2_Leave_Group – IGMP Leave Group, version 2
Group	Group multicast address in IGMP header

no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format: `no debug igmpsnooping receive`

Command mode: Privileged

debug ip acl

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Default: disabled

Format: `debug ip acl` *`acl Number`*

Command mode: Privileged

no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

Format: `no debug ip acl` *`acl Number`*

Command mode: Privileged

debug ip bgp

Use this command to enable BGP packet debug trace. Debug messages are sent to the system log at the DEBUG severity level. To print the debug messages to the console, enable console logging at the DEBUG level using the command logging console debug. The debug options enabled for a specific peer are the union of the options enabled globally and the options enabled specifically for the peer. Enabling one of the packet type options enables packet tracing in both the inbound and outbound directions.

Default: disabled

Format: `debug ip bgp [vrf` *`vrf-name`*`] {`*`ipv4-address`*`|`*`ipv6-address`*`} [ events | in | interface {`*`unit/slot/port`*` | vlan `*`1-4093`*`} | keepalives | notification | open | out | refresh | updates ]`

Command mode: Privileged

Parameter	*Description*
peer-address	(Optional) The IPv4 address of a BGP peer. Debug traces are enabled for a specific peer when this option is specified. The command can be issued multiple times to enable simultaneous tracing for multiple peers.
events	(Optional) Trace adjacency state events
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.
refresh	(Optional) Traces transmit and receive of ROUTE REFRESH packets.
updates	(Optional) Traces transmit and receive of UPDATE packets.

no debug bgp

Use this command to disable debug tracing of BGP events.

Format: `no debug ip bgp [`*`peer-address`*`|events|keepalives|notification|open|refresh|updates]`

Command mode: Privileged

debug ip vrrp

Use this command to enable VRRP debug protocol messages.

Default: disabled

Format: `debug ip vrrp`

Command mode: Privileged

no debug ip vrrp

Use this command to disable VRRP debug protocol messages.

Format: `no debug ip vrrp`

Command mode: Privileged

debug ipv6 dhcp

This command displays debug information about DHCPv6 client activities and traces DHCPv6 packets to and from the local DHCPv6 client.

Default: disabled

Format: `debug ipv6 dhcp`

Command mode: Privileged

no debug ipv6 dhcp

This command disables the display of “debug” trace output for DHCPv6 client activity.

Format: `no debug ipv6 dhcp`

Command mode: Privileged

debug ipv6 ospfv3 packet

Use this command to enable IPv6 OSPFv3 packet debug trace.

Default: disabled

Format: `debug ipv6 ospfv3 packet`

Command mode: Privileged

no debug ipv6 ospfv3 packet

Use this command to disable tracing of IPv6 OSPFv3 packets.

Format: `no debug ipv6 ospfv3 packet`

Command mode: Privileged

debug lacp packet

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

Default: disabled

Format: `debug lacp packet`

Command mode: Privileged

no debug lacp packet

This command disables tracing of LACP packets.

Format: `no debug lacp packet`

Command mode: Privileged

debug mldsnooping packet

Use this command to trace MLD snooping packet reception and transmission. **receive** traces only received MLD snooping packets and **transmit** traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default: disabled

Format: `debug mldsnooping packet [receive | transmit]`

Command mode: Privileged

no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

debug ospf packet

This command enables tracing of OSPF packets received and transmitted by the switch or, optionally, a virtual router can be specified.

Default: disabled

Format: `debug ospf packet [vrf` *`vrf-name`*`]`

Command mode: Privileged

Parameters displayed in the trace message

Parameter	*Value*
TX/RX	TX — packets sent by the device. RX — packets received by the device
Intf	The interface through which the packet came in or out of. Used format — unit/slot/port (inner 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 remaining fields in the trace are specific to the type of OSPF Packet. HELLO packet field definitions:

Parameter	*Value*
Netmask	The netmask in the hello packet.
DesignRouter	Designated Router IP address
Backup	Backup router IP address

DB_DSCR packet field definitions:

Field	*Value*
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:

Field	*Value*
Length	Packet length

LS_UPD packet field definitions:

Field	*Value*
Length	Packet length

LS_ACK packet field definitions:

Field	*Value*
Length	Packet length

no debug ospf packet

This command disables tracing of OSPF packets.

Format: `no debug ospf packet`

Command mode: Privileged

debug ospfv3 packet

Use this command to enable OSPFv3 packet debug trace.

Default: disabled

Format: `debug ospfv3 packet`

Command mode: Privileged

no debug ospfv3 packet

Use this command to disable tracing of OSPFv3 packets.

Format: `no debug ospfv3 packet`

Command mode: Privileged

debug ping packet

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

Default: disabled

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

Command mode: Privileged

Parameter	*Value*
TX/RX	TX — packets sent by the device. RX — packets received by the device
Intf	The interface through which the packet came in or out of. Used format — unit/slot/port (inner interface number). For device interfaces outside the stack, the unit is always displayed as 1.
SRC_IP	The source IP address in the IP header of the packet
DEST_IP	The destination IP address in the IP header of the packet
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format: `no debug ping packet`

Command mode: Privileged

debug rip packet

This command turns on tracing of RIP requests and responses. This command takes no options. The output is directed to the log file.

Default: disabled

Format: `debug rip packet`

Command mode: Privileged

The following parameters are displayed in the trace message:

Field	*Value*
TX/RX	TX — packets sent by the device. RX refers to packets received by the device.
Intf	The interface through which the packet came in or out of. Used format — unit/slot/port (inner interface number). For device interfaces outside the stack, the unit is always displayed as 1.
SRC_IP	The source IP address in the IP header of the packet.
DEST_IP	The destination IP address in the IP header of the packet.
Rip_Version	RIP version used: RIPv1 or RIPv2.
Packet_Type	Type of RIP packet: RIP_REQUEST or RIP_RESPONSE
Routes	Up to 5 routes in the packet are displayed in the following format: Network: a.b.c.d Mask a.b.c.d Next_Hop a.b.c.d Metric a The next hop is only displayed if it is different from 0.0.0.0. For RIPv1 packets, Mask is always 0.0.0.0.
Number of routes not printed	Only the first five routes present in the packet are included in the trace. There is another notification of the number of additional routes present in the packet that were not included in the trace.

no debug rip packet

This command disables tracing of RIP requests and responses.

Format: `no debug rip packet`

Command mode: Privileged

debug sflow packet

Use this command to enable sFlow debug packet trace.

Default: disabled

Format: `debug sflow packet`

Command mode: Privileged

no debug sflow packet

Use this command to disable sFlow debug packet trace.

Format: `no debug sflow packet`

Command mode: Privileged

debug spanning-tree bpdu

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

Default: disabled

Format: `debug spanning-tree bpdu`

Command mode: Privileged

no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format: `no debug spanning-tree bpdu`

Command mode: Privileged

debug spanning-tree bpdu receive

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

Default: disabled

Format: `debug spanning-tree bpdu receive`

Command mode: Privileged

Field	*Value*
TX/RX	TX — packets sent by the device. RX — packets received by the device
Intf	The interface through which the packet came in or out of. Used format — unit/slot/port (inner interface number). For device interfaces outside the stack, the unit is always displayed as 1.
Source_Mac	MAC address of the packet source.
Version	Version of the spanning tree rotocol (0–3). 0 means STP, 2 - RSTP, 3 - MSTP
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	CIST root bridge priority. Permissible value: from 0 to 61440. It is displayed in hex in multiples of 4096
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format: `no debug spanning-tree bpdu receive`

Command mode: Privileged

debug spanning-tree bpdu transmit

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

Default: disabled

Format: `debug spanning-tree bpdu transmit`

Command mode: Privileged

Field	*Value*
TX/RX	TX — packets sent by the device. RX — packets received by the device
Intf	The interface through which the packet came in or out of. Used format — unit/slot/port (inner interface number). For device interfaces outside the stack, the unit is always displayed as 1.
Source_Mac	MAC address of the packet source.
Version	Version of the spanning tree rotocol (0–3). 0 means STP, 2 - RSTP, 3 - MSTP
Root_Mac	MAC address of the CIST root bridge
Root_Priority	CIST root bridge priority. Permissible value: from 0 to 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format: `no debug spanning-tree bpdu transmit`

Command mode: Privileged

debug tacacs

Use the debug tacacs packet command to turn on TACACS+ debugging.

Format: `debug tacacs {packet [receive | transmit] | accounting | authentication}`

Command mode: Global Config

Parameter	*Description*
packet receive	Turn on TACACS+ receive packet debugs.
packet transmit	Turn on TACACS+ transmit packet debugs.
accounting	Turn on TACACS+ authentication debugging.
authentication	Turn on TACACS+ authorization debugging.

debug telnetd start

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

Format: `debug telnetd start [password][port]`

Command mode: Privileged

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

debug telnetd stop

Use this command to stop the telnet daemon previously started by the debug telnetd start command.

Format: `debug telnetd stop`

Command mode: Privileged

debug transfer

This command enables debugging for file transfers.

Format: `debug transfer`

Command mode: Privileged

no debug transfer

This command disables debugging for file transfers.

Format: `no debug transfer`

Command mode: Privileged

debug udld events

This command enables debugging for the UDLD events.

Default: disabled

Format: `debug udld events`

Command mode: Privileged

debug udld packet receive

This command enables debugging on the received UDLD PDU's.

Default: disabled

Format: `debug udld packet receive`

Command mode: Privileged

debug udld packet transmit

This command enables debugging on the transmitted UDLD PDU's.

Default: disabled

Format: `debug udld packet transmit`

Command mode: Privileged

show debugging

Use this command to display enabled packet tracing configurations.

Format: `show debugging`

Command mode: Privileged

exception protocol

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

Default: none

Format: `exception protocol {nfs | tftp | ftp | local | usb | none}`

Command mode: Global Config

no exception protocol

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

Format: `no exception protocol`

Command mode: Global Config

exception dump tftp-server

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

Default: none

Format: `exception dump tftp-server {ip-address}`

Command mode: Global Config

no exception dump tftp-server

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

Format: `no exception dump tftp-server`

Command mode: Global Config

exception dump nfs

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

Default: none

Format: `exception dump nfs ip-address/dir`

Command mode: Global Config

no exception dump nfs

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

Format: `no exception dump nfs`

Command mode: Global Config

exception dump filepath

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

Default: none

Format: `exception dump filepath` *`dir`*

Command mode: Global Config

no exception dump filepath

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

Format: `exception dump filepath`

Command mode: Global Config

exception core-file

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

If hostname is selected:

`file-name-prefix_hostname_Time_Stamp.bin`

If hostname is not selected:

`file-name-prefix_MAC_Address_Time_Stamp.bin`

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

Default: core

Format: `exception core-file {`*`file-name-prefix`* `| [hostname] | [time-stamp]}`

Command mode: Global Config

no exception core-file

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

Default: core

Format: `no exception core-file`

Command mode: Global Config

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.

Default: disabled

Format: `exception switch-chip-register {enable | disable}`

Command mode: Global Config

exception dump ftp-server

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

Default: none

Format: `exception dump ftp-server` *`ip-address`* `[{username` *`user-name`* `password` *`password`*`}]`

Command mode: Global Config

no exception dump ftp-server

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

Default: none

Format: `no exception dump ftp-server`

Command mode: Global Config

exception dump compression

This command enables compression mode.

Default: enabled

Format: `exception dump compression`

Command mode: Global Config

no exception dump compression

This command disables compression mode.

Default: none

Format: `no exception compression`

Command mode: Global Config

exception dump stack-ip-address protocol

This command configures protocol (dhcp or static) to be used to configure service port when a unit has crashed. If configured as dhcp then the unit gets the IP address from dhcp server available in the network.

Default: DHCP

Format: `exception dump stack-ip-address protocol {dhcp | static}`

Command mode: Global Config

no exception dump stack-ip-address protocol

This command resets stack IP protocol configuration (dhcp or static) to its default value.

Default: none

Format: `no exception dump stack-ip-address protocol`

Command mode: Global Config

exception dump stack-ip-address add

This command adds static IP address to be assigned to individual unit's service port in the stack when the switch has crashed. This IP address is used to perform the core dump.

Default: none

Format: `exception dump stack-ip-address add` *`ip-address netmask`* [*`gateway`*]

Command mode: Global Config

exception dump stack-ip-address remove

This command removes stack IP address configuration. If this IP address is assigned to any unit in the stack then this IP is removed from the unit.

Default: none

Format: `exception dump stack-ip-address remove` *`ip-address netmask`*

Command mode: Global Config

exception nmi

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

Default: disabled

Format: `exception nmi {enable | disable}`

Command mode: Global Config

write core

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

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

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

Default: none

Format: `write core [test [`*`dest_file_name`*`]]`

Command mode: Privileged

debug exception

The command displays core dump features support.

Default: none

Format: `debug exception`

Command mode: Privileged

show exception

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

Default: none

Format: `show exception`

Command mode: Privileged

show exception core-dump-file

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

Default: none

Format: `show exception core-dump-file`

Command mode: priveleged or configuration mode

show exception log

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

Default: none

Format: `show exception log [previous]`

Command mode: priveleged or configuration mode

mbuf

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

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

Command mode: Global Config

Field	*Description*
rising threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. Valid values: from 1 to 100. Default value — 0 (disabled).
falling threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. Valid values: from 1 to 100. Default value — 0 (disabled).
Severity	The severity level at which Mbuf logs messages. Valid values: from 1 to 7. Default: 5 (L7_LOG_SEVERITY_NOTICE).

show mbuf total

Use this command to display memory buffer (MBUF) information.

Format: `show mbuf total`

Command mode: Privileged

Field	*Description*
Mbufs Total	Total number of message buffers in the system.
Mbufs Free	Number of message buffers currently available.
Mbufs Rx Used	Number of message buffers currently in use.
Total Rx Norm Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Norm.
Total Rx Mid2	Number of times the system tried to allocate a message buffer allocation of class RX Mid2.

Total Rx Mid1 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid1.
Total Rx Mid0 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid0.
Total Rx High Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX High.
Total Tx Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class TX.
Total Rx Norm Alloc Failures	Number of message buffer allocation failures for RX Norm class of message buffer.
Total Rx Mid2 Alloc Failures	Number of message buffer allocation failures for RX Mid2 class of message buffer.
Total Rx Mid1 Alloc Failures	Number of message buffer allocation failures for RX Mid1 class of message buffer.
Total Rx Mid0 Alloc Failures	Number of message buffer allocation failures for RX Mid0 class of message buffer.
Total Rx High Alloc Failures	Number of message buffer allocation failures for RX High class of message buffer.
Total Tx Alloc Failures	Number of message buffer allocation failures for TX class of message buffer.

show msg-queue

Use this command to display the message queues.

Default: none

Format: `show msg-queue`

Command mode: Privileged

debug packet-trace

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

Default: none

Format: `debug packet-trace`

Command mode: Privileged

session start

Use this command to initiate a console session from the stack master to another unit in the stack, or from a member unit to a manager or another member unit. During the session, troubleshooting and debugging commands can be issued on the member unit, and the output displays the relevant information from the member unit specified in the session. Commands are displayed on the member unit using the user help option.

Default: disabled

Format: `session start {unit` *`unit-number`* `| manager}`

Command mode: Global Config

Parameter	Description
unit	Use to connect to the specified unit from the stack master.
manager	Use to connect directly to the manager unit from any member unit without entering the manager's unit number.

session stop

Use this command to terminate a session started from a manager to a member, a member to a member, or a member to manager that was started with the session start command.

Default: disabled

Format: `session stop`

Command mode: Global Config

6.16 Cable Test commands

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

The cable test feature is supported only for copper cable. It is not supported for optical fiber cable.

If the port has an active link while the cable test is run, the link can go down for the duration of the test.

cablestatus

This command returns the status of the specified port.

Format: `cablestatus` *`unit/slot/port`*

Command mode: Privileged

Field	Description
Cable Status	One of the following statuses is returned: • **Normal:** The cable is working correctly. • **Open:** The cable is disconnected or there is a faulty connector. • **Short:** There is an electrical short in the cable. • **Cable Test Failed:** The cable status could not be determined. The cable may in fact be working. • **Crosstalk:** There is crosstalk present on the cable. • **No Cable:** There is no cable present.
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

6.17 sFlow commands

sFlow is the standard for monitoring high-speed switched and routed networks. SFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

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.

Format: `sflow poller {rcvr-indx | interval poll-interval}`

Command mode: Interface Config

Field	*Description*
Receiver Index	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. Default: 0
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. Default: zero (0). A value of N means once in N seconds a counter sample is generated.

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 taskis 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:
The maximum number of allowed interfaces for the polling intervals max (1, (interval – 10)) to min ((interval + 10), 86400) is:interval * 5.
For every one second increment in the polling interval that is configured, the number of allowed interfaces that can be configured increases by 5.

no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

Format: `no sflow poller [interval]`

Command mode: Interface Config

sflow receiver

Use this command to configure the sFlow collector parameters.

Format: `no sflow receiver index {ip ip-address | maxdatagram size | owner string timeout interval | port 14-port}`

Command mode: Global Config

Parameter	*Description*
index	Receiver index. Valid values: from 1 to 8
owner	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. Default: blank. The null string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.
timeout	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0–2147483647 seconds. The default is zero (0).
notimeout	The configured entry will be in the config until you explicitly removes the entry.
maxdatagram	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The range is 200–9116. Default: 1400.
ip	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. Default: 0.0.0.0.
port	The destination Layer4 UDP port for sFlow datagrams. The range is 1–65535. Default: 6343.

no sflow receiver

Use this command to set the sFlow collector parameters back to the defaults.

Format: `no sflow receiver indx {ip ip-address | maxdatagram size | owner string timeout interval | port 14-port}`

Command mode: Global Config

sflow receiver owner timeout

Use this command to configure a receiver as a timeout entry. As the sFlow receiver is configured as a timeout entry, information related to sampler and pollers are also shown in the running-config and are retained after reboot.

Format: `sflow receiver` *`index`* `owner` *`owner-string`* `timeout`

Command mode: Global Config

sflow receiver owner notimeout

Use this command to configure a receiver as a non-timeout entry. Unlike entries configured with a specific timeout value, this command will be shown in show running-config and retained after reboot. As the sFlow receiver is configured as a non-timeout entry, information related to sampler and pollers will also be shown in the running-config and will be retained after reboot.

Format: `sflow receiver` *`index`* `owner` *`owner-string`* `notimeout`
Command mode: Global Config

sflow sampler

A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance on an interface or range of interfaces for this data source if rcvr_idx is valid.

Format: `sflow sampler {rcvr-indx | rate sampling-rate | maxheadersize size}`

Command mode: Interface Config

Field	*Description*
rcvr-indx	The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. A value of zero (0) means that no receiver is configured, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. Possible values are: 1–8. Default: zero (0).
maxheadersize	The maximum number of bytes that should be copied from the sampler packet. The range is 20–256. Default: 128. When set to zero (0), all the sampler parameters are set to their corresponding default value.
rate	The statistical sampling rate for packet sampling from this source. A value of zero (0) disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. The range is 1024–65536 and 0. Default: 0

no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

Format: `no sflow sampler {rcvr-indx | rate sampling-rate | maxheadersize size}`

Command mode: Interface Config

sflow sampler rate

Use this command to set the sampling rate for ingress sampling.

Default: 0 for the ingress sampling rate.

Format: `sflow sampler rate value`

Command mode: Interface Config

no sflow sample rate

Use this command to remove the sampling rate for ingress sampling.

Format: `no sflow sampler rate`

Command mode: Interface Config

sflow source-interface

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

Format: `sflow source-interface {unit/slot/port | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}`

Command mode: Global Config

Parameter	*Description*
unit/slot/port	VLAN or port-based routing interface
loopback-id	Configures the loopback interface to use as the source IP address. The range of the loopback ID is from 0 to 7
tunnel-id	Configures the tunnel interface to use as the source IP address. The range of the tunnel ID is from 0 to 7
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN identifier: 1–4093.

no sflow source-interface

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

Format: `no sflow source-interface`

Command mode: Global Config

show sflow agent

Use this command to display the sFlow agent information.

Format: `show sflow agent`

Command mode: Privileged

Field	*Description*
sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: MIB Version: 1.3, the version of this MIB. Organization: Corp. Revision: 1.0
IP Address	The IP address associated with this agent.

show sflow pollers

Use this command to display the sFlow polling instances created on the switch.

Format: `show sflow pollers`

Command mode: Privileged

Field	*Description*
Poller Data Source	sFlowDataSource (slot/port) for this sFlow poller. This agent supports only physical ports
Receiver Index	The sFlow Receiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

Format: `show sflow receivers [index]`

Command mode: Privileged

Parameter	*Description*
Receiver Index	The sFlow Receiver associated with the sampler/poller.
Owner String	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry
Time Out	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. The no timeout value of this parameter means that the sFlow receiver is configured as a non-timeout entry.
Max Datagram Size	The maximum number of bytes that can be sent in a single sample datagram.
Port	The destination UDP port for sFlow datagrams.
IP adress	The sFlow receiver IP address
Address Type	The sFlow receiver IP address ензу. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.
Datagram Version	The sFlow protocol version to be used while sending samples to sFlow receiver.

show sflow source-interface

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

Format: `show sflow source-interface`

Command mode: Privileged

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

6.18 SDM Template configuration commands

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

If you attach a unit to a stack and its template does not match the stack's template, the new unit will automatically reboot using the template used by other stack members. To avoid the automaticreboot, you may first set the template to the template used by existing members of the stack. Then power off the new unit, attach it to the stack, and power it on.

sdm prefer

Use this command to change the template that will be active after the next reboot. The keywords are as follows:

- **dual-ipv4-and-ipv6** — Filters subsequent template choices to those that support both IPv4 and IPv6. The default template 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 support increases the number of ECMP next hops to 32.
- **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.

After setting the template, you must reboot in order for the configuration change to take effect.

Default: dual-ipv4-and-ipv6

Format: `sdm prefer {dual-ipv4-and-ipv6 {default | data-center } | ipv4-routing {default | {data-center {default | plus}}}`

Command mode: Global Config

no sdm prefer

Use this command to revert to the default template after the next reboot.

Format: `no sdm prefer`

Command mode: Global Config

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.

Format: `show sdm prefer [dual-ipv4-and-ipv6 {default | data-center} | ipv4-routing {default | data-center {default | plus}} ]`

Command mode: Privileged

Parameter	*Description*
dual-ipv4-and-ipv6 default	(Optional) List the scaling parameters for the template supporting IPv4 and IPv6.
dual-ipv4-and-ipv6 data-center	(Optional) List the scaling parameters for the Dual IPv4 and IPv6 template supporting more ECMP next hops.
ipv4-routing default	(Optional) List the scaling parameters for the IPv4-only

	template maximizing the number of unicast routes.
ipv4-routing data-center default	(Optional) List the scaling parameters for the IPv4-only template supporting more ECMP next hops.
ipv4-routing data-center plus	(Optional) List the scaling parameters for the IPv4-only template maximizing the number of unicast routes and also supporting more ECMP next hops.

Field	*Description*
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

6.19 Remote Monitoring commands

Remote Monitoring (RMON) is a method of collecting a variety of data about network traffic. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).

There is no configuration command for ether stats and high capacity ether stats. The data source for ether stats and high capacity ether stats are configured during initialization.

rmon alarm

This command sets the RMON alarm entry in the RMON alarm MIB group.

Format: `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`*`]`

Command mode: Global Config

Parameter	*Description*
Alarm Index	An index that uniquely identifies a record in the alert table. Each entry defines a diagnostic sample at a particular interval for an object on the device. Valid values: from 1 to 65535.
Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
Alarm Interval	The interval in seconds over which data is sampled and compared with the lower and upper thresholds. Valid values: from 1 to 2147483647. Default: 1.
Alarm Rising Threshold	Upper notification threshold. Valid values: from 2147483648 to 2147483647. Default: 1.
Alarm Rising Event Index	The index of the eventEntry event object that is used

	when crossing the upper threshold. Valid values: from 1 to 65535. Default: 1
Alarm Falling Threshold	Lower notification threshold. Valid values: from 2147483648 to 2147483647. Default: 1.
Alarm Falling Event Index	The index of the eventEntry event object that is used when crossing the lower threshold. Valid values: from 1 to 65535. Default: 2
Alarm Startup Alarm	Notification that should be sent. Possible values are: `rising`, `falling` or `rising-falling`. Default: `rising-falling`.
Alarm Owner	Owner name string associated with the alert record. Default: `monitorAlarm`.

no rmon alarm

This command deletes the RMON alarm entry.

Format: `no rmon alarm` *`alarm number`*

Command mode: Global Config

rmon hcalarm

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

Format: `rmon hcalarm` *`alarm 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`*]

Command mode: Global Config

Parameter	*Description*
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. Valid values: from 1 to 65535.
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that are of the primitive ASN.1 integer type are allowed.
High Capacity Alarm Interval	The interval in seconds over which data is sampled and compared with the lower and upper thresholds. Valid values: from 1 to 2147483647. Default: 1
High Capacity Alarm Sample Type	The method of fetching a variable and calculating the value that will be compared with the thresholds. Possible types: Absolute Value or Delta Value. Default: Absolute Value.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject).
High Capacity Alarm Startup Alarm	Possible status types: valueNotAvailable, valuePositive or valueNegative. Default: valueNotAvailable. Notification that should be sent. High capacity alarm startup alarm that may be sent.

	Possible values are: rising, falling or rising-falling. Default: rising-falling.
High Capacity Alarm Rising- Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. Valid values: from 0 to 4294967295. Default: 1
High Capacity Alarm Rising- Threshold Absolute Value High	The upper 32 bits of the absolute value of the upper threshold for the alert. Valid values: from 0 to 4294967295. Default: 0
High Capacity Alarm Rising- Threshold Value Status	The sign of the number of upper thresholds defined by objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are: valueNotAvailable, valuePositive, or valueNegative. Default: valuePositive.
High Capacity Alarm Falling- Threshold Absolute Value Low	The lower 32 bits of the absolute value of the lower threshold for the alert. Valid values: from 0 to 4294967295. Default: 1
High Capacity Alarm Falling- Threshold Absolute Value High	The upper 32 bits of the absolute value of the lower threshold for the alert. Valid values: from 0 to 4294967295. Default: 0
High Capacity Alarm Falling- Threshold Value Status	The sign of the number of lower thresholds defined by objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are: valueNotAvailable, valuePositive, or valueNegative. Default: valuePositive
High Capacity Alarm Rising Event Index	The index of the eventEntry event object that is used when crossing the upper threshold. Valid values: from 1 to 65535. Default: 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry event object that is used when crossing the lower threshold. Valid values: from 1 to 65535. Default: 2.
High Capacity Alarm Owner	Owner name string associated with the alert record. Default: monitorHCAlarm.

no rmon hcalarm

Removes RMON hcalarm entry.

Format: `no rmon hcalarm` *`alarm number`*

Command mode: Global Config

rmon event

This command sets the RMON event entry in the RMON event MIB group.

Format: `rmon event` *`event number`* `[description` *`string`*`|log|owner` *`string`*`|trap` *`community`*`]`

Command mode: Global Config

Parameter	Description
Event Index	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. Valid values: from 1 to 65535.
Event Description	Comment that describes the event object. Default: alarmEvent
Event Type	Evevnt notification type. Possible values are: None, Log, SNMP Trap, Log and SNMP Trap. Default: None.
Event Owner	Owner name string associated with the record. Default: monitorEvent.
Event Community	The SNMP community specific by this octet string which is used to send an SNMP trap. Default: public

no rmon event

This command deletes the rmon event entry.

Format: `no rmon event` *`event number`*

Command mode: Global Config

rmon collection history

This command sets the history control parameters of the RMON historyControl MIB group.

This command is not supported on interface range. Each RMON history control collection entry can be configured on only one interface. If you try to configure on multiple interfaces, DUT displays anerror.

Format: `rmon collection history` *`index number`* [`buckets` *`number`*|`interval` *`interval in sec`*|`owner` *`string`*]

Command mode: Interface Config

Parameter	Description
History Control Index	An index that uniquely identifies a record in the historyControl table. Each such record describes a series of samples for a certain interval for an interface on a device. Valid values: from 1 to 65535.
History Control Data Source	The source interface on which the data is collected.
History Control Buckets Requested	The required number of time intervals for which data should be stored. Valid values: from 1 to 65535. Default: 50
History Control Interval	Data sampling interval in seconds. Valid values: from 1 to 3600. Default: 1800.
History Control Owner	Owner name string associated with the collection history management record. Default: monitorHistoryControl.

no rmon collection history

This command will delete the history control group entry with the specified index number.

Format: `no rmon collection history` *index number*

Command mode: Interface Config

show rmon

This command displays the entries in the RMON alarm table.

Format: `show rmon {alarms | alarm` *alarm-index*`}`

Command mode: Privileged

Parameter	*Description*
Alarm Index	An index that uniquely identifies a record in the alert table. Each entry defines a diagnostic sample at a particular interval for an object on the device. Valid values: from 1 to 65535.
Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that are of the primitive ASN.1 integer type are allowed.
Alarm Interval	The interval in seconds over which data is sampled and compared with the lower and upper thresholds. Valid values: from 1 to 2147483647. Default: 1.
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
Alarm Rising Threshold	Upper notification threshold. Valid values: from 2147483648 to 2147483647. Default: 1.
Alarm Rising Event Index	The index of the eventEntry event object that is used when crossing the upper threshold. Valid values: from 1 to 65535. Default: 1.
Alarm Falling Threshold	Lower notification threshold. Valid values: from 2147483648 to 2147483647. Default: 1
Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. Valid values: from 1 to 65535. Default: 2.
Alarm Startup Alarm	The alarm that may be sent. Possible values are: rising, falling or rising-falling. Default: rising-falling.
Alarm Owner	Owner name string associated with the alert record. Default: monitorAlarm

show rmon collection history

This command displays the entries in the RMON history control table.

Format: `show rmon collection history [interfaces` *unit/slot/port*`]`

Command mode: Privileged

Parameter	*Description*
History Control Index	An index that uniquely identifies a record in the historyControl table. Each such record describes a series of samples for a certain interval for an interface on a

	device. Valid values: from 1 to 65535
History Control Data Source	The source interface on which the data is collected.
History Control Buckets Requested	The required number of time intervals for which data should be stored. Valid values: from 1 to 65535. Default: 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only Default: 10
History Control Interval	Data sampling interval in seconds. Valid values: from 1 to 3600. Default: 1800.
History Control Owner	The owner string associated with the history control entry. Default: monitorHistoryControl

show rmon events

This command displays the entries in the RMON event table.

Format: `show rmon events`

Command mode: Privileged

Parameter	*Description*
Event Index	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. Valid values: from 1 to 65535
Event Description	Comment that describes the event object. Default: alarmEvent.
Event Type	Evevnt notification type. Possible values are: None, Log, SNMP Trap, Log and SNMP Trap. Default: None
Owner	Owner name string associated with the record. Default: monitorEvent
Event Community	The SNMP community specific by this octet string which is used to send an SNMP trap. Default: public.
Last time sent	The last time over which a log or a SNMP trap message is generated.

show rmon history

This command displays the specified entry in the RMON history table.

Format: `show rmon history` *`index`* `{errors [period` *`seconds`*`]|other [period` *`seconds`*`]|throughput [period` *`seconds`*`]}`

Command mode: Privileged

Parameter	*Description*
History Control Index	An index that uniquely identifies a record in the historyControl table. Each such record describes a series of samples for a certain interval for an interface on a device. Valid values: from 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The required number of time intervals for which data should be stored. Range — from 1 to 65535. Default: 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. The object is read-only. Default: 10

History Control Interval	Data sampling interval in seconds. Valid values: from 1 to 3600. Default: 1800
History Control Owner	Owner name string associated with the collection history management record. Default: monitorHistoryControl
Maximum Table Size	Maximum number of entries that the history table can hold.
Time	Time at which the sample is collected, displayed as period seconds.
CRC Align	Number of CRC align errors.
Undersize Packets	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Packets	The total number of oversized packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	The total number of fragmented packets. Packets, the number of octets in which is not integer, and packets with an erroneous checksum of less than 64 octets (excluding the interframe interval, but taking into account the packet checksum octets).
Jabbers	The total number of failured packets. Packets, the number of octets in which is not integer, and packets with an erroneous checksum of more than 1518 octets (excluding the interframe interval, excluding coding bits, but taking into account the packet checksum octets).
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 Broadcast packets received on the interface.
Multicast	Total number of good Multicast packets received on the interface.
Util	Port utilization of the interface associated with the history index specified.
Dropped Collisions	Total number of dropped collisions.

show rmon log

This command displays the entries in the RMON log table.

Format: `show rmon log [`*`event-index`*`]`

Command mode: Privileged

Parameter	*Description*
Maximum table size	Maximum number of entries that the log table can hold.
Event	Event index for which the log is generated.
Description	A comment describing the event entry for which the log is generated.
Time	Time at which the event is generated.

show rmon statistics interfaces

This command displays the RMON statistics for the given interfaces.

Format: `show rmon statistics interfaces` *unit/slot/port*

Command mode: Privileged

Parameter	*Description*
Port	Port number in unit/slot/port format.
Dropped	Total number of dropped events on the interface.
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 Multicast packets received on the interface.
Multicast	Total number of good Multicast packets received on the interface.
CRC Align Errors	Total number of packets received have a length (excluding framing bits, including FCS octets) of between 64 and 1518 octets inclusive.
Collisions	Total number of collisions on the interface.
Undersize Pkts	The total number of undersized packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Pkts	The total number of oversized packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	The total number of fragmented packets. Packets, the number of octets in which is not integer, and packets with an erroneous checksum of less than 64 octets (excluding the interframe interval, but taking into account the packet checksum octets).
Jabbers	The total number of failured packets. Packets, the number of octets in which is not integer, and packets with an erroneous checksum of more than 1518 octets (excluding the interframe interval, excluding coding bits, but taking into account the packet checksum octets).
64 Octets	Total number of packets which are 64 octets in length (excluding framing bits, including FCS octets).
65-127 Octets	Total number of packets which are between 65 and 127 octets in length (excluding framing bits, including FCS octets).
128-255 Octets	Total number of packets which are between 128 and 255 octets in length (excluding framing bits, including FCS octets).
256-511 Octets	Total number of packets which are between 256 and 511 octets in length (excluding framing bits, including FCS octets).
512-1023 Octets	Total number of packets which are between 512 and 1023 octets in length (excluding framing bits, including FCS octets).
1024-1518 Octets	Total number of packets which are between 1024 and 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 which are 64 octets in length.
HC Overflow Pkts 65 - 127 Octets	Total number of HC overflow packets which are between 65 and 127 octets in length.
HC Overflow Pkts 128 - 255 Octets	Total number of HC overflow packets which are between

	128 and 255 octets in length.
HC Overflow Pkts 256 - 511 Octets	Total number of HC overflow packets which are between 256 and 511 octets in length.
HC Overflow Pkts 512 - 1023 Octets	Total number of HC overflow packets which are between 512 and 1023 octets in length.
HC Overflow Pkts 1024 - 1518 Octets	Total number of HC overflow packets which are between 1024 and 1518 octets in length.

show rmon hcalarms

This command displays the entries in the RMON high-capacity alarm table.

Format: `show rmon {hcalarms|hcalarm` *`alarm index`*`}`

Command mode: Privileged

Parameter	*Description*
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. Valid values: from 1 to 65535
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that are of the primitive ASN.1 integer type are allowed.
High Capacity Alarm Interval	The interval in seconds over which data is sampled and compared with the lower and upper thresholds. Valid values: from 1 to 2147483647. Default: 1.
High Capacity Alarm Sample Type	The method of fetching a variable and calculating the value that will be compared with the thresholds. Possible types: Absolute Value or Delta Value. Default: Absolute Value
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types: valueNotAvailable, valuePositive or valueNegative. Default: valueNotAvailable.
High Capacity Alarm Startup Alarm	Notification that should be sent. Possible values are: rising, falling or rising-falling. Default: rising-falling.
High Capacity Alarm Rising- Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. Valid values: from 0 to 4294967295. Default: 1.
High Capacity Alarm Rising- Threshold Absolute Value High	The upper 32 bits of the absolute value of the upper threshold for the alert. Valid values: from 0 to 4294967295. Default: zero (0).
High Capacity Alarm Rising- Threshold Value Status	The sign of the number of upper thresholds defined by objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are: valueNotAvailable, valuePositive, or valueNegative.

	Default: valuePositive.
High Capacity Alarm Falling- Threshold Absolute Value Low	The lower 32 bits of the absolute value of the lower threshold for the alert. Valid values: from 0 to 4294967295. Default: 1.
High Capacity Alarm Falling- Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. Valid values: from 0 to 4294967295. Default: zero (0).
High Capacity Alarm Falling- Threshold Value Status	The sign of the number of lower thresholds defined by objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are: valueNotAvailable, valuePositive, or valueNegative. Default: valuePositive.
High Capacity Alarm Rising Event Index	The index of the eventEntry event object that is used when crossing the upper threshold. Valid values: from 1 to 65535. Default: 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry event object that is used when crossing the lower threshold. Valid values: from 1 to 65535. Default: 2
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of the hcAlarmEntry (while in the active state) and the value was not available.
High Capacity Alarm Owner	Owner name string associated with the alert record. Default: monitorHCAlarm.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. The object is read-only. Default: volatile

6.20 Statistics Application commands

The statistics application gives you the ability to query for statistics on port utilization, flow-based and packet reception on programmable time slots. The statistics application collects the statistics at a configurable time range. You can specify the port number(s) or a range of ports for statistics to be displayed. The configured time range applies to all ports. Detailed statistics are collected between a specified time range in date and time format. You can define the time range as having an absolute time entry and/or a periodic time. For example, you can specify the statistics to be collected and displayed between 9:00 12 NOV 2011 (START) and 21:00 12 NOV 2012 (END) or schedule it on every Mon, Wed, and Fri 9:00 (START) to 21:00 (END).

You can receive the statistics in the following ways:

• User requests through the CLI for a set of counters.

• Configuring the device to display statistics using syslog or email alert. The syslog or email alert messages are sent by the statistics application at END time.

You can configure the device to display statistics on the console. The collected statistics are presented on the console at END time.

stats group

This command creates a new group with the specified id or name and configures the time range and the reporting mechanism for that group.

Format: `stats group group id|name timerange time range name reporting list of reporting methods`

Command mode: Global Config

Parameter	*Description*
group ID, name	Name of the group of statistics or its identifier to apply on the interface. The range is: • received • received-errors • transmitted • transmitted-errors • received-transmitted • port-utilization • congestion Default: none
time range name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. Default: none
list of reporting methods	Report the statistics to the configured method. Possible values are: • none • console • syslog • e-mail Default: there is no default value.

stats flow-based

This command configures flow based statistics rules for the given parameters over the specified time range. Only an IPv4 address is allowed as source and destination IP address.

Format: `stats flow-based` *`rule-id`* `timerange` *`time range name`* `[{srcip` *`ip-address`*`} {dstip` *`ip- address`*`} {srcmac` *`mac-address`*`} {dstmac` *`mac-address`*`} {srctcpport` *`portid`*`} {dsttcpport` *`portid`*`} {srcudpport` *`portid`*`} {dstudpport` *`portid`*`}]`

Command mode: Global Config

Parameter	*Description*
rule ID	The flow-based rule ID. Valid values: from 1 to 16. Default: none
time range name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. Default: there is no default value.
srcip ip-address	The source IP address.
dstip ip-address	The destination IP address.
srcmac mac- address	The source MAC address
dstmac mac- address	The destination MAC address

srctcpport portid	The source TCP port number.
dsttcpport portid	The destination TCP port number.
srcudpport portid	The source UDP port number.
dstudpport portid	The destination UDP port number.

no stats flow-based

This command deletes flow-based statistics.

Format: `stats flow-based` *`rule-id`*

Command mode: Global Config

stats flow-based reporting

This command configures the reporting mechanism for all the flow-based rules configured on the system. There is no per flow-based rule reporting mechanism. Setting the reporting method as ***none*** resets all the reporting methods.

Format: `stats flow-based reporting` *`list of reporting methods`*

Command mode: Global Config

stats group

This command applies the group specified on an interface or interface-range.

Format: `stats group <group id | name>`

Command mode: Interface Config

Parameter	*Description*
group id	Unique ID of the Group
name	The name of the group.

no stats group

This command deletes the interface or interface-range from the group specified.

Format: `no stats group <group id | name>`

Command mode: Interface Config

stats flow-based

This command applies the flow-based rule specified by the ID on an interface or interface-range.

Format: `stats flow-based <rule-id>`

Command mode: Interface Config

Parameter	*Description*
rule-id	The unique identifier for the stream based statistics collection rule.

no stats flow-based

This command deletes the interface or interface-range from the flow-based rule specified.

show stats group

This command displays the configured time range and the interface list for the group specified and shows collected statistics for the specified time-range name on the interface list after the time-range expiry.

Format: `show stats group <group id | name>`

Command mode: Privileged

Parameter	*Description*
group id	Unique ID of the Group
name	The name of the group.

show stats flow-based

This command displays the configured time range, flow-based rule parameters, and the interface list for the flow specified.

Format: `show stats flow-based` *`rule-id`*`|all`

Command mode: Privileged

Parameter	Description
rule-id	The unique identifier for the stream based statistics collection rule.

6.21 Configuration Backup commands

This section describes the commands used to set up a configuration backup by timer or while saving the current configuration to a flash drive.

backup url <url>

Using this command sets the protocol, server address, path on the server and the file prefix to record the configuration on the remote server.

Default: Disabled

Format `backup url <tftp://<ipaddr>/<filepath>/<filename>>`

Command Mode: Global Config Mode

no backup url <url>

Disable the configuration entry on the remote server.

Format `backup url <tftp://<ipaddr>/<filepath>/<filename>>`

Command Mode: Global Config Mode

backup time-period

With the help of this command a time interval is set, after which an automatic reservation of the configuration will be performed.

Default: 720 min

Format `backup time-period` *`period`*

Command Mode: Global Config Mode

backup auto

This command enables automatic configuration backup.

Default: Disabled

Format `backup auto`

Command Mode: Global Config Mode

backup write-memory

This command enables configuration backup when the user saves the configuration to a flash drive.

Default: Disabled

Format `backup write-memory`

Command Mode: Global Config Mode

7 STACKING MODE COMMANDS

This chapter describes the stacking commands available in the CLI.

The commands in this section can be divided into 2 functional groups:

- **Operational status commands (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.**

The Primary Management Unit is the unit that controls the stack.

7.1 Stacking

This section describes the commands you use to configure dedicated port stacking.

stack

This command sets the mode to Stack Global Config.

Format `stack`

Command Mode Global Config Mode

member

This command configures a switch. The `Unit` is the switch identifier of the switch to be added/removed from the stack. The `switchindex` is the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer. This command is executed on the Primary Management Unit.

Format `member` *`unit switchindex`*

Command Mode Stack Global Config Mode

Switch index can be obtained by executing the *show supported switchtype* command.

no member

This command removes a switch from the stack. The `Unit` is the switch identifier of the switch to be removed from the stack. This command is executed on the Primary Management Unit.

Format `no member` *`unit`*

Command Mode Global Config Mode

switch priority

This command configures the ability of a switch to become the Primary Management Unit. The `Unit` is the switch identifier. The *`Value`* is the preference parameter that allows the user to specify, priority of one backup switch over another. Range of values: 1-15. The switch with the highest priority value will be chosen to become the Primary Management Unit if the active Primary Management Unit fails. The switch priority defaults to the hardware management preference value 1. Switches that do not have the hardware capability to become the Primary Management Unit are not eligible for management.

After rebooting the switch stack, the master unit will be the switch with the highest priority value.

Default: 1

Format `switch` *`unit`* `priority` *`value`*

Command Mode Global Config Mode

switch renumber

This command changes the switch identifier for a switch in the stack. The `Oldunit` is the current switch identifier on the switch whose identifier is to be changed. The `Newunit` is the updated value of the switch identifier. Upon execution, the switch will be configured with the configuration information for the new switch, if any. The old switch configuration information will be retained, however the old switch will be operationally unplugged. This command is executed on the Primary Management Unit.

If the management unit is renumbered, then the running configuration is no longer applied (i.e. the stack acts as if the configuration had been cleared).

Format `switch` *`oldunit`* `renumber` *`newunit`*

Command Mode Global Config Mode

movemanagement

This command passes the Primary Management Unit functionality from one switch to another. The *`Fromunit`* is the switch identifier of the current Primary Management Unit. The *`Tounit`* is the switch identifier of the new Primary Management Unit. Upon command execution, the entire stack (including all interfaces in the stack) is reconfigured with the configuration of the new Primary Management Unit. After the reload is complete, all stack management must be performed through the new Primary Management Unit. To preserve the current configuration before a stack move (reconfiguration), execute the `copy system:running-config nvram:startup-config` (in Privileged Mode) command before performing the stack move (changing Primary Management Unit). A stack move causes loss of MAC table entries and layer 3 routes. This command is executed on the Primary Management Unit. The system will ask you to confirm the management move.

Format `movemanagement` *`fromunit tounit`*

Command Mode Stack Global Config Mode

standby

Use this command to configure a unit as a Standby Management Unit (STBY).

The Standby Management Unit cannot be the current Management Unit. The Standby unit should be a management-capable unit.

Format standby *unit number*

Command Mode Stack Global Config Mode

Parameter	*Description*
Standby Management Unit Number	Indicates the unit number which is to be the Standby Management Unit. **Unit number** must be a valid unit number.

no standby

The no form of this command allows the application to run the auto Standby Management Unit logic.

Format no standby

Command Mode Stack Global Config Mode

slot

This command configures a slot in the system. The *unit/slot* is the slot identifier of the slot. The *cardindex* is the index into the database of the supported card types, indicating the type of the card being preconfigured in the specified slot. The card index is a 32-bit integer. If a card is currently present in the slot that is unconfigured, the configured information will be deleted and the slot will be reconfigured with default information for the card.

Format slot *unit/slot cardindex*

Command Mode Global Config Mode

The card index can be obtained by issuing the *show supported cardtype* command.

no slot

This command removes configured information from an existing slot in the system.

Format no slot *unit/slot cardindex*

Command Mode Global Config Mode

The card index can be obtained by issuing the *show supported cardtype* command.

set slot disable

This command configures the administrative mode of the slot(s). If you specify [all], the command is applied to all slots, otherwise the command is applied to the slot identified by *unit/slot*.

If a card or other module is present in the slot, this administrative mode will effectively be applied to the contents of the slot. If the slot is empty, this administrative mode will be applied to any module that is inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as “unplugged” on management screens.

Format `set slot disable [unit/slot] | all]`

Command Mode Global Config Mode

no set slot disable

This command disables the administrative mode of the slot(s). If you specify all, the command removes the configuration from all slots, otherwise the configuration is removed from the slot identified by *unit/slot*.

If a card or other module is present in the slot, this administrative mode removes the configuration from the contents of the slot. If the slot is empty, this administrative mode removes the configuration from any module inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as “unplugged” on management screens.

Format `no set slot disable [unit/slot] | all]`

Command Mode Global Config Mode

set slot power

This command configures the power mode of the slot(s) and allows power to be supplied to a card located in the slot. If you specify `all`, the command is applied to all slots, otherwise the command is applied to the slot identified by *unit/slot*.

Use this command when installing or removing cards. If a card or other module is present in this slot, the power mode is applied to the contents of the slot. If the slot is empty, the power mode is applied to any card inserted into the slot.

Format `set slot power [unit/slot] | all]`

Command Mode Global Config Mode

no set slot power

This command disables the power mode of the slot(s) and prohibits power from being supplied to a card located in the slot. If you specify `all`, the command prohibits power to all slots, otherwise the command prohibits power to the slot identified by *unit/slot*.

Use this command when installing or removing cards. If a card or other module is present in this slot, power is prohibited to the contents of the slot. If the slot is empty, power is prohibited to any card inserted into the slot.

Format `no set slot power [unit/slot] | all]`

Command Mode Global Config Mode

reload (Stack)

This command resets the entire stack or the identified *unit*. The *Unit* is the switch identifier. The system prompts you to confirm that you want to reset the switch.

Format `reload [unit]`

Command Mode Privileged Mode

stack-status sample-mode

Use this command to configure global status management mode, sample size. The mode, sample size parameters are applied globally on all units in the stack. The default sampling mode of the operation is cumulative summing.

This configuration command is implemented as part of serviceability functionality and therefore is not expected to be persistent across reloads. This configuration is never visible in the runningconfiguration under any circumstances. It is the responsibility of the user to switch the sample mode on-demand as per the requirement. This configuration is applied to all the members that are part of the stack when the command is triggered. This configuration cannot play onto cards that are part of the stack at later point of the time.

Default: Cumulative Summing

Format `stack-status sample-mode {cumulative | history} [max-samples 100 - 500]`

Command Mode Stack Global Config Mode

Keywords	*Description*
sample-mode	Mode of sampling
cumulative	Tracks the sum of received time stamp offsets cumulatively.
history	Tracks history of received timestamps
max-samples	Maximum number of samples to keep

show slot

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

Format `show slot [unit/slot]`

Command Mode User mode

Privileged Mode

Parameter	*Description*
Slot	The slot identifier in a *unit/slot* format.
Slot Status	The slot is empty, full, or has encountered an error
Admin State	The slot administrative mode is enabled or disabled.
Power State	The slot power mode is enabled or disabled.
Configured Card	The model identifier of the card preconfigured in the slot. Model Identifier is a 32-character

Model Identifier	field used to identify a card.
Pluggable	Cards are pluggable or non-pluggable in the slot.
Power Down	Indicates whether the slot can be powered down.

If you supply a value for *unit/slot*, the following additional information appears:

Parameter	*Description*
Inserted Card Model Identifier	Model identifier of the card inserted in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full. This field is displayed only if the slot is full.
Inserted Card Description	The card description. This field is displayed only if the slot is full.
Configured Card Description	Half-Duplex 10BASE-T

show stack-status

Use this command to display the stack unit's received HB message timings, and the dropped/lost statistics for the specified unit.

Format `show stack stack-status [1-n | all] [clear]`

Command Mode Privileged Mode

Keywords	*Description*
Current	Current time of heartbeat message reception
Average	Average time of heartbeat messages received
Min	Minimum time of heartbeat messages received
Max	Maximum time of heartbeat messages received
Dropped	Heartbeat message dropped/lost counter

show supported cardtype

This commands displays information about all card types or specific card types supported in the system.

Format `show supported cardtype [cardindex]`

Command Mode User mode

Privileged Mode

If you do not supply a value for *cardindex*, the following output appears:

Parameter	*Description*
Card Index (CID)	The index into the database of the supported card types. This index is used when preconfiguring a slot.
Card Model Identifier	Model identifier for the supported card type.

If you supply a value for *cardindex*, the following output appears:

Parameter	Description
Card Type	The 32-bit numeric card type for the supported card.
Model Identifier	Model identifier for the supported card type.
Card Description	The description for the supported card type.

show switch

This command displays switch status information about all units in the stack or a single unit when you specify the unit value.

Format `show switch [unit]`

Command Mode Privileged Mode

Parameter	Description
Switch	The unit identifier assigned to the switch.

When you do not specify a value for *unit*, the following information appears:

Parameter	Description
Management Status	Indicates whether the switch is the Primary Management Unit, a stack member, a configured standby switch, an operational standby switch, or the status is unassigned.
Preconfigured Model Identifier	The model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Plugged-In Model Identifier	The model identifier of the switch in the stack. The Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Switch Status	Switch status. The switch status. Possible values for this state are: **OK, Unsupported, Code Mismatch, SDM Mismatch, Config Mismatch,** or **Not Present**. **Mismatch** indicates that on the stack unit the firmware version, SDM template, or configuration is different from the one on the main unit. The **SDM Mismatch** status indicates that the unit joined the stack, but is running a different SDM template than the management unit. This status is temporary; the stack unit should automatically reload using the template running on the stack manager. If there is a Stacking Firmware Synchronization operation in progress status is shown as **Updating Code**.
Code Version	The detected version of code on this switch.

When you specify a value for *unit*, the following information appears.

Parameter	Description
Management Status	Indicates whether the switch is the Primary Management Unit, a stack member, or the status is unassigned.
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.
Admin Management Preference	The administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the Primary Management Unit.
Switch Type	The 32-bit numeric switch type.
Model Identifier	The model identifier for this switch. Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.

Switch Status	Switch status. Possible values are: OK, Unsupported, Code Mismatch, SDM Mismatch, Config Mismatch, or Not Present.
Switch Description	The switch description.
Expected Code Type	The expected code type.
Expected Code Version	The expected code version.
Detected Code Version	The version of code running on this switch. If the switch is not present and the data is from preconfiguration, then the code version is “None”.
Detected Code in Flash	The version of code that is currently stored in FLASH memory on the switch. This code executes after the switch is reset. If the switch is not present and the data is from preconfiguration, then the code version is “None”.
SFS Last Attempt Status	The stack firmware synchronization status in the last attempt for the specified unit.
Serial Number	The serial number for the specified unit.
Up Time	The system up time.

show supported switchtype

This commands displays information about all supported switch types or a specific switch type.

Format `show supported switchtype` *`[switchindex]`*

Command Mode User mode

Privileged Mode

If you specify a value for *`switchindex`*, the following data appears:

Parameter	*Description*
Switch Index (SID)	The index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.
Model Identifier	The model identifier for the supported switch type.
Management Preference	The model identifier for the supported switch type.
Code Version	The management preference value of the switch type.

If you specify a value for *`switchindex`*, the following data appears:

Parameter	*Description*
Switch Type	The 32-bit numeric switch type for the supported switch.
Model Identifier	The model identifier for the supported switch type.
Switch Description	The description for the supported switch type.

7.2 Stack Port configuration commands

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

Stacking is performed at the maximum speed of the port. For MES7048 - 100G, for MES5448 - 40G

stack-port

This command sets stacking per port or range of ports to either *stack* or *ethernet* mode.

Default: stack

Format `stack-port` *unit/slot/port* `[{ethernet | stack}]`

Command Mode Stack Global Config Mode

show stack-port

This command displays summary stack-port information for all interfaces.

Format `show stack-port`

Command Mode Privileged Mode

For each Interface:

Parameter	*Description*
Unit	Unit number.
Interface	Slot and port numbers.
Configured Stack Mode	Stack or Ethernet.
Running Stack Mode	Stack or Ethernet.
Link Status	Status of the link.
Link Speed	Speed (Gbps) of the stack port link.

show stack-port counters

This command displays summary data counter information for all interfaces.

Format `show stack-port counters [`*1-n* `| all]`

Command Mode Privileged Mode

Parameter	*Description*
Unit	Unit number.
Interface	Slot and port numbers.
Tx Data Rate	Trashing data rate in megabits per second on the stacking port.
Tx Error Rate	Platform-specific number of transmit errors per second.
Tx Total Errors	Platform-specific number of total receive errors since power-up.

Rx Data Rate	Receive data rate in megabits per second on the stacking port.
Rx Error Rate	Platform-specific number of receive errors per second.
Rx Total Errors	Platform-specific number of total receive errors since power-up.
Link Flaps	The number of up/down events for the link since system boot up.

show stack-port diag

This command shows stack port diagnostics for each port and is only intended for Field Application Engineers (FAEs) and developers. An FAE will advise on the necessity to run this command and capture this information. In verbose mode, the statistics and counters for RPC, transport, CPU, and transport RX/TX modules are displayed.

Format `show stack-port diag [1-n | all] [verbose]`

Command Mode Privileged Mode

Parameter	*Description*
Unit	Unit number.
Interface	Slot and port numbers.
Diagnostic Entry1	A string of 80 characters used for diagnostics.
Diagnostic Entry2	A string of 80 characters used for diagnostics.
Diagnostic Entry3	A string of 80 characters used for diagnostics.
TBYT	Transmitted Bytes
TPKT	Transmitted Packets
TFCS	Transmit FCS Error Frame Counter
TERR	Transmit Error (set by system) Counter
RBYT	Received Bytes
RPKT	Received Packets
RFCS	Received FCS Error Frame Counter
RFRG	Received Fragment Counter
RJBR	Received Jabber Frame Counter
RUND	Received Undersize Frame Counter
ROVR	Received Oversized Frame Counter
RUNT	Received RUNT Frame Counter

show stack-port stack-path

This command displays the route a packet will take to reach the destination.

Format `show stack-port stack-path {1-8 | all}`

Command Mode Privileged Mode

7.3 Stack Firmware Synchronization commands

Stack Firmware Synchronization (SFS) provides the ability to automatically synchronize firmware for all stack members. If a unit joins the stack and its firmware version is different from the version running on the stack manager, the SFS feature can either upgrade or downgrade the firmware on the mismatched stack member. There is no attempt to synchronize the stack to the latest firmware in the stack.

boot auto-copy-sw

Use this command to enable the Stack Firmware Synchronization feature on the stack.

Default: Disabled

Format `boot auto-copy-sw`

Command Mode: Privileged Mode

no boot auto-copy-sw

Use this command to disable the Stack Firmware Synchronization feature on the stack

Format `no boot auto-copy-sw`

Command Mode Privileged Mode

boot auto-copy-sw trap

Use this command to enable the sending of SNMP traps related to the Stack Firmware Synchronization feature.

Default: Enabled

Format `boot auto-copy-sw trap`

Command Mode Privileged Mode

no boot auto-copy-sw trap

Use this command to disable the sending of traps related to the Stack Firmware Synchronization feature.

Format `no boot auto-copy-sw trap`

Command Mode Privileged Mode

boot auto-copy-sw allow-downgrade

Use this command to allow the stack manager to downgrade the firmware version on the stack member if the firmware version on the manager is older than the firmware version on the member.

Default: Enabled

Format `boot auto-copy-sw allow-downgrade`

Command Mode Privileged Mode

no boot auto-copy-sw allow-downgrade

Use this command to prevent the stack manager from downgrading the firmware version of a stack member.

Format `no boot auto-copy-sw allow-downgrade`

Command Mode Privileged Mode

show auto-copy-sw

Use this command to display Stack Firmware Synchronization configuration status information.

Format `show auto-copy-sw`

Command Mode Privileged Mode

Parameter	*Description*
Synchronization	Shows whether the SFS feature is enabled.
SNMP Trap Status	Shows whether the stack will send traps for SFS events.
Allow Downgrade	Shows wether the manager is permitted to downgrade the firmware version of a stack member.

Nonstop Forwarding commands (NSF)

A switch can be described in terms of three semi-independent functions called the forwarding plane, the control plane, and the management plane. The forwarding plane forwards data packets. The forwarding plane is implemented in hardware. The control plane is the set of protocols that determine how the forwarding plane should forward packets, deciding which data packets are allowed to be forwarded and where they should go. Application software on the management unit acts as the control plane. The management plane is application software running on the management unit that provides interfaces allowing a network administrator to configure and monitor the device.

Nonstop forwarding (NSF) allows the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the management unit. A nonstop forwarding failover can also be manually initiated using the *initiate failover* command. Traffic flows that enter and exit the stack through physical ports on a unit other than the management continue with at most subsecond interruption when the management unit fails.

To prepare the backup management unit in case of a failover, applications on the management unit continuously checkpoint some state information to the backup unit. Changes to the running configuration are automatically copied to the backup unit. MAC addresses stay the same across a nonstop forwarding failover so that neighbors do not have to relearn them.

When a nonstop forwarding failover occurs, the control plane on the backup unit starts from a partially-initialized state and applies the checkpointed state information. While the control plane is initializing, the stack cannot react to external changes, such as network topology changes. Once the control plane is fully operational on the new management unit, the control plane ensures that the hardware state is updated as necessary. Control plane failover time depends on the size of the stack, the complexity of the configuration, and the speed of the CPU.

The management plane restarts when a failover occurs. Management connections must be reestablished.

For NSF to be effective, adjacent networking devices must not reroute traffic around the restarting device. Firmware uses three techniques to prevent traffic from being rerouted:

1. A protocol may distribute a part of its control plane to stack units so that the protocol can give the appearance that it is still functional during the restart. Spanning tree and port channels use this technique.
2. A protocol may enlist the cooperation of tis neighbors through a technique known as graceful restart. OSPF uses graceful restart if it is enabled.
3. A protocol may simply restart after the failover if neighbors react slowly enough that they will not normally detect the outage. The IP multicast routing protocols are a good example of this behavior.

To take full advantage of nonstop forwarding, layer 2 connections to neighbors should be via port channels that span two or more stack units, and layer 3 routes should be ECMP routes with next hops via physical ports on two or more units. The hardware can quickly move traffic flows from port channel members or ECMP paths on a failed unit to a surviving unit.

nsf (Stack Global Config Mode)

This command enables nonstop forwarding feature on the stack. When nonstop forwarding is enabled, if the management unit of a stack fails, the backup unit takes over as the master without clearing the hardware tables of any of the surviving units. Data traffic continues to be forwarded in hardware while the management functions initialize on the backup unit.

NSF is enabled by default on platforms that support it. The administrator may wish to disable NSF in order to redirect the CPU resources consumed by data checkpointing.

If a unit that does not support NSF is connected to the stack, then NSF is disabled on all stack members. When a unit that does not support NSF is disconnected from the stack and all other units support NSF, and NSF is administratively enabled, then NSF operation resumes.

Default: Enabled

Format `nsf`

Command Mode Stack Global Config Mode

no nsf

This command disables NSF on the stack.

Format `no nsf`

Command Mode Stack Global Config Mode

show nsf

This command displays global and per-unit information on NSF configuration on the stack.

Format `show nsf`

Command Mode Privileged Mode

Parameter	*Description*
NSF Administrative Status	Whether nonstop forwarding is administratively enabled or disabled. Default: enable
NSF Operational Status	Indicates whether NSF is enabled on the stack.
Last Startup Reason	The type of activation that caused the software to start the last time: • "Power-On" means that the switch rebooted. This could have been caused by a power cycle or an administrative "Reload" command. • "Administrative Move" means that the administrator issued the movemanagement command for the stand-by manager to take over. • "Warm-Auto-Restart" means that the primary management card restarted due to a failure, and the system executed a nonstop forwarding failover. • "Cold-Auto-Restart" means that the system switched from the active manager to the backup manager and was unable to maintain user data traffic. This is usually caused by multiple failures occurring close together.
Time Since Last Restart	Time since the current management unit became the active management unit.
Restart in progress	Whether a restart is in progress.
Warm Restart Ready	Whether the system is ready to perform a nonstop forwarding failover from the management unit to the backup unit.
Copy of Running Configuration to Backup Unit: Status	Whether the running configuration on the backup unit includes all changes made on the management unit. Displays as Current or Stale.
Time Since Last Copy	When the running configuration was last copied from the management unit to the backup unit.
Time Until Next Copy	The number of seconds until the running configuration will be copied to the backup unit. This line only appears when the running configuration on the backup unit is Stale.
Per Unit Status Parameters	
NSF Support	Whether a unit supports NSF.

initiate failover

This command forces the backup unit to take over as the management unit and perform a "warm restart" of the stack. On a warm restart, the backup unit becomes the management unit without clearing its hardware tables (on a cold restart, hardware tables are cleared). Applications apply checkpointed data from the former management unit. The original management unit reboots.

If the system is not ready for a warm restart, for example because no backup unit has been elected or one or more members of the stack do not support nonstop forwarding, the command fails with a warning message.

The movemanagement command also transfers control from the current management unit; however, the hardware is cleared and all units reinitialize.

Format `initiate failover`

Command Mode Stack Global Config Mode

show checkpoint statistics

This command displays general information about the checkpoint service operation.

Format `show checkpoint statistics`

Command Mode Privileged Mode

Parameter	*Description*
Messages Checkpointed	Number of checkpoint messages transmitted to the backup unit. Range of values: integer. Default: zero (0).
Bytes Checkpointed	Number of bytes transmitted to the backup unit. Range of values: integer. Default: zero (0).
Time Since Counters Cleared	Number of days, hours, minutes and seconds since the counters were reset to zero. The counters are cleared when a unit becomes manager and with a support command. Default: 0d00:00:00
Checkpoint Message Rate	Average number of checkpoint messages per second. The average is computed over the time period since the counters were cleared. Range of values: integer. Default: zero (0).
Last 10-second Message Rate	Average rate recorded over a 10-second interval since the counters were cleared. Range of values: integer. Default: zero (0).
Highest 10-second Message Rate	The highest rate recorded over a 10-second interval since the counters were cleared. Range of values: integer. Default: zero (0).

clear checkpoint statistics

This command clears all checkpoint statistics to their initial values.

Format `clear checkpoint statistics`

Command Mode Privileged Mode

7.4 Mixed Stacking commands

Mixed stacking allows heterogeneous stacks to form by enforcing a homogeneous set of capacities and capabilities through the use of templates. Each template defines operational characteristics for a stacking unit. These characteristics include the capacities of the various tables in the silicon (for example, L2 table size) as well as an implicit set of capabilities based on the underlying silicon for the given template. There is one template for each chip type supported by Mixed Stacking. There are additional templates that provide a *least common denominator* set of capacities and capabilities which allow different chip types to be stacked together.

When more capable devices are stacked with less capable devices, the templates ensure that the stack as a whole operates to the capabilities of the least capable device in the stack. In some cases, one device in a stack may have a larger table size than another device in the stack, but it may not have as many features as the device with the smaller table size. The templates ensure that the stack as a whole operates in a *least common denominator* mode under this condition.

stack-template

This command sets the stack template ID on a single unit (if specified) or on the entire stack. The user is prompted to confirm that the startup configuration will be deleted on the affected units and that the unit(s) being modified will be rebooted.

Default: Set by platform

Format `stack-template templateId [unit]`

Command Mode Stack mode

no stack-template

This command restores the stack template ID on a single unit to the default value for that platform. The user is prompted to confirm that the startup configuration will be deleted on the affected unit and that the unit being modified will be rebooted.

Default: Set by platform

Format `no stack-template unit`

Command Mode Stack mode

show stack-template list

This command shows a list of template IDs. This command has an optional *switchindex* parameter that correlates to the supported switch models. If the switch index is provided, then this command shows the templates that can be configured on that switch type. Note that not all templates can be configured on all switch types.

Format `show stack-template list`

Command Mode Privileged Mode

show stack-template switch

This command shows the template IDs that are configured on each switch in the stack. Preconfigured units or units that have a code mismatch show the template ID as *unknown*.

Format `show stack-template switch`

Command Mode Priveleged EXEC

8 MANAGEMENT COMMANDS

This chapter describes the management commands available in the CLI.

There is no default IP address on the MES5448 and MES7048 switches. DHCP Client on the service OOB port is enabled by default.

All commands listed in this section are divided into three functional groups:

- **Show commands display switch configuration information, statistics, and other information.**
- **Configuration commands configure switch features. 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.**

8.1 Remote control interface configuration commands

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

enable (access to privileged mode)

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

Format enable

Command Mode User mode

do (Privileged commands)

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

Format do *Priv Exec Mode Command*

Command Mode Global Config Mode
Interface Config
VLAN configuration mode
Routing configuration mode

serviceport ip

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

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

Command Mode Privileged Mode

serviceport protocol

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

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

Command Mode Privileged Mode

serviceport protocol dhcp

This command enables the DHCPv4 client on a Service port. If the *client-id* optional parameter is given, the DHCP client messages are sent with the client identifier option.

Default: none

Format `serviceport protocol dhcp [client-id]`

Command Mode Privileged Mode

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.

network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet. When you specify the `none` option, the IP address and subnet mask are set to the factory defaults.

Format `network parms {ipaddr netmask [gateway]| none}`

Command Mode Privileged Mode

network protocol

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

Default: none

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

Command Mode Privileged Mode

network protocol dhcp

This command enables the DHCPv4client on a Network port. If the `client-id` optional parameter is given, the DHCPclient messages are sent with the client identifier option.

Default: none

Format `network protocol dhcp [client-id]`

Command Mode Global Config Mode

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

network mac-address

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

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

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

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

Command Mode Privileged Mode

network mac-type

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

Default: burnedin

Format `network mac-type {local | burnedin}`

Command Mode Privileged Mode

no network mac-type

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

Format `no network mac-type`

Command Mode Privileged Mode

network javamode

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the Web interface. When access is enabled, the Java applet can be viewed from the Web interface. When access is denied, the user cannot view the Java applet.

Default: Enabled

Format `network javamode`

Command Mode Privileged Mode

no network javamode

This command disallows access to the Java applet in the header frame of the Web interface. When access is denied, the user cannot view the Java applet.

Format no network javamode

Command Mode Privileged Mode

show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The network interface is always considered to be up, whether or not any member ports are up. Therefore, the *show network* command will always show **Interface Status** as **Up**.

Format show network
Command Mode Privileged Mode
User mode

Parameter	*Definition*
Interface Status	The network interface status.
IP Address	IP address of the interface. The value specified by the factory configuration: 0.0.0.0.
Subnet Mask	Interface subnet IP mask. The value specified by the factory configuration: 0.0.0.0.
Default Gateway	Default gateway for interface of specified IP. Default: 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/Length	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
Burned in MAC Address	Factory default MAC address
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique Bridge Identifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Configured IPv4 Protocol	The IPv4 network protocol used. Possible values are: bootp | dhcp | none (not in use).
Configured IPv6 Protocol	The IPv6 network protocol used. Possible values are: dhcp | none (not in use).
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the **client-id** option on the network port. See network protocol dhcp.

show serviceport

This command displays service port configuration information.

Format `show serviceport`

Command Mode Privileged Mode

User mode

Parameter	*Definition*
Interface Status	The network interface status. It is always considered to be up.
IP Address	IP address of the interface. The value specified by the factory configuration: 0.0.0.0.
Subnet Mask	Interface subnet IP mask. The value specified by the factory configuration: 0.0.0.0.
Default Gateway	Default gateway for interface of specified IP. The value specified by the factory configuration: 0.0.0.0.
IPv6 Administrative Mode	Enable or disable. Default: Enabled
IPv6 Address/Length	The IPv6 address and length. Default: Local network (Link Local).
IPv6 Default Router	TheIPv6 default router address on the service port. Default: Unspecified address.
Configured IPv4 Protocol	The IPv4 network protocol used. Possible values are: bootp | dhcp | none (not in use).
Configured IPv6 Protocol	The IPv6 network protocol used. Possible values are: dhcp | none (not in use).
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
Burned in MAC Address	Factory default MAC address.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the service port.

8.2 Console Port access commands

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

configure

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

Format `configure`

Command Mode Privileged Mode

line

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

Format `line {console | telnet | ssh}`

Command Mode Global Config Mode

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

serial baudrate

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

Default: 115200

Format `serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`

Command Mode Line Config

no serial baudrate

This command sets the communication rate of the terminal interface.

Format `no serial baudrate`

Command Mode Line Config

serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value 0 corresponds to infinite time. The time range is 0-160.

Default: 5

Format `serial timeout` *`0-160`*

Command Mode Line Config

no serial timeout

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

Format `no serial timeout`

Command Mode Line Config

show serial

This command displays serial communication settings for the switch.

Format `show serial`

Command Mode Privileged Mode

User mode

Parameter	*Definition*
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. A value 0 corresponds to infinite time.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity	The parity method used on the Serial Port. Always None («Not in use»).

8.3 Telnet configuration commands

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

ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default: Disabled

Format `ip telnet server enable`

Command Mode Privileged Mode

no ip telnet server enable

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

Format `no ip telnet server enable`

Command Mode Privileged Mode

ip telnet port

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

Default: 23

Format `ip telnet port` *`1-65535`*

Command Mode Privileged Mode

no ip telnet port

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

Format `no ip telnet port`

Command Mode Privileged Mode

telnet

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

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

Command Mode Privileged Mode

User mode

transport input telnet

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

If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the `ip telnet server enable` command to enable Telnet Server Admin Mode.

Default: Enabled

Format `transport input telnet`

Data entry mode Line Config

no transport input telnet

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

Format `no transport input telnet`

Data entry mode Line Config

transport output telnet

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

Default: Enabled

Format `transport output telnet`

Command Mode Line Config

no transport output telnet

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

Format `no transport output telnet`

Command Mode Line Config

session-limit

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

Default: 5

Format `session-limit` *`0-5`*

Data entry mode Line Config

no session-limit

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

Format `no session-limit`

Command Mode Line Config

session-timeout

This command sets the Telnet session timeout valueю The value is set in minutes.

Default: 5

Format `session-timeout` *`1-160`*

Data entry mode Line Config

no session-timeout

Reset the Telnet session time out to its default value. The value is set in minutes.

Format `no session-timeout`

Command Mode Line Config

telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. Range of values: 0-5.

Default: 5

Format `telnetcon maxsessions` *`0-5`*

Command Mode Privileged Mode

no telnetcon maxsessions

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

Format `no telnetcon maxsessions`

Command Mode Privileged Mode

telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. Range of values: decimal number from 1 to 160.

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

Default: 5

Format `telnetcon timeout` *`1-160`*

Data entry mode Privileged Mode

no telnetcon timeout

Reset the Telnet session time out to its default value.

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

Format `no telnetcon timeout`

Data entry mode Privileged Mode

show telnet

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

Format `show telnet`

Command Mode Privileged Mode

User mode

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

show telnetcon

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

Format `show telnetcon`

Command Mode Privileged Mode

User mode

Parameter	*Definition*
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. Value: decimal number from 1 to 160. Default: 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. Default: 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. Default: Yes.
Telnet Server Admin Mode	If Telnet Admin mode is enabled or disabled.
Telnet Server Port	The configured TCP port number on which the Telnet server listens for requests. (The default is 23)

8.4 SSH configuration commands

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

The system allows a maximum of 5 SSH sessions.

ip ssh

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

Default: Disabled

Format `ip ssh`

Command Mode Privileged Mode

ip ssh port

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

Default: 22

Format `ip ssh port` *`1-65535`*

Command Mode Privileged Mode

no ip ssh port

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

Format `no ip ssh port`

Command Mode Privileged Mode

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Possible values are: SSH1 (1), SSH2 (2) or both SSH 1 and SSH 2 (1 and 2).

Default: 2

Format `ip ssh protocol [1] [2]`

Command Mode Privileged Mode

ip ssh server enable

This command enables the IP secure shell server.

Default: Disabled

Format `ip ssh server enable`

Command Mode Privileged Mode

no ip ssh server enable

This command disables the IP secure shell server.

Format `no ip ssh server enable`

Command Mode Privileged Mode

sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. Range of values: 0-5.

Default: 5

Format `sshcon maxsessions` *`0-5`*

Command Mode: Privileged Mode

no sshcon maxsessions

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

Format `no sshcon maxsessions`

Command Mode Privileged Mode

sshcon timeout

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

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

Default: 5

Format `sshcon timeout` *`1-160`*

Command Mode Privileged Mode

no sshcon timeout

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

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

Format `no sshcon timeout`

Command Mode Privileged Mode

show ip ssh

This command displays the SSH settings.

Format `show ip ssh`

Command Mode Privileged Mode

Parameter	*Definition*
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
SSH Port	The SSH port.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

8.5 Security Keys management commands

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

crypto certificate generate

Use this command to generate a self-signed certificate for HTTPS. The generated RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format `crypto certificate generate`

Command Mode Global Config Mode

no crypto certificate generate

Use this command to delete the HTTPS certificate files from the device, regardless of whether they are self- signed or downloaded from an outside source.

Format `no crypto certificate generate`

Command Mode Global Config Mode

crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format `crypto key generate rsa`

Command Mode Global Config Mode

no crypto key generate rsa

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

Format `no crypto key generate rsa`

Command Mode Global Config Mode

crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format `crypto key generate dsa`

Command Mode Global Config Mode

no crypto key generate dsa

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

Format `no crypto key generate dsa`

Command Mode Global Config Mode

8.6 HTTP/HTTPS configuration commands

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

ip http accounting exec, ip https accounting exec

This command applies user exec (start-stop/stop-only) accounting list to the line methods HTTP and HTTPS.

The user exec accounting list should be created using the command `aaa accounting`

Format `ip {http|https} accounting exec {default|`*`listname`*`}`

Command Mode Global Config Mode

Parameter	*Definition*
http/https	The line method for which the list needs to be applied.
default	The default list of methods for authorization services.
listname	An alphanumeric character string used to name the list of accounting methods.

no ip http/https accounting exec

This command deletes the accounting method list.

Format `no ip {http|https} accounting exec {default|`*`listname`*`}`

Command Mode Global Config Mode

ip http authentication

Use this command to specify authentication methods for http server users. The default configuration is the local user database is checked. This action has the same effect as the command ip http authentication local. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. For example, if none is specified as an authentication method after radius, no authentication is used if the RADIUS server is down.

Default: `Local`

Format `ip http authentication method1 [method2...]`

Command Mode Global Config Mode

Parameter	*Description*
local	Use a local username database for authentication.
none	Do not use authentication
radius	Use for authentication a list of all RADIUS servers
tacacs	Use for authentication a list of all TACACS+ servers.

no ip http authentication

Restore the default value.

Format `no ip http authentication`

Command Mode Global Config Mode

ip https authentication

Use this command to specify authentication methods for https server users. The default configuration is the local user database is checked. This action has the same effect as the command ip https authentication local. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. For example, if none is specified as an authentication method after radius, no authentication is used if the RADIUS server is down.

Default: `local`

Format `ip https authentication method1 [method2...]`

Command Mode Global Config Mode

Parameter	*Description*
local	Use a local username database for authentication.
none	Do not use authentication
radius	Use for authentication a list of all RADIUS servers
tacacs	Use for authentication a list of all TACACS+ servers.

no ip https authentication

Restore the default value.

Format `no ip https authentication`

Command Mode Global Config Mode

ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Default: Enabled

Format `ip http server`

Command Mode Privileged Mode

no ip http server

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

Format `no ip http server`

Command Mode Privileged Mode

ip http secure-server

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

Default: Disabled

Format `ip http secure-server`

Command Mode Privileged Mode

no ip http secure-server

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

Format `no ip http secure-server`

Command Mode Privileged Mode

ip http java

This command enables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Default: Enabled

Format `ip http java`

Command Mode Privileged Mode

no ip http java

This command disables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Format `no ip http java`

Command Mode Privileged Mode

ip http port

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

Default: 80

Format `ip http port` *`1-65535`*

Command Mode Privileged Mode

no ip http port

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

Format `no ip http port`

Command Mode Privileged Mode

ip http rest-api port

This command configures the HTTP TCP port number on which the OpEN restful API server listens for restful requests.

Default: 8080

Format `ip http rest-api port` *`1025-65535`*

Command Mode Privileged Mode

no ip http rest-api port

This command restores the open restful API HTTP server listen port to its factory default value.

Format `no ip http rest-api port`

Command Mode Privileged Mode

ip http rest-api secure-port

This command configures the HTTPS TCP port number on which the open restful API server listens for secure restful requests

Default: 8443

Format `ip http rest-api secure-port` *`1025-65535`*

Command Mode Privileged Mode

no ip http rest-api secure-port

This command restores the OpEN restful API HTTP server listen port to its factory default value.

Format `no ip http rest-api secure-port`

Command Mode Privileged Mode

ip http session hard-timeout

This command configures the hard timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite timeout. When this timeout expires, the user will be forced to reauthenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default: 24

Format `ip http session hard-timeout` *`1-168`*

Command Mode Privileged Mode

no ip http session hard-timeout

This command restores the hard timeout for un-secure HTTP sessions to the default value.

Format `no ip http session hard-timeout`

Command Mode Privileged Mode

ip http session maxsessions

This command limits the number of allowable un-secure HTTP sessions. Minimal value: 0 (null).

Default: 16

Format `ip http session maxsessions` *`0-16`*

Command Mode Privileged Mode

no ip http session maxsessions

This command restores the number of allowable un-secure HTTP sessions to the default value.

Format `no ip http session maxsessions`

Command Mode Privileged Mode

ip http session soft-timeout

This command configures the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite timeout. When this timeout expires, the user will be forced to reauthenticate. The countdown is from the beginning of the session and is restarted with each new connection.

Default: 5

Format `ip http session soft-timeout` *`1-60`*

Command Mode Privileged Mode

no ip http session soft-timeout

This command resets the soft timeout for un-secure HTTP sessions to the default value.

Format `no ip http session soft-timeout`

Command Mode Privileged Mode

ip http secure-session hard-timeout

This command configures the hard timeout for secure HTTP sessions in hours. When this timeout expires, the user will be forced to reauthenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection. This parameter cannot be equal to zero (infinity).

Default: 24

Format `ip http secure-session hard-timeout` *`1-168`*

Command Mode Privileged Mode

no ip http secure-session hard-timeout

This command resets the hard timeout for secure HTTP sessions to the default value.

Format `no ip http secure-session hard-timeout`

Command Mode Privileged Mode

ip http secure-session maxsessions

This command limits the number of secure HTTP sessions. Minimal value: 0 (null).

Default: 16

Format `ip http secure-session maxsessions` *`0-16`*

Command Mode Privileged Mode

no ip http secure-session maxsessions

This command restores the number of allowable secure HTTP sessions to the default value.

Format `no ip http secure-session maxsessions`

Command Mode Privileged Mode

ip http secure-session soft-timeout

This command configures the soft timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, the user will be forced to reauthenticate. The countdown is from the beginning of the session and is restarted with each new connection. This parameter cannot be equal to zero (infinity).

Default: 5

Format `ip http secure-session soft-timeout` *`1-60`*

Command Mode Privileged Mode

no ip http secure-session soft-timeout

This command restores the soft timeout for secure HTTP sessions to the default value.

Format `no ip http secure-session soft-timeout`

Command Mode Privileged Mode

ip http secure-port

This command is used to set the SSL port where port can be 1025-65535 and the default is port 443.

Default: 443

Format `ip http secure-port` *`portid`*

Command Mode Privileged Mode

no ip http secure-port

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

Format `no ip http secure-port`

Command Mode Privileged Mode

ip http secure-protocol

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

Default: SSL3 and TLS1

Format `ip http secure-protocol` *`[SSL3] [TLS1]`*

Command Mode Privileged Mode

show ip http

This command displays the http settings for the switch.

Format `show ip http`

Command Mode Privileged Mode

Parameter	*Definition*
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
HTTP Port	The configured TCP port on which the HTTP server listens for requests. (The default is 80.)
RESTful API HTTP Port	The HTTPS TCP port number on which the OpEN RESTful API server listens for RESTful requests.
RESTful API HTTPS Port	The HTTPS TCP port number on which the OpEN RESTful API server listens for secure RESTful requests.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.
HTTP Session Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http sessions in minutes.
Certificate Present	Indicates whether the secure-server certificate files are present on the device.
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

8.7 Access commands

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

disconnect

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

Format `disconnect {session_id | all}`

Command Mode Privileged Mode

linuxsh

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

Access to linuxsh is available with a specially generated debug key. If you need a key, contact technical support.

Default: ip-port:2324

Format `linuxsh [ip-port]`

Command Mode Privileged Mode

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

show loginsession

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

Format `show loginsession`

Command Mode Privileged Mode

Parameter	*Description*
ID	Login Session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.
Session Time	Total time this session has been connected.
Session Type	Shows the type of session, which can be HTTP, HTTPS, telnet, serial, or SSH.

show loginsession long

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

Format `show loginsession long`

Command Mode Privileged Mode

8.8 User Account commands

This section describes the commands you use to add, manage, and delete system users. Software has one default user — Admin. The admin user can view and configure system settings.

You cannot delete the admin user. You can configure up to five local users on the system.

aaa authentication login

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

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

Default: `defaultList`. Used by the console and only contains the method none.
`networkList`. Used by telnet and SSH and only contains the method `local`.

Format `aaa authentication login {default | list-name} method1 [method2...]`

Command Mode Global Config Mode

Parameter	*Description*
default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string of up to 15 characters used to name the list of authentication methods activated when a user logs in.
method1... ***[method2...]***	At least one from the following: • *deny*. Used to deny access. • *enable*. Uses the enable password for authentication. • *line*. Uses the line password for authentication. • *none*. Uses no authentication. • *radius*. Uses the list of all RADIUS servers for authentication. • *tacacs*. Uses the list of all TACACS servers for authentication.

no aaa authentication login

This command returns to the default.

Format `aaa authentication login {default | list-name}`

Command Mode Global Config Mode

aaa authentication enable

Use this command to set authentication for accessing higher privilege levels. The default enable list is enableList. It is used by console, and contains the method as enable followed by none.

A separate default enable list, enableNetList, is used for Telnet and SSH users instead of enableList. This list is applied by default for Telnet and SSH, and contains enable followed by deny methods. In software, by default, the enable password is not configured. That means that, by default, Telnet and SSH users will not get access to Privileged EXEC mode. On the other hand, with default conditions, a console user always enter the Privileged mode without entering the enable password.

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

The user manager returns ERROR (not PASS or FAIL) for enable and line methods if no password is configured, and moves to the next configured method in the authentication list. The method none reflects that there is no authentication needed.

The user will only be prompted for an enable password if one is required. The following authentication methods do not require passwords:

- none (not specified)
- deny (denied)
- enable (if no enable password is configured)
- line (if no line password is configured)

Examples a and b do not prompt for a password, however because examples c and d contain the radius and tacacs methods, the password prompt is displayed.

If the login methods include only enable, and there is no enable password configured, then system does not prompt for a username. In such cases, software only prompts for a password. Software supports configuring methods after the local method in authentication and authorization lists. If the user is not present in the local database, then the next configured method is tried.

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

Use the `show authorization methods` command to display information about the authentication methods.

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

Default: Default:

Format `aaa authentication enable {default | list-name} method1 [method2...]`

Command Mode Global Config Mode

Parameter	*Description*
default	Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
list-name	Character string used to name the list of authentication methods activated, when using access higher privilege levels. Range: 1-15 characters.
Method1 *[***method2...***]***	Specify at least one from the following: • *deny*. Used to deny access. • *enable*. Uses the enable password for authentication. • *line*. Uses the line password for authentication. • *none*. Uses no authentication. • *radius*. Uses the list of all RADIUS servers for authentication. • *tacacs*. Uses the list of all TACACS servers for authentication.

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

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

no aaa authentication enable

Use this command to return to the default configuration.

Format `no aaa authentication enable {default | list-name}`

Command Mode Global Config Mode

aaa authorization

Use this command to configure command and exec authorization method lists. This list is identified by default or a user-specified list-name. A maximum of five authorization method lists can be created.

Local method is not supported for command authorization.

Per-Command Authorization

When authorization is configured for a line mode, the user manager sends information about an entered command to the AAA server. The AAA server validates the received command, and responds with either a PASS or FAIL response. If approved, the command is executed. Otherwise, the command is denied and an error message is shown to the user. The various utility commands like tftp, and ping, and outbound telnet should also pass command authorization. Applying the script is treated as a single command apply script, which also goes through authorization. Startup-config commands applied on device boot-up are not an object of the authorization process.

The per-command authorization usage scenario is this:

1 Configure Authorization Method List

```
aaa authorization commands listname tacacs radius none
```

2 Apply AML to an Access Line Mode (console, telnet, SSH)

```
authorization commands listname
```

3 Commands entered by the user will go through command authorization via TACACS+ or RADIUS server and will be accepted or denied.

Exec Authorization

When exec authorization is configured for a line mode, the user may not be required to use the enable command to enter Privileged mode. If the authorization response indicates that the user has sufficient privilege levels for Privileged mode, then the user bypasses User mode entirely.

The exec authorization usage scenario is this:

1 Configure Authorization Method List

```
aaa authorization exec listname method1 [method2....]
```

2 Apply AML to an Access Line Mode (console, telnet, SSH)

```
authorization exec listname
```

3 When the user logs in, in addition to authentication, authorization will be performed to determine if the user is allowed direct access to Privileged mode.

Format `aaa authorization {commands|exec} {default|list-name} method1[method2]`

Command Mode Global Config Mode

Parameter	*Description*
commands	Provides authorization for all user-executed commands.
exec	Provides exec authorization.
default	The default list of methods for authorization services.
list-name	Alphanumeric character string used to name the list of authorization methods.
method	Valid values: TACACS+/RADIUS/Local and none

no aaa authorization

This command deletes the authorization method list.

Format `no aaa authorization {commands|exec} {default|list-name}`

Command Mode Global Config Mode

authorization commands

This command applies a command authorization method list to an access method. For usage scenarios on per command authorization, see the aaa authorization command.

Format `authorization commands [default|list-name]`

Command Mode Line console, Line telnet, Line SSH

Parameter	*Description*
commands	This causes command authorization for each command execution attempt.

no authorization commands

This command removes command authorization from a line config mode.

Format `no authorization {commands|exec}`

Command Mode Line console, Line telnet, Line SSH

authorization exec

This command applies a command authorization method list to an access method so that the user may not be required to use the enable command to enter Privileged mode. The procedure for configuring authorization, see aaa authorization.

Format `authorization exec list-name`

Command Mode Line console, Line telnet, Line SSH

Parameter	*Description*
list-name	The command authorization method list.

no authorization exec

This command removes command authorization from a line config mode.

Format `no authorization exec`

Command Mode Line console, Line telnet, Line SSH

authorization exec default

This command applies a default command authorization method list to an access method so that the user may not be required to use the enable command to enter Privileged mode. The procedure for configuring authorization, see aaa authorization.

Format `authorization exec default`

Command Mode Line console, Line telnet, Line SSH

no authorization exec default

This command removes command authorization from a line config mode.

Format `no authorization exec default`

Command Mode Line console, Line telnet, Line SSH

show authorization methods

This command displays the configured authorization method lists.

Format `show authorization methods`

Command Mode Privileged Mode

enable authentication

Use this command to specify the authentication method list when accessing a higher privilege level from a remote telnet or console.

Format `enable authentication {default | list-name}`

Command Mode Line Config

Parameter	*Description*
default	Uses the default list created with the `aaa authentication` command.
list-name	Uses the indicated list created with the `aaa authentication enable` command.

no enable authentication

Use this command to return to the default specified by the `enable authentication` command.

Format `no enable authentication`

Command Mode Line Config

username (global configuration mode)

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

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

Command Mode Global Config Mode

Parameter	*Description*
name	Username. Length: 1-64 characters
password	The authentication password for the user. Range 8-64 characters. This value can be zero if the no passwords min-length command has been executed. The special characters allowed in the password include ! # $ % & ' ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Values: 0, 1, 15. Enter access level 1 for non-privileged (switch> prompt) or 15 for highest privilege (switch# prompt) Access. If not specified where it is optional, the privilege level is 1.

encrypted	Encrypted password entered, copied from another switch configuration.
override-complexity-check	Disables the validation of the password strength.

no username

Use this command to remove a user name.

Format `no username` *name*

Command Mode Global Config Mode

username nopassword

Use this command to remove an existing user's password (NULL password).

Format `username` *name* `nopassword` *[level level]*

Command Mode Global Config Mode

Parameter	*Description*
name	Username. Length: 1-32 characters
password	The authentication password for the user. The range is 8-64 characters
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Values: 0, 1, 15.

username unlock

Use this command to allows a locked user account to be unlocked. Only a user with Level 1 access can reactivate a locked user account.

Format `username` *name* `unlock`

Command Mode Global Config Mode

username snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid access mode values are `readonly` or `readwrite`. The *username* is the login user name for which the specified access mode applies. The default is readwrite for the "`admin`" user and `readonly` for all other users. You must enter the *username* in the same case you used when you added the user. To see the case of the *username*, enter the `show users` command.

Default: Admin - readwrite

Other - readonly

Format `username snmpv3 accessmode` *username* {*readonly* | *readwrite*}

Command Mode Global Config Mode

no username snmpv3 accessmode

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

Format `no username snmpv3 accessmode` *username*

Command Mode Global Config Mode

username snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are `none`, `md5` or `sha`. If you specify `md5` or `sha`, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The *username* is the user name associated with the authentication protocol. You must enter the *username* in the same case you used when you added the user. To see the case of the *username*, enter the `show users` command.

Default: no authentication

Format `username snmpv3 authentication` *username* {`none` | `md5` | `sha`}

Command Mode Global Config Mode

no username snmpv3 authentication

This command sets the authentication protocol to be used for the specified user to `none`. The *username* is the user name associated with the authentication protocol.

Format `no username snmpv3 authentication` *username*

Command Mode Global Config Mode

username snmpv3 encryption

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

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

The *username* parameter is the registration name of the user who is assigned a specific encryption protocol. You must enter the *username* in the same case you used when you added the user. To see the case of the *username*, enter the `show users` command.

Default: Encryption is not used

Format `username snmpv3 encryption` *username* {`none` | `des`*[key]*}

Command Mode Global Config Mode

no username snmpv3 encryption

This command sets the encryption protocol to **none**. The *username* parameter is the registration name of the user who is assigned a specific encryption protocol.

Format `no username snmpv3 encryption` *username*

Command Mode Global Config Mode

username snmpv3 encryption encrypted

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

Default: Encryption is not used

Format `username snmpv3 encryption encrypted` *`username`* `des` *`key`*

Command Mode Global Config Mode

show users

This command displays the configured user names and their settings. The show users command displays truncated user names. Use the `users long` command to display the complete usernames. The `show users` command is only available for users with Level 15 privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format `show users`

Command Mode Privileged Mode

Parameter	*Description*
User Name	The name the user enters to login using the serial port, Telnet or Web.
Access Mode	Shows whether the user is able to change parameters on the switch (Level 15) or is only able to view them (Level 1). As a factory default, the “admin” user has Level 15 access and the “guest” has Level 1 access.
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to ReadWrite, the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.
SNMPv3 Authentication	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

show users long

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

Format `show users long`

Command Mode Privileged Mode

show users accounts

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

Format `show users accounts [detail]`

Command Mode Privileged Mode

Parameter	*Description*
User Name	The local user account’s user name.
Access Level	The user’s access level (1 for non-privilege (switch>prompt) or 15 for highest privilege (switch# prompt).

Password Aging	Number of days, since the password was configured, until the password expires.
Password Expiry Date	The current password expiration date in date format.
Lockout	Indicates whether the user account is locked out (true or false).

If the detail keyword is included, the following additional fields display.

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

show users login-history [long]

Show information about user connection history.

Format `show users login-history [long]`

Command Mode Privileged Mode

show users login-history [username]

Show information about user connection history.

Format `show users login-history [username` *`name`*`]`

Command Mode Privileged Mode

Parameter	*Description*
name	Username. Length: 1-20 characters

login authentication

Use this command to specify the login authentication method list for a line (console, telnet, or SSH). The default configuration uses the default set with the *aaa authentication login* command.

Format `login authentication {default | list-name}`

Command Mode Line Configuration

Parameter	*Description*
default	Uses the default list created with the `aaa authentication login` command.
list-name	Uses the indicated list created with the `aaa authentication login` command.

no login authentication

Use this command to return to the default specified by the *authentication login* command.

password

This command allows the currently logged in user to change his or her password without having Level 15 privileges.

Format `password cr`

Command Mode User mode

password (Line Configuration)

Use the *password* command in Line Configuration mode to specify a password on a line. The default configuration is no password is specified.

Format `password [password [encrypted]]`

Command Mode Line Config

Parameter	*Description*
password	Password for this level. Length: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

no password (Line Config)

Use this command to remove the password on a line.

Format `no password`

Command Mode Line Config

password (user mode)

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

Format `password`

Command Mode User mode

password (AAA IAS User Configuration)

This command is used to configure a password for a user. An optional parameter [encrypted] is provided to indicate that the password given to the command is already preencrypted.

Format `password password [encrypted]`

Command Mode IAS aaa user configuration mode

no password (IAS aaa user configuration mode)

This command is used to clear the password of a user.

Format `no password`

Command Mode IAS aaa user configuration mode

enable password (Privileged mode)

Use the enable password configuration command to set a local password to control access to the privileged mode.

Format `enable password [password [encrypted]]`

Command Mode Privileged Mode

Parameter	*Description*
password	Password string. Length: 8-64 characters
encrypted	Encrypted password you entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

no enable password (Privileged mode)

Use the no enable password command to remove the password requirement.

Format `no enable password`

Command Mode Privileged Mode

passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 8-64.

Default: 8

Format `passwords min-length 8-64`

Command Mode Global Config Mode

no passwords min-length

Use this command to set the minimum password length to the default value.

Format `no passwords min-length`

Command Mode Global Config Mode

passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don’t reuse their passwords often. Valid values: 0-10.

Default: 0

Format `passwords history 0-10`

Command Mode Global Config Mode

no passwords history

Use this command to set the password history to the default value.

Format `no passwords history`

Command Mode Global Config Mode

passwords aging

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

Default: 0

Format `passwords aging` *`1-365`*

Command Mode Global Config Mode

no passwords aging

Use this command to set the password aging to the default value.

Format `no passwords aging`

Command Mode Global Config Mode

passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with Level 15 access can reactivate a locked user account. Password lockout does not apply to logins from the serial console. Valid values: 1-5. The default is 0, or no lockout count enforced.

Default: 0

Format `passwords lock-out` *`1-5`*

Command Mode Global Config Mode

no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format `no passwords lock-out`

Command Mode Global Config Mode

passwords strength-check

Use this command to enable the password strength feature. It is used to verify the strength of a password during configuration.

Default: Disabled

Format `passwords strength-check`

Command Mode Global Config Mode

no passwords strength-check

Use this command to set the password strength checking to the default value.

Format `no passwords strength-check`

Command Mode Global Config Mode

passwords strength maximum consecutive-characters

Use this command to set the maximum number of consecutive characters to be used in password strength. Valid values: 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default: 0

Format `passwords strength maximum consecutive-characters` *`0-15`*

Command Mode Global Config Mode

passwords strength maximum repeated-characters

Use this command to set the maximum number of repeated characters to be used in password strength. Valid values: 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default: 0

Format `passwords strength maximum consecutive-characters` *`0-15`*

Command Mode Global Config Mode

passwords strength minimum uppercase-letters

Use this command to enforce a minimum number of uppercase letters that a password should contain. Valid values: 0-16. Default value – 2. Minimum of 0 means no restriction on that set of characters.

Default: 2

Format `passwords strength minimum uppercase-letters`

Command Mode Global Config Mode

no passwords strength minimum uppercase-letters

Use this command to reset the minimum uppercase letters required in a password to the default value.

Format `no passwords minimum uppercase-letter`

Command Mode Global Config Mode

passwords strength minimum lowercase-letters

Use this command to enforce a minimum number of lowercase letters that a password should contain. Valid values: 0-16. Default value – 2. Minimum of 0 means no restriction on that set of characters.

Default: 2

Format `passwords strength minimum lowercase-letters`

Command Mode Global Config Mode

no passwords strength minimum lowercase-letters

Use this command to reset the minimum lower letters required in a password to the default value.

Format `no passwords minimum lowercase-letter`

Command Mode Global Config Mode

passwords strength minimum numeric-characters

Use this command to enforce a minimum number of numeric characters that a password should contain. Valid values: 0-16. Default value – 2. Minimum of 0 means no restriction on that set of characters.

Default: 2

Format `passwords strength minimum numeric-characters`

Command Mode Global Config Mode

no passwords strength minimum numeric-characters

Use this command to reset the minimum numeric characters required in a password to the default value.

Format `no passwords minimum numeric-characters`

Command Mode Global Config Mode

passwords strength minimum special-characters

Use this command to enforce a minimum number of special characters that a password should contain. Valid values: 0-16. Default value – 2. Minimum of 0 means no restriction on that set of characters.

Default: 2

Format `passwords strength minimum special-characters`

Command Mode Global Config Mode

no passwords strength minimum special-characters

Use this command to reset the minimum special characters required in a password to the default value.

Format `no passwords minimum special-characters`

Command Mode Global Config Mode

passwords strength minimum character-classes

Use this command to enforce a minimum number of characters classes that a password should contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. Valid values: 0-4. The default is 4.

Default: 4

Format `passwords strength minimum character-classes`

Command Mode Global Config Mode

no passwords strength minimum character-classes

Use this command to reset the minimum number of character classes required in a password to the default value.

Format `no passwords minimum character-classes`

Command Mode Global Config Mode

passwords strength exclude-keyword

Use this command to exclude the specified keyword while configuring the password. The password does not accept the keyword in any form (in between the string, case in-sensitive and reverse) as a sub-string. User can configure up to a maximum of 3 keywords.

Format `passwords strength exclude-keyword` *`keyword`*

Command Mode Global Config Mode

no passwords strength exclude-keyword

Use this command to reset the restriction for the specified keyword or all the keywords configured.

Format `no passwords exclude-keyword` *`[keyword]`*

Command Mode Global Config Mode

show passwords configuration

Use this command to display the configured password management settings.

Format `show passwords configuration`

Command Mode Privileged Mode

Parameter	*Description*
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when configuring passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when configuring passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when configuring passwords.
Maximum Password Consecutive Characters	Maximum number of consecutive characters required that the password should contain when configuring passwords.
Maximum Password	Maximum number of repetition of characters that the password should con-

Repeated Characters	tain when configuring passwords.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.

show passwords result

Use this command to display the last password set result information.

Format `show passwords result`

Command Mode Privileged Mode

Parameter	*Description*
Last User Whose Password Is Set	Shows the name of the user with the most recently set password.
Password Strength Check	Shows whether password strength checking is enabled.
Last Password Set Result	Shows whether the attempt to set a password was successful. If the attempt failed, the reason for the failure is included.

aaa accounting

Use this command in Global Config mode to create an accounting method list for user sessions, user- executed commands, or DOT1X. This list is identified by **default** or a user-specified **list_name**. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end (**start-stop**) or only at the end (**stop-only**). If none is specified, then accounting is disabled for the specified list. If **tacacs** is specified as the accounting method, accounting records are notified to a **TACACS+** server. If **radius** is the specified accounting method, accounting records are notified to a **RADIUS** server.

Please note the following:

- **A maximum of five Accounting Method lists can be created for each exec and commands type.**
- **Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.**
- **The same list-name can be used for both exec and commands accounting type.**
- **AAA Accounting for commands with RADIUS as the accounting method is not supported.**
- **Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.**
- **RADIUS is the only accounting method type supported for DOT1X accounting.**

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

Command Mode Global Config Mode

Parameter	*Description*
exec	Provides accounting for a user terminal sessions.
commands	Provides accounting for all user executed commands.
dot1x	Provides accounting for DOT1X user commands.

default	The default list of methods for accounting services.
list-name	Character string used to name the list of accounting methods.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the beginning of a process and a stop accounting notice at the end of a process.
stop-only	Sends a stop accounting notice at the end of the requested user process.
none	Disables accounting services on this line.
method	Use either TACACS or radius server for accounting purposes.

For the same set of accounting type and list name, the administrator can change the record type, or the methods list, without having to first delete the previous configuration.

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

The first **aaa** command creates a method list for exec sessions with the name ExecList, with **record-type** as `stop-only` and the **method** as TACACS+. The second command changes the **record type** to `start-stop from stop-only` for the same method list. The third command, for the same list changes the methods list to{*tacacs,radius*} from {*tacacs*}.

no aaa accounting

This command deletes the accounting method list.

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

Command Mode Global Config Mode

accounting

Use this command in Line Configuration mode to apply the accounting method list to a line config (console/ telnet/ssh).

Format `accounting {exec | commands } {default | listname}`

Command Mode Line Config

Parameter	*Description*
exec	Only to start/end the session.
commands	This causes accounting for each command execution attempt. If a user is enabling accounting for exec mode for the current line-configuration type, the user will be logged out.
default	The default Accounting List.
listname	The name of the list. String, 15 characters max.

no accounting

Use this command to remove accounting from a Line Configuration mode.

Format `no accounting {exec|commands]`

Command Mode Line Config

show accounting

Use this command to display ordered methods for accounting lists.

Format `show accounting`

Command Mode Privileged Mode

show accounting methods

Use this command to display configured accounting method lists.

Format `show accounting methods`

Command Mode Privileged Mode

clear accounting statistics

This command clears the accounting statistics.

Format `clear accounting statistics`

Command Mode Privileged Mode

show domain-name

This command displays the configured domain-name.

Format `show domain-name`

Command Mode Privileged Mode

aaa ias-user username

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

Use the `aaa ias-user username` command in Global Config mode to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format `aaa ias-user username` *user*

Command Mode Global Config Mode

no aaa ias-user username

Use this command to remove the specified user from the internal user database.

Format `no aaa ias-user username` *user*

Command Mode Global Config Mode

aaa session-id

Use this command in Global Config mode to specify if the same session-id is used for Authentication, Authorization and Accounting service type within a session.

Default: common

Format aaa session-id [common | unique]

Command Mode Global Config Mode

Parameter	*Description*
common	Use the same session-id for all AAA Service types.
unique	Use a unique session-id for all AAA Service types.

no aaa session-id

Use this command in Global Config mode to reset the aaa session-id behavior to the default.

Format no aaa session-id [unique]

Command Mode Global Config Mode

password (AAA IAS User Configuration)

Use this command to specify a password for a user in the IAS database. An optional parameter encrypted is provided to indicate that the password given to the command is already preencrypted.

Format password *password* [encrypted]

Command Mode AAA IAS User Config

Parameter	*Description*
password	Password for this level: 8-64 characters
encrypted	Encrypted password that can be entered or copied from the configuration of another switch

no password (IAS aaa user configuration mode)

Use this command to clear the password of a user.

Format no password

Command Mode IAS aaa user configuration mode

clear aaa ias-users

Use this command to remove all users from the IAS database.

Format clear aaa ias-users

Command Mode Privileged Mode

Parameter	*Definition*
password	Password for this level: 8-64 characters
encrypted	Encrypted password that can be entered or copied from the configuration of another switch

show aaa ias-users

Use this command to display configured IAS users and their attributes. Passwords configured are not shown in the show command output.

Format `show aaa ias-users [username]`

Command Mode Privileged Mode

8.9 SNMP configuration commands

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

snmp-server

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

Default: None

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

Command Mode Global Config Mode

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

snmp-server community

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

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

Default: Two communities are created by default:

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

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

Command Mode Global Config Mode

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

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

no snmp-server community

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

Format `no snmp-server community` *`community-name`*

Command Mode Global Config Mode

snmp-server community-group

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

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

Command Mode Global Config Mode

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

snmp-server enable traps violation

The Port MAC locking component interprets this command and configures violation action to send an SNMP trap with default trap frequency of 30 seconds. The Global command configures the trap violation mode across all interfaces valid for port-security.

Default: Disabled

Format `snmp-server enable traps violation`

Command Mode Global Config Mode

Interface Config

no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format `no snmp-server enable traps violation`

Command Mode Interface Config

snmp-server enable traps

This command enables the Authentication Flag.

Default: Enabled

Format `snmp-server enable traps`

Command Mode Global Config Mode

no snmp-server enable traps

This command disables the Authentication Flag.

Format `no snmp-server enable traps`

Command Mode Global Config Mode

snmp-server enable traps bgp

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

Default: BGP traps are disabled by default.

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

Command Mode Global Config Mode

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

no snmp-server enable traps bgp state-changes limited

This command disables the two traps defined in the standard BGP MIB, RFC 4273.

Format `no snmp-server enable traps bgp state-changes limited`

Command Mode Global Config Mode

snmp-server enable traps fip-snooping

This command enables FCoE Initialization Protocol (FIP) snooping traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See section `show snmp`.

Default: Enabled

Format `snmp-server enable traps fip-snooping`

Command Mode Global Config Mode

no snmp-server enable traps fip-snooping

This command disables FCoE Initialization Protocol (FIP) snooping traps for the entire switch.

Default: Enabled

Format `no snmp-server enable traps fip-snooping`

Command Mode Global Config Mode

snmp-server port

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

Default: 161

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

Command Mode Privileged Mode

no snmp-server port

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

Format `no snmp-server port`

Command Mode Privileged Mode

snmp trap link-status

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

The command is available only when the Link Up/Down Flag is enabled.

Format `snmp trap link-status`

Command Mode Interface Config

no snmp trap link-status

This command disables link status traps by interface.

The command is available only when the Link Up/Down Flag is enabled.

Format `no snmp trap link-status`

Command Mode Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

The command is available only when the Link Up/Down Flag is enabled.

Format `snmp trap link-status all`

Command Mode Global Config Mode

no snmp trap link-status all

This command disables link status traps for all interfaces.

The command is available only when the Link Up/Down Flag is enabled.

Format `no snmp trap link-status all`
Command Mode Global Config Mode

snmp-server enable traps linkmode

The command is available only when the Link Up/Down Flag is enabled.

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled.

Default: Enabled
Format `snmp-server enable traps linkmode`
Command Mode Global Config Mode

no snmp-server enable traps linkmode

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

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

snmp-server enable traps multiusers

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

Default: Enabled
Format `snmp-server enable traps multiusers`
Command Mode Global Config Mode

no snmp-server enable traps multiusers

This command disables Multiple User traps.

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

snmp-server enable traps stpmode

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

Default: Enabled

Format `snmp-server enable traps stpmode`

Command Mode Global Config Mode

no snmp-server enable traps stpmode

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

Format `no snmp-server enable traps stpmode`

Command Mode Global Config Mode

snmp-server engineID local

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

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

Format `snmp-server engineID local {`*`engineid-string`*`|default}`

Command Mode Global Config Mode

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

Caution! Changing the engine-id will invalidate all SNMP configuration that exists on the box.

no snmp-server engineID local

This command removes the specified engine ID.

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

Format `no snmp-server engineID local`

Command Mode Global Config Mode

snmp-server filter

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

Default: There is no default filters.

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

Command Mode Global Config Mode

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

no snmp-server filter

This command removes the specified filter.

Default: There is no default filters.

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

Command Mode Global Config Mode

snmp-server group

This command creates an SNMP access group.

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

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

Command Mode Global Config Mode

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

no snmp-server group

This command removes the specified group.

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

Command Mode Global Config Mode

snmp-server host

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

Default: No default hosts are configured.

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

Command Mode Global Config Mode

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

no snmp-server host

This command removes the specified host entry.

Format `no snmp-server host host-addr [traps|informs]`

Command Mode Global Config Mode

snmp-server user

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

Default: No default users are created.

Format snmp-server user *username groupname* [remote *engineid-string*] [{auth-md5 *password* | auth-sha *password* | auth-md5-key *md5-key* | auth-sha-key *sha-key*} [priv-des *password* | priv-des-key *des-key*]

Command Mode Global Config Mode

Parameter	*Description*
username	The username the SNMPv3 user will connect to the switch as. The range is 1-30 characters
group-name	The name of the group the user belongs to. The range is 1-30 characters
engineid-string	The engine-id of the remote management station that this user will be connecting from. The range is 5 to 32 characters.
password	The password the user will use for the authentication or encryption mechanism. The range is 1 to 32 characters.
md5-key	A pregenerated MD5 authentication key. The length is 32 characters.
sha-key	A pregenerated SHA authentication key. The length is 48 characters.
des-key	A pregenerated DES encryption key. The length is 32 characters if MD5 is selected, 48 characters if SHA is selected.

no snmp-server user

This command removes the specified SNMPv3 user.

Format no snmp-server user *username*

Command Mode Global Config Mode

snmp-server view

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

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

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

Command Mode Global Config Mode

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

no snmp-server view

This command removes the specified view.

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

Command Mode Global Config Mode

snmp-server v3-host

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

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

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

Command Mode Global Config Mode

Parameter	*Description*
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
user-name	User used to send a Trap or Inform message. This user must be associated with a group that supports the version and access method. The range is 1-30 characters
traps	Send SNMP traps to the host. This is the default option.
informs	Send SNMP informs to the host.
seconds	Number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	Number of times to resend an Inform. Default: 3 attempts. The range is 0 to 255 retries.
auth	Enables authentication but not encryption.
noauth	No authentication or encryption. This is the default.
priv	Enables authentication and encryption.
port	The SNMP Trap receiver port. Default: port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1-30 characters.

snmptrap source-interface

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

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

Command Mode Global Config Mode

Parameter	*Description*
unit/slot/port	Configures the IPv6 tunnel interface as the SNMP messages source IP address.
loopback-id	Configures the loopback interface as the SNMP messages source IP address. The range of the loopback ID is 0 to 7.
tunnel-id	Configures the IPv6 tunnel interface as the SNMP messages source IP address. The range of the tunnel ID is 0 to 7.
vlan-id	Configures the VLAN interface to use as the SNMP messages source IP address. ID VLAN range: 1-4093
serviceport	Configures the OOB interface to use as the SNMP messages source IP address.

network	Configures the management interface to use as the SNMP messages source IP address.

no snmptrap source-interface

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

Format `no snmptrap source-interface`

Command Mode Global Config Mode

snmptrap ipaddr snmpversion[1]

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

This command doesn't have the negative form.

Format `snmptrap ipaddr snmpversion` *`name snmpversion`*

Command Mode Global Config Mode

snmptrap ip6addr snmpversion[1]

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

This command doesn't have the negative form.

Format `snmptrap ip6addr snmpversion` *`name snmpversion`*

Command Mode Global Config Mode

show snmp

This command displays the current SNMP configuration.

Format `show snmp`

Command Mode Privileged Mode

Parameter		*Definition*
Community Table:	**Community-String**	The community string for the entry. This is used by SNMPv1 and SNMPv2 protocols to access the switch.
	Community-Access	The type of access the community has: • Read only • Read write • Super User

[1] Not supported in the current firmware version 8.4.0.6

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

show snmp engineID

This command displays the currently configured SNMP engineID.

Format `show snmp engineID`

Command Mode Privileged Mode

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

show snmp filters

This command displays the configured filters used when sending traps.

Format `show snmp filters [`*`filtername`*`]`

Command Mode Privileged Mode

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

show snmp group

This command displays the configured groups.

Format `show snmp group [`*`groupname`*`]`

Command Mode Privileged Mode

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

show snmp-server

This command displays the current SNMP server user configuration.

Format `show snmp-server`

Command Mode Privileged Mode

show snmp source-interface

Use this command in Privileged mode to display the configured global source-interface (Source IP address) details used for an SNMP client.

Format `show snmp source-interface`

Command Mode Privileged Mode

show snmp user

This command displays the currently configured SNMPv3 users.

Format `show snmp user [`*`username`*`]`

Command Mode Privileged Mode

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

show snmp views

This command displays the currently configured views.

Format `show snmp views [`*`viewname`*`]`

Command Mode Privileged Mode

Parameter	Description
Name	The view name for this entry.

OID Tree	The OID tree that this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID tree.

show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 and OSPFv3 trapflags. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`

Command Mode Privileged Mode

Parameter	*Definition*
Authentication Flag	Can be enabled or disabled. Default: enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled/disabled. Default: enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled/disabled. Default: enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled/disabled. Default: enabled. Indicates whether spanning tree traps are sent.
ACL Traps	Can be enabled/disabled. Default: disabled. Indicates whether ACL traps are sent.
BGP4 Traps	Can be enabled/disabled. Default: disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)
OSPFv2 Traps	Can be enabled/disabled. Default: disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays disabled. Otherwise, the command shows all the enabled OSPF traps' information.
OSPFv3 Traps	Can be enabled/disabled. Default: disabled. Indicates whether OSPF traps are sent. If any of the OSPFv3 trap flags are not enabled, then the command displays disabled. Otherwise, the command shows all the enabled OSPFv3 traps' information.

8.10 RADIUS configuration commands

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

aaa server radius dynamic-author

This command enables CoA functionality and enters dynamic authorization local server configuration mode.

Default: None

Format `aaa server radius dynamic-author`

Command Mode Global Config Mode

no aaa server radius dynamic-author

Disable CoA.

Default: None

Format `no aaa server radius dynamic-author`

Command Mode Global Config Mode

authentication command bounce-port ignore

Use this command to prevent the system from processing bounce-host-port commands from a RADIUS server. The bounce-host-port command causes the device to drop the connection on the authenticated port.

Default: Off

Format `authentication command bounce-port ignore`

Command Mode Global Config Mode

no authentication command bounce-port ignore

Use this command to cancel the prevention of the system from processing bounce-host-port commands from a RADIUS server.

Format `no authentication command bounce-port ignore`

Command Mode Global Config Mode

auth-type

Use this command to specify the type of authorization that the device uses for RADIUS clients. The client must match the configured attributes for authorization.

Default: All

Format `auth-type { any | all | session-key }`

Command Mode Dynamic authorization mode

no auth-type

Use this command to reset the type of authorization that the device must use for RADIUS clients.

Default: None

Format `no auth-type`

Command Mode Dynamic authorization mode

authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Default: Disabled

Format `authorization network radius`

Command Mode Global Config Mode

no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the radius server.

Format `no authorization network radius`

Command Mode Global Config Mode

clear radius dynamic-author statistics

This command clears radius dynamic authorization counters.

Default: none

Format `clear radius dynamic-author statistics`

Command Mode Privileged Mode

client

Use this command to configure the IP address or hostname of the AAA server client. Use the optional server- key keyword and string argument to configure the server key at the client level.

Default: None

Format `client { ip-address | hostname } [server-key [0|7] key-string]`

Command Mode Dynamic authorization mode

no client

Use this command to remove the configured Dynamic Authorization client and the key associated with that client in the device.

Default: None

Format `no client { ip-address | hostname }`

Command Mode Dynamic authorization mode

debug aaa coa

Use this command to display Dynamic Authorization Server processing debug information.

Default: None

Format `debug aaa coa`

Command Mode Dynamic authorization mode

debug aaa pod

Use this command to display Disconnect Message packets.

Default: None

Format `debug aaa pod`

Command Mode Dynamic authorization mode

ignore server-key

Use this optional command to configure the device to ignore the server key.

Default: Disabled

Format `ignore server-key`

Command Mode: Dynamic authorization mode

no ignore server-key

Use this optional command to configure the device not to ignore the server key. Optional command.

Default: Disabled

Format `no ignore server-key`

Command Mode: Dynamic authorization mode

ignore session-key

Use this optional command to configure the device to ignore the session key. Optional command.

Default: Disabled

Format `ignore session-key`

Command Mode: Dynamic authorization mode

no ignore session-key

Use this optional command to configure the device to not ignore the session key. Optional command.

Default: Enabled

Format `no ignore session-key`

Command Mode: Dynamic authorization mode

port

Use this command to specify the UDP port on which a device listens for RADIUS requests from configured Dynamic Authorization clients. The supported range for the port-number is 1025 to 65535.

Default: 3799

Format `port port-number`

Command Mode: Dynamic authorization mode

no port

Use this command to reset the configured UDP port on which a device listens for RADIUS requests from configured Dynamic Authorization clients.

Default: 3799

Format `no port`

Command Mode: Dynamic authorization mode

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default: Disabled

Format `radius accounting mode`

Command Mode: Global Config Mode

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format `no radius accounting mode`

Command Mode: Global Config Mode

radius server attribute 4

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

Format `radius server attribute 4 [ipaddr]`

Command Mode: Global Config Mode

Parameter	*Description*
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IP address of the server.

no radius server attribute 4

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

Format `no radius server attribute 4 [ipaddr]`

Command Mode: Global Config Mode

radius server attribute 95

This command specifies the RADIUS client to use the NAS-IPv6 Address attribute in the RADIUS requests. If the specific IPv6 address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format `radius server attribute 95 [ipv6addr]`

Command Mode: Global Config Mode

Parameter	*Description*
95	NAS-IPv6-Address attribute to be used in RADIUS requests.
Ipv6addr	The IPv6 address of the server.

no radius server attribute 95

The no version of this command disables the NAS-IPv6-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IPv6-Address attribute in RADIUS requests.

Format `no radius server attribute 95 [ipv6addr]`

Command Mode: Global Config Mode

radius server attribute 31

This command specifies the calling station id to use the NAS client in the specified MAC format in the RADIUS requests.

Format `radius server attribute 31 mac-format [ietf | legacy | unformated] [lower-case | upper-case]`

Command Mode: Global Config Mode

calling station id format	**Description**
ietf	aa-bb-cc-dd-ee-ff
legacy	aa:bb:cc:dd:ee:ff
unformated	aaaabbbbcccc

no radius server attribute 31 mac-formate

The no version of this command disables the 31 NAS attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the calling station id attribute in RADIUS requests.

Format `radius server attribute 31 mac-format`

Command Mode: Global Config Mode

radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the Default_RADIUS_Auth_Server and Default_RADIUS_Acct_Server as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the auth parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the "no" form of the command. If you use the optional port parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The port number range is 1 - 65535, with 1812 being the default value.

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

If you use the acct token, the command configures the IP address or hostname to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the "no" form of the command to remove it from the configuration. The IP address or hostname you specify must match that of a previously configured accounting server. If you use the optional port parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a port is already configured for the accounting server, the new port replaces the previously configured port. The port must be a value in the range 0 - 65535, with 1813 being the default.

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

Format `radius server host {auth | acct} {`*`ipaddr`*`|`*`dnsname`*`} [name `*`servername`*`] transport {tls | udp} [0-8] [port `*`0-65535`*`]`

Command Mode: Global Config Mode

Field	*Description*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
0-65535	The port number to use to connect to the specified RADIUS server.
0-8	The number of the memory cell where the uploaded keys and certificates for tls connection are stored.
servername	The alias name to identify the server.
tls	Use tls connection to communicate with radius server.
udp	Use udp to communicate with radius server.

no radius server host

The no version of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration.

Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The ipaddr|dnsname parameter must match the IP address or DNS name of the previously configured RADIUS authentication / accounting server.

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

Command Mode: Global Config Mode

radius server key

This command configures the key to be used in RADIUS client communication with the specified server. Depending on whether the 'auth' or 'acct' token is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

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

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

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

Command Mode: Global Config Mode

Field	*Description*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
password	The password in encrypted format.

radius server msgauth

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

Format `radius server msgauth` *`ipaddr|dnsname`*

Command Mode: Global Config Mode

Field	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.

no radius server msgauth

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

Format `no radius server msgauth` *ipaddr|dnsname*

Command Mode Global Config Mode

radius server primary

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

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

Command Mode: Global Config Mode

Field	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.

radius server retransmit

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

Default: 4

Format `radius server retransmit` *retries*

Command Mode: Global Config Mode

Field	Description
retries	The maximum number of transmission attempts. Range of values: 1-15.

no radius server retransmit

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

Format `no radius server retransmit`

Command Mode: Global Config Mode

radius source-interface

Use this command to specify the physical or logical interface to use as the RADIUS client source interface (Source IP address). If configured, the address of source Interface is used for all RADIUS communications between the RADIUS server and the RADIUS client. The selected source-interface IP address is used for filling the IP header of RADIUS management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the RADIUS client falls back to its default behavior.

Format `radius source-interface {`*`unit/slot/port`* | `loopback` *`loopback-id`* | `vlan` *`vlan-id`* | *`serviseport`* | *`network`*`}`

Command Mode: Global Config Mode

Field	*Description*
unit/slot/port	The unit identifier assigned to the switch.
loopback-id	Configures the loopback interface. The range of the loopback ID is 0 to 63.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4094.

no radius source-interface

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

Format `no radius source-interface`

Command Mode: Global Config Mode

radius server timeout

This command configures the global parameter for the RADIUS client that specifies the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. Range of values: integer from 1 to 30.

Default: 5

Format `radius server timeout` *`seconds`*

Command Mode: Global Config Mode

Field	*Description*
retries	Maximum number of transmission attempts in the range 1–30.

no radius server timeout

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

Format `no radius server timeout`

Command Mode: Global Config Mode

server-key

Use this command to configure a global shared secret that is used for all dynamic authorization clients that do not have an individual shared secret key configured.

Default: None

Format `server-key [7] key-string`

Command Mode Dynamic authorization mode

Field	*Description*
0	An unencrypted key is to be entered
7	An encrypted key is to be entered
string	The shared secret string. Maximum length is 128 characters for unencrypted key and 256 characters for encrypted key. Overrides the global setting for this client only. Enclose in quotes to use special characters or embedded blanks.

no server-key

Use this command to remove the global shared secret key configuration.

Default: None

Format `no server-key`

Mode Dynamic authorization mode

show radius servers

Use this command to display the authentication parameters.

Format `show radius servers { serverIP | name serverName }`

Command Mode User mode

show radius

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

Format `show radius`

Command Mode: Privileged Mode

Parameter	*Definition*
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Number of Named Authentication Server Groups	The number of configured named RADIUS authentication server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.

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

show radius servers

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

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

Command Mode Privileged Mode

Field	*Description*
ipaddr	The IP address of the authenticating server.
dnsname	The DNS name of the authenticating server.
servername	The alias name to identify the server.
Current	The * symbol preceding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	Global parameter. A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	Global parameter. A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	Global parameter. A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	Global parameter. A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format `show radius accounting name [servername]`

Command Mode Privileged Mode

Field	*Description*
servername	An alias name to identify the server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

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

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

show radius accounting statistics

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

Format `show radius accounting statistics {ipaddr|dnsname | name servername}`

Command Mode Privileged Mode

Parameter	*Description*
ipaddr.	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Accounting Server Name	The name of the accounting server.
Server Host Address	The IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authen-

	ticators or signature attributes or unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

show radius source-interface

Use this command in Privileged mode to display the configured RADIUS client source-interface (Source IP address) information.

Format `show radius source-interface`

Command Mode Privileged Mode

show radius statistics

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

Format `show radius statistics {`*`ipaddr`*`|`*`dnsname`*` | name `*`servername`*`}`

Command Mode Privileged Mode

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

Malformed Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

8.11 TACACS+ configuration commands

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

tacacs-server host

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

Format `tacacs-server host { ip-address | ipv6-address | hostname}`

Command Mode Global Config Mode

no tacacs-server host

Use the no tacacs-server host command to delete the specified hostname or IP address. The ip- address|hostname parameter is the IP address of the TACACS+ server.

Format `no tacacs-server host { ip-address | ipv6-address | hostname}`

Command Mode Global Config Mode

tacacs-server key

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

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

Format `tacacs-server key [key-string | encrypted key-string]`

Command Mode Global Config Mode

no tacacs-server key

Use the no tacacs-server key command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The key-string parameter has a range of 0 - 128 characters. This key must match the key used on the TACACS+ daemon.

Format `no tacacs-server key key-string`

Command Mode Global Config Mode

tacacs-server keystring

Use the tacacs-server keystring command to set the global authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format `tacacs-server keystring`

Command Mode Global Config Mode

tacacs-server source-interface

Use this command in Global Configuration mode to configure the source interface (Source IP address) for TACACS+ server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Format `tacacs-server source-interface {unit/slot/port|loopback loopback-id|vlan vlan-id|serviseport|network}`

Command Mode Global Config Mode

Parameter	*Description*
unit/slot/port	The unit identifier assigned to the switch, in unit/slot/port format.
loopback-id	The loopback interface. The range of the loopback ID is 0-63
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1-4093

no tacacs-server source-interface

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

Format `no tacacs-server source-interface`

Command Mode Global Config Mode

tacacs-server timeout

Use the tacacs-server timeout command to set the timeout value for communication with the TACACS+ servers. The *timeout* parameter has a range of 1-30 and is the timeout value in seconds. If you do not specify a timeout value, the command sets the global timeout to the default value. TACACS+ servers that do not use the global timeout will retain their configured timeout values.

Default: 5

Format `tacacs-server timeout` *timeout*

Command Mode Global Config Mode

no tacacs-server timeout

Use the no tacacs-server timeout command to restore the default timeout value for all TACACS servers.

Format `no tacacs-server timeout`

Command Mode Global Config Mode

key

Use the key command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS+ daemon. The key-string parameter specifies the key name. For an empty string use " ". (Range: 0 - 128 characters).

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

Format `key [`*key-string* | `encrypted` *key-string*`]`

Command Mode TACACS Config

keystring

Use the keystring command in TACACS Server Configuration mode to set the TACACS+ server-specific authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format `keystring`

Command Mode TACACS server configuration mode

port

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

Default: 49

Format port *port-number*

Command Mode TACACS Config

priority (TACACS Config)

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

Default: 0

Format priority *priority*

Command Mode TACACS Config

timeout

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

Format timeout *timeout*

Command Mode TACACS Config

show tacacs

Use the show tacacs command to display the configuration, statistics, and source interface details of the TACACS+ client.

Format show tacacs [*ip-address*|*hostname*|*client*|*server*]

Command Mode Privileged Mode

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

show tacacs source-interface

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

Format show tacacs source-interface

Command Mode Privileged Mode

8.12 Configuration Scripting commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit

them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the `show running-config` command to capture the running configuration into a script. Use the `copy` command to transfer the configuration script to or from the switch.

Use the `show` command to view the configuration stored in the startup-config, backup-config, or factory- defaults file.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- Script files are not distributed across the stack, and only live in the unit that is the master unit at the time of the file download.
- The file extension must be ".scr".
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the "!" character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

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

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

script apply

This command applies the commands in the script to the switch. The *scriptname* parameter is the name of the script to apply.

Format `script apply scriptname`

Command Mode Privileged Mode

script delete

This command deletes a specified script. The *scriptname* parameter is the name of the script to be deleted. The *all* option deletes all the scripts present on the switch.

Format `script delete {scriptname | all}`

Command Mode Privileged Mode

script list

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

Format `script list`

Command Mode Privileged Mode

Parameter	*Description*
Configuration Script	Name of the script.
Size	Size of the script file.

script show

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

Format `script show scriptname`

Command Mode Privileged Mode

Parameter	*Description*
Output Format	Line number: `line contents.`

script validate

This command validates a script file by parsing each line in the script file where *scriptname* is the name of the script to validate. The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

Format `script validate scriptname`

Command Mode Privileged Mode

8.13 Prelogin Banner, System Prompt, and Host Name commands

This section describes the commands you use to configure the prelogin banner and the system prompt. The prelogin banner is the text that displays before you login at the User: prompt.

copy (pre-login banner)

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

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

Default: None

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

Command Mode Privileged Mode

set prompt

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

Format `set prompt prompt_string`

Command Mode Privileged Mode

hostname

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

Format `hostname hostname`

Command Mode Privileged Mode

show clibanner

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

Default: No contents to display before displaying the login prompt.

Format `show clibanner`

Command Mode Privileged Mode

set clibanner

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

Format `set clibanner line`

Command Mode Global Config Mode

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

no set clibanner

Use this command to disable configured CLI banner.

Format `no set clibanner`
Command Mode Global Config Mode

9 SWITCHING CONFIGURATION COMMANDS

This chapter describes the switching commands available in the CLI.

All commands listed in this section are divided into three functional groups:

- **Show commands display switch configuration information, statistics, and other information.**
- **Configuration commands configure switch features. 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.**

9.1 Port configuration commands

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

interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port). You can also specify a range of ports to configure at the same time by specifying the starting unit/slot/port and ending unit/slot/port, separated by a hyphen.

Format: `interface {unit/slot/port | unit/slot/port(start of the range)-unit/slot/port(end of the range)}`

Command mode: Global Config

auto-negotiate

This command enables automatic negotiation on a port or range of ports.

This command has been deprecated. The Auto-negotiation enable/disable option is no longer available using auto-negotiate. Instead, different variants of the speed command (i.e., speed andspeed auto are used to disable and enable auto-negotiation, respectively. However, backward compatibility will be maintained for the auto-negotiate command, so a configuration script that has the auto-negotiate command is still supported. Both, text-based as well as binary-based configuration migration will be handled to keep this command backward compatible.

Default: enabled

Format: `auto-negotiate`

Command mode: Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Automatic sensing is disabled when automatic negotiation is disabled.

Format: `no auto-negotiate`

Command mode: Interface Config

auto-negotiate all

This command enables automatic negotiation on all ports.

Default: enabled

Format: `auto-negotiate all`

Command mode: Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format: `no auto-negotiate all`

Command mode: Global Config

description

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format: `description description`

Command mode: Interface Config

media-type

Use this command to change between fiber and copper mode on the Combo port.

- Combo Port: A port or an interface that can operate in either copper or in fiber mode.
- Copper and Fiber port: A port that uses copper a medium for communication (for example, RJ45 ports). A fiber port uses the fiber optics as a medium for communication (for example, example SFP ports).

Default: Auto-select, SFP preferred

Format: `media-type {auto-select | rj45 | sfp }`

Command mode: Interface Config

The following modes are supported by the media-type command.

- ***Auto-select, SFP preferred:*** The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the fiber link takes precedence and the fiber link is up.
- ***Auto-select, RJ45 preferred:*** The medium is selected automatically based on the physical medium

presence. However, when both the fiber and copper links are connected, the copper link takes precedence and the copper link is up.

- ***SFP:*** Only the fiber medium works. The copper medium is always down.
- ***RJ45:*** Only the copper medium works. The fiber medium is always down.

no media-type

Use this command to revert the media-type configuration and configure the default value on the interface.

Format: `no media-type`

Command mode: Interface Config

mtu

Use the mtu command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the mtu command to configure jumbo frame support for physical and port- channel (LAG) interfaces. For the standard implementation, the MTU size is a valid integer between 1504–12270 for tagged packets and a valid integer between 1500–12270 for untagged packets.

To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IPHeader + IP payload), see "ip mtu" command on page 819.

Default: 1500 (untagged)

Format: `mtu 1500-12270 (for MES5448)/mtu 1500-9394 (for MES7048)`

Command mode: Interface Config

no mtu

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

Format: `no mtu`

Command mode: Interface Config

shutdown

This command disables a port or range of ports.

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

Default: enabled

Format: `shutdown`

Command mode: Interface Config

no shutdown

This command enables a port.

Format: `no shutdown`

Command mode: Interface Config

shutdown all

This command disables all ports.

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

Default: enabled

Format: `shutdown all`

Command mode: Global Config

no shutdown all

This command enables all ports.

Format: `no shutdown all`

Command mode: Global Config

speed

Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. The duplex parameter allows you to set the advertised speed for both half as well as full duplex mode.

Use the auto keyword to enable auto-negotiation on the port. Use the command without the auto keyword to ensure auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is disabled, the speed and duplex mode must be set.

Default: autonegotiation enabled.

Format: `speed auto {10|100|1000|2.5G|10G|20G|25G|40G|50G|100G} [10|100|1000|2.5G|10G|20G|25G|40G|50G|100G] [half-duplex|full-duplex]`

`speed {10|100|1000|2.5G|10G|20G|25G|40G|50G|100G} {half-duplex|full-duplex}.`

Command mode: Interface Config

speed all

This command sets the speed and duplex setting for all interfaces if auto-negotiation is disabled. If auto-negotiation is enabled, an error message is returned. Use the no auto-negotiate command to disable.

Default: autonegotiation enabled. Adv. is 10h, 10f, 100h, 100f, 1000f.

Format: `speed all {100 | 10} {half-duplex | full-duplex}`

Command mode: Global Config

hardware profile portmode

This command is used to change the operating mode of interfaces x/0/49-52 (for MES5448) and x/0/49-54 (for MES7048).

Format: `hardware profile portmode {1x100G | 1x40G | 4x10G}`

Command mode: interface configuration

MES7048 supports 1x100G/1x40G interfaces and MES5448 supports 1x40G/4x10G interfaces.

show interface media-type[1]

Use this command to display the media-type configuration of the interface.

Format: `show interface media-type`

Command mode: Privileged

The following information is displayed for the command.

Parameter	*Description*
Port	The interface in unit/slot/port format.
Configured Media Type	The media type for the interface. auto-select—The media type is automatically selected. The preferred media type is displayed. RJ45 — port RJ45 SFP — port SFP-port
Active	Displays the current operational state of the combo port.

show interfaces status

Use this command to display interface information, including the description, port state, speed and auto-neg capabilities. The command is similar to *show port* all but displays additional fields like interface description and port-capability. The description of the interface is configurable through the existing command description <*name*> which has a maximum length of 28 characters.

Default: Disabled

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

Command Mode: Privileged

Parameter	*Description*
Port	The interface in unit/slot/port format.

[1] Not supported in the current firmware version

Name	The descriptive user-configured name for the interface.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. Possible values are: enabled or disabled. The factory default is enabled.
Link State	Shows whether the link is up or down.
Physical Mode	The speed and duplex settings on the interface. If autonegotiation support is selected, speed and duplex mode are set during the auto negotiation process. Note that the maximum capability of the port (full duplex - 100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is auto (autonegotiation).
Physical Status	The port speed and duplex mode.
Media type	The type of the connected SFP module.
Flow Control Status	Flow Control status.

show port

This command displays port information.

Format: `show port {intf-range | all}`

Command mode: Privileged

Parameter	***Description***
Interface	The interface in unit/slot/port format
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: *Mirror* — this port is a monitoring port. For more information, see “Port Mirroring Commands” on page 617. *PC Mbr* — this port is a member of a port-channel (LAG). *Probe* — this port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. Possible values are: enabled or disabled. The factory default is enabled.
Physical Mode	The speed and duplex settings on the interface. If autonegotiation support is selected, speed and duplex mode are set during the auto negotiation process. Note that the maximum capability of the port (full duplex - 100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is auto (autonegotiation).
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

show port advertise

Use this command to display the local administrative link advertisement configuration, local operational link advertisement, and the link partner advertisement for an interface. It also displays priority Resolution for speed and duplex as per 802.3 Annex 28B.3. It displays the Auto negotiation state, PHY Master/Slave Clock configuration, and Link state of the port.

If the link is down, the Clock is displayed as No Link, and a dash is displayed against the Oper Peer advertisement, and Priority Resolution. If Auto negotiation is disabled, then the admin Local Link advertisement, operational local link advertisement, operational peer advertisement, and Priority resolution fields are not displayed.

If this command is executed without the optional unit/slot/port parameter, then it displays the Auto- negotiation state and operational Local link advertisement for all the ports. Operational link advertisement will display speed only if it is supported by both local as well as link partner. If auto-negotiation is disabled, then operational local link advertisement is not displayed.

Format: `show port advertise [unit/slot/port]`

Command mode: Privileged

show port description

This command displays the interface description. Instead of unit/slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Format: `show port description unit/slot/port`

Command mode: Privileged

Parameter	*Description*
Interface	The interface in unit/slot/port format.
Index	The interface index number associated with the port.
Description	The alpha-numeric description of the interface created by the “description” commandon page 425.
MAC Address	The MAC address of the port. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Bit Offset Val	The bit offset value.

show interfaces hardware profile

This command displays the current mode of the interfaces x/0/49-52 (for MES5448) and x/0/49-54 (for MES7048), as well as the mode that will be activated after rebooting the device.

Format: `show interfaces hardware profile [unit/slot/port]`

Command mode: privileged

9.2 STP configuration commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

STP is enabled on the switch and on all ports and LAGs by default.

spanning-tree

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

Default: enabled

Format: `spanning-tree`

Command mode: Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format: `no spanning-tree`

Command mode: Global Config

spanning-tree auto-edge

Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

Default: enabled

Format: `spanning-tree auto-edge`

Command mode: Interface Config

no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Format: `no spanning-tree auto-edge`

Command mode: Interface Config

spanning-tree backbonefast

Use this command to enable the detection of indirect link failures and accelerate spanning tree convergence on PVSTP+ configured switches.

Backbonefast accelerates finding an alternate path when an indirect link to the root port goes down.

Backbonefast can be configured even if the switch is configured for MST(RSTP) or PVST+ mode. It only has an effect when the switch is configured for the PVST+ mode.

If a backbonefast-enabled switch receives an inferior BPDU from its designated switch on a root or blocked port, it sets the maximum aging time on the interfaces on which it received the inferior BPDU if there are alternate paths to the designated switch. This allows a blocked port to immediately move to the listening state where the port can be transitioned to the forwarding state in the normal manner.

On receipt of an inferior BPDU from a designated bridge, backbonefast enabled switches send a Root Link Query (RLQ) request to all non-designated ports except the port from which it received the

inferior BPDU. This check validates that the switch can receive packets from the root on ports where it expects to receive BPDUs. The port from which the original inferior BPDU was received is excluded because it has already encountered a failure. Designated ports are excluded as they do not lead to the root.

On receipt of an RLQ response, if the answer is negative, the receiving port has lost connection to the root and its BPDU is immediately aged out. If all nondesignated ports have already received a negative answer, the whole bridge has lost the root and can start the STP calculation from scratch.

If the answer confirms the switch can access the root bridge on a port, it can immediately age out the port on which it initially received the inferior BPDU.

A bridge that sends an RLQ puts its bridge ID in the PDU. This ensures that it does not flood the response on designated ports.

A bridge that receives an RLQ and has connectivity to the root forwards the query toward the root through its root port.

A bridge that receives a RLQ request and does not have connectivity to the root (switch bridge ID is different from the root bridge ID in the query) or is the root bridge immediately answers the query with its root bridge ID.

RLQ responses are flooded on designated ports.

Default: NA

Format: `spanning-tree backbonefast`

Command mode: Global Config

no spanning-tree backbonefast

This command disables backbonefast.

RPVSTP+ embeds support for backbonefast and uplinkfast. Even if FastUplink and FastBackbone are configured, they are effective only in PVSTP+ mode.

Format: `no spanning-tree backbonefast`

Command mode: Global Config

spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

Default: disabled

Format: `spanning-tree bpdufilter`

Command mode: Interface Config

no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default: disabled

Format: `no spanning-tree bpdufilter`

Command mode: Interface Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default: disabled

Format: `spanning-tree bpdufilter default`

Command mode: Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default: disabled

Format: `no spanning-tree bpdufilter default`

Command mode: Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on an interface or range of interfaces.

Default: disabled

Format: `spanning-tree bpduflood`

Command mode: Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface or range of interfaces.

Default: disabled

Format: `no spanning-tree bpduflood`

Command mode: Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default: disabled

Format: `spanning-tree bpduguard`

Command mode: Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default: disabled

Format: `no spanning-tree bpduguard`

Command mode: Global Config

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *unit/slot/port* parameter to transmit a BPDU from a specified interface, or use the *all* keyword to transmit RST or MST BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a no version.

Format: `spanning-tree bpdumigrationcheck {unit/slot/port | all}`

Command mode: Global Config

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The name is a string of up to 32 characters.

Default: base MAC address in hexadecimal notation

Format: `spanning-tree configuration name name`

Command mode: Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format: `no spanning-tree configuration name`

Command mode: Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default: 0

Format: `spanning-tree configuration revision 0-65535`

Command mode: Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format: `no spanning-tree configuration revision`

Command mode: Global Config

spanning-tree cost

Use this command to configure the external path cost for port used by a MST instance. When the auto keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a cost value from 1–200000000.

Default: auto

Format: `spanning-tree cost {cost | auto}`

Command mode: Interface Config

no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Format: `no spanning-tree cost`

Command mode: Interface Config

spanning-tree edgeport

This command specifies that an interface (or range of interfaces) is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format: `spanning-tree edgeport`

Command mode: Interface Config

no spanning-tree edgeport

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

Format: `no spanning-tree edgeport`

Command mode: Interface Config

spanning-tree forward-time

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

Default: 15

Format: `spanning-tree forward-time 4-30`

Command mode: Global Config

no spanning-tree forward-time

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

Format: `no spanning-tree forward-time`

Command mode: Global Config

spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface or range of interfaces. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default: none

Format: `spanning-tree guard {none | root | loop}`

Command mode: Interface Config

no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format: `no spanning-tree guard`

Command mode: Interface Config

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to 2 x (Bridge Forward Delay - 1).

Default: 20

Format: `spanning-tree max-age` *`6-40`*

Command mode: Global Config

no spanning-tree max-age

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

Format: `no spanning-tree` *`max-age`*

Command mode: Global Config

spanning-tree max-hops

This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 6 to 40.

Default: 20

Format: `spanning-tree max-hops` *`6-40`*

Command mode: Global Config

no spanning-tree max-hops

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

Format: `no spanning-tree max-hops`

Command mode: Global Config

spanning-tree mode

This command configures global spanning tree mode per VLAN spanning tree, Rapid-PVST+, MST, RSTP or STP. Only one of MSTP (RSTP), PVST+ or RPVST+ can be enabled on a switch.

When PVSTP+ or Rapid-PVSTP+ (RPVSTP+) is enabled, MSTP/RSTP/STP is operationally disabled. To switch to MSTP/RSTP/STP, disable PVSTP+/RPVSTP+. By default, MSTP enabled. In PVSTP+ or RPVSTP+ mode, BPDUs contain per-VLAN information instead of the common spanning-tree information (MST/RSTP).

PVSTP+ maintains independent spanning tree information about each configured VLAN. PVSTP+ uses IEEE 802.1Q trunking and allows a trunked VLAN to maintain blocked or forwarding state per port on a per-VLAN basis. This allows a trunk port to be forwarded on some VLANs and blocked on other VLANs.

RPVSTP+ is based on the IEEE 8012.1w standard. It supports fast convergence IEEE 802.1D. RPVSTP+ is compatible with IEEE 802.1D spanning tree. RPVSTP+ sends BPDUs on all ports, instead of only the root bridge sending BPDUs, and supports the discarding, learning, and forwarding states.

When the mode is changed to RPVSTP+, version 0 STP BPDUs are no longer transmitted and version 2 RPVSTP+ BPDUs that carry per-VLAN information are transmitted on the VLANs enabled for spanning-tree. If a version 0 BPDU is seen, RPVSTP+ reverts to sending version 0 BPDUs.

Rapid Per VLAN Spanning Tree Protocol Plus (RPVSTP+) embeds support for PVSTP+ FastBackbone and FastUplink. There is no provision to enable or disable these features in RPVSTP+.

Default: disabled

Format: `spanning-tree mode {mst | pvst | rapid-pvst | stp | rstp }`

Command mode: Global Config

no spanning-tree mode

This command globally configures the switch to the default spanning-tree mode, MSTP.

Format: `no spanning-tree mode { pvst | rapid-pvst }`

Command mode: Global Config

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an *mstid* parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *mstid*, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **port-priority** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. The **port-priority** value is a number in the range of 0 to 240 in increments of 16.

Default: cost—auto

port-priority—128

Format: `spanning-tree mst` *`mstid`* `{{cost` *`1-200000000`* `| auto} | port-priority` *`0-240`*`}`

Command mode: Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an

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

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value, i.e., a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value.

Format: `no spanning-tree mst mstid {cost | port-priority}`

Command mode: Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter mstid is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 32.

Default: none

Format: `spanning-tree mst instance mstid`

Command mode: Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format: `no spanning-tree mst instance mstid`

Command mode: Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The *mstid* parameter is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 4094.

If you specify 0 (defined as the default CIST ID) as the *mstid*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 4094. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default: 32768

Format: `spanning-tree mst priority mstid 0-4094`

Command mode: Global Config

To configure bridge priority in STP, RSTP mode, you should use the `spanning-tree mst priority` command for a zero MST instance (Example: `spanning-tree mst priority 0 <0-61440>`)

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The *mstid* parameter is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the *mstid*, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format: `no spanning-tree mst priority` *mstid*

Command mode: Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The *mstid* parameter is a multiple spanning tree instance identifier, in the range of 0 to 4094, that corresponds to the desired existing multiple spanning tree instance. The *vlanid* can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs in the range 1 to 4093, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). Spaces and zeros are not permitted. The VLAN IDs may or may not exist in the system.

Format: `spanning-tree mst vlan` *mstid vlanid*

Command mode: Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format: `no spanning-tree mst vlan` *mstid vlanid*

Command mode: Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled for use by spanning tree.

Default: enabled

Format: `spanning-tree port mode`

Command mode: Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled, disabling the port for use by spanning tree.

Format: `no spanning-tree port mode`

Command mode: Interface Config

spanning-tree port mode all

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

Default: enabled

Format: `spanning-tree port mode all`

Command mode: Global Config

no spanning-tree port mode all

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

Format: `no spanning-tree port mode all`

Command mode: Global Config

spanning-tree port-priority

Use this command to change the priority value of the port to allow the operator to select the relative importance of the port in the forwarding process. Set this value to a lower number to prefer a port for forwarding of frames.

All LAN ports have 128 as priority value by default. PVSTP+/RPVSTP+ puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.

The application uses the port priority value when the LAN port is configured as an edge port.

Default: enabled

Format: `spanning-tree port-priority` *`0-240`*

Command mode: Interface Config

spanning-tree tcnguard

Use this command to enable TCN guard on the interface. When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

Default: disabled

Format: `spanning-tree tcnguard`

Command mode: Interface Config

no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Format: `no spanning-tree tcnguard`

Command mode: Interface Config

spanning-tree transmit

This command sets the Bridge Transmit Hold Count parameter.

Default: 6

Format: `spanning-tree transmit hold-count`

Command mode: Global Config

Parameter	*Description*
hold-count	The Bridge Tx hold-count parameter. The value is an integer between 1 and 10.

spanning-tree uplinkfast

Use this command to configure the rate at which gratuitous frames are sent (in packets per second) after switchover to an alternate port on PVSTP+ configured switches and enables uplinkfast on PVSTP+ switches. The range is 0-32000; the default is 150. This command has the effect of accelerating spanning-tree convergence after switchover to an alternate port.

Uplinkfast can be configured even if the switch is configured for MST(RSTP) mode, but it only has an effect when the switch is configured for PVST+ mode. Enabling FastUplink increases the priority by 3000. Path costs less than 3000 have an additional 3000 added when uplinkfast is enabled. This reduces the probability that the switch will become the root switch.

Uplinkfast immediately changes to an alternate root port on detecting a root port failure and changes the new root port directly to the forwarding state. A TCN is sent for this event.

After a switchover to an alternate port (new root port), uplinkfast multicasts a gratuitous frame on the new root port on behalf of each attached machine so that the rest of the network knows to use the secondary link to reach that machine.

RPVSTP+ embeds support for backbonefast and uplinkfast. There is no provision to enable or disable these features in PVRSTP configured switches.

Default: 150

Format: `spanning-tree uplinkfast [max-update-rate` *`packets`*`]`

Command mode: Global Config

no spanning-tree uplinkfast

This command disables uplinkfast on PVSTP+ configured switches. All switch priorities and path costs that have not been modified from their default values are set to their default values.

Format: `no spanning-tree uplinkfast [max-update-rate]`

Command mode: Global Config

spanning-tree vlan

Use this command to enable/disable spanning tree on a VLAN.

Default: none

Format: `spanning-tree vlan` *`vlan-list`*

Command mode: Global Config

Parameter	*Description*
vlan list	The VLANs to which to apply this command.

spanning-tree vlan cost

Use this command to set the path cost for a port in a VLAN. The valid values are in the range of 1 to 200000000 or auto. If auto is selected, the path cost value is set based on the link speed.

Default: none

Format: `spanning-tree vlan vlan-id cost {auto |1-200000000}`

Command mode: Interface Config

spanning-tree vlan forward-time

Use this command to configure the spanning tree forward delay time for a VLAN or a set of VLANs. The default is 15 seconds.

Set this value to a lower number to accelerate the transition to forwarding. The network operator should take into account the end-to-end BPDU propagation delay, the maximum frame lifetime, the maximum transmission halt delay, and the message age overestimate values specific to their network when configuring this parameter.

Default: 15 seconds

Format: `spanning-tree vlan` *`vlan-list`* `forward-time` *`4-30`*

Command mode: Global Config

Parameter	*Description*
vlan list	The VLANs to which to apply this command.
forward-time	The spanning tree forward delay time. The range is 4-30 seconds.

spanning-tree vlan hello-time

Use this command to configure the spanning tree hello time for a specified VLAN or a range of VLANs. The default is 2 seconds. Set this value to a lower number to accelerate the discovery of topology changes.

Default: 2 seconds

Format: `spanning-tree vlan vlan-`*`list`* `hello-time` *`1-10`*

Command mode: Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.
hello-time	The spanning tree forward hello time. The range is 1-10 seconds.

spanning-tree vlan max-age

Use this command to configure the spanning tree maximum age time for a set of VLANs. The default is 20 seconds.

Set this value to a lower number to accelerate the discovery of topology changes. The network operator must take into account the end-to-end BPDU propagation delay and message age overestimate for their specific topology when configuring this value.

The default setting of 20 seconds is suitable for a network of diameter 7, lost message value of 3, transit delay of 1, hello interval of 2 seconds, overestimate per bridge of 1 second, and a BPDU delay of 1 second. For a network of diameter 4, a setting of 16 seconds is appropriate if all other timers remain at their default values.

Default: 20 seconds

Format: `spanning-tree vlan vlan-list max-age 6-40`

Command mode: Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.
hello-time	The spanning tree forward hello time. The range is 1-10 seconds.

spanning-tree vlan root

Use this command to configure the switch to become the root bridge or standby root bridge by modifying the bridge priority from the default value of 32768 to a lower value calculated to ensure the bridge is the root (or standby) bridge.

The logic takes care of setting the bridge priority to the lowest value (for primary bridge) or next (for redundant bridge) bridge priority value for the specified VLAN or a range of VLANs.

Default: 32768

Format: `spanning-tree vlan vlan-list root {primary|secondary}`

Command mode: Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.

spanning-tree vlan port-priority

Use this command to change the VLAN port priority value of the VLAN port to allow the operator to select the relative importance of the VLAN port in the forwarding selection process when the port is configured as a point- to-point link type. Set this value to a lower number to prefer a port for forwarding of frames.

Default: none

Format: `spanning-tree vlan vlan-id port-priority priority`

Command mode: Interface Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.
priority	The VLAN port priority. Range of values: 0-255.

spanning-tree vlan priority

Use this command to configure the bridge priority of a VLAN. The default value is 32768.

If the value configured is not among the specified values, it will be rounded off to the nearest valid value.

Default: 32768

Format: `spanning-tree vlan` *`vlan-list`* `priority` *`priority`*

Command mode: Global Config

Parameter	*Description*
vlan-list	The VLANs to which to apply this command.
priority	The VLAN bridge priority. Valid values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440.

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format: `show spanning-tree`

Command mode: Privileged
User

Parameter	*Description*
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CIST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifer	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change in Progress	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CIST
Bridge Max Age	Derived value.
Bridge Max Hops	Timer of a maximum number of bridge hops for a device.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CIST.
Bridge Hold Time	Minimum time between transmission of configuration Bridge Protocol Data Units (BPDU).
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CIST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

show spanning-tree active

Use this command to display the spanning tree values on active ports for the modes (xSTP and PV(R)STP).

Format: show spanning-tree active

Command mode: Privileged
User

show spanning-tree backbonefast

This command displays spanning tree information for backbonefast.

Format: `show spanning-tree backbonefast`

Command mode: Privileged
User

Parameter	*Description*
Transitions via Backbonefast	The number of backbonefast transitions.
Inferior BPDUs received (all VLANs)	The number of inferior BPDUs received on all VLANs.
RLQ request PDUs received (all VLANs)	The number of Root Link Query (RLQ) requests PDUs received on all VLANs.
RLQ response PDUs received (all VLANs)	The number of RLQ response PDUs received on all VLANs.
RLQ request PDUs sent (all VLANs)	The number of RLQ request PDUs sent on all VLANs.
RLQ response PDUs sent (all VLANs)	The number of RLQ response PDUs sent on all VLANs.

show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format: `show spanning-tree brief`

Command mode: Privileged
User

Parameter	*Description*
Bridge Priority	Configured value.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Timer of a maximum number of bridge hops for a device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of configuration Bridge Protocol Data Units (BPDU).

show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *unit/slot/port* is the desired switch port. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number. The following details are displayed on execution of the command.

Format: `show spanning-tree interface` *unit/slot/port*|`lag` *lag-intf-num*

Command mode: Privileged
User

Parameter	*Description*
Hello Time	Admin hello time for this port.
Port Mode	Enable or disable.
BPDU Guard Effect	Enable or disable.
Root Guard	Enable or disable.
Loop Guard	Enable or disable.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enable or disable.
BPDU Flood Mode	Enable or disable.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for **edge delay** time, to become an edge port and transition to forwarding faster.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

show spanning-tree mst detailed

This command displays the detailed settings for an MST instance.

Format: `show spanning-tree mst detailed` *mstid*

Command mode: Privileged
User

Parameter	*Description*
mstid	A multiple spanning tree instance identifier. Range of values: from 0 to 4094.

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The *mstid* parameter is a number that corresponds to the desired existing multiple spanning tree instance. The *unit/slot/port* is the desired switch port. Instead of *unit/slot/port*, lag lag-intf-num can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `show spanning-tree mst port detailed` *`mstid unit/slot/port`*|`lag` *`lag-intf-num`*

Command mode: Privileged
User

Parameter	*Description*
MST Instance ID	The ID of the existing multiple spanning tree (MST) instance identifier. Range of values: from 0 to 4094.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. 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 this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

If you specify 0 (defined as the default CIST ID) as the *mstid*, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *unit/slot/port* is the desired switch port. In this case, the following are displayed.

Parameter	*Description*
Port Identifier	The port identifier for this port within the CIST.
Port Priority	The priority of the port within the CIST.
Port Forwarding State	The forwarding state of the port within the CIST.
Port Role	The role of the specified interface within the CIST.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgment	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. 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 this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *mstid* indicates a particular MST instance. The parameter *{unit/slot/port|all}* indicates the desired switch port or all ports. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an

alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

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

Format: `show spanning-tree mst port summary` *mstid {unit/slot/port* |`lag` *lag-intf-num*| `all}`

Command mode: Privileged

User

Parameter	*Description*
MST Instance ID	The MST instance associated with this port.
Interface	The interface in unit/slot/port format.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format: `show spanning-tree mst port summary` *mstid* `active`

Command mode: Privileged

User

Parameter	*Description*
MST Instance ID	The MST instance associated with this port.
Interface	The interface in unit/slot/port format.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format: `show spanning-tree mst summary`

Command mode: Privileged
User

Parameter	*Description*
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: • Associated FIDs • Associated VLANs	• List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format: `show spanning-tree summary`

Command mode: Privileged
User

Parameter	*Description*
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version (FPV) parameter.
BPDU Guard Mode	Enable or disable.
BPDU Filter Mode	Enable or disable.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

show spanning-tree uplinkfast

This command displays spanning tree information for uplinkfast.

Format: `show spanning-tree uplinkfast`

Command mode: Privileged
User

Parameter	*Description*
Uplinkfast transitions (all VLANs)	List of multiple spanning trees IDs currently configured.
Proxy multicast addresses transmitted (all VLANs)	The number of proxy multicast addresses transmitted on all VLANs.

show spanning-tree vlan

This command displays spanning tree information per VLAN and also lists out the port roles and states along with port cost. The *vlan-list* parameter is a list of VLANs or VLAN-ranges separated by commas and with no embedded blank spaces. VLAN ranges are of the form “X-Y” where X and Y are valid VLAN identifiers and X<Y.

The *vlanid* corresponds to an existing VLAN ID.

Format: `show spanning-tree vlan {vlanid | vlan-list}`

Command mode: Privileged
User

spanning-tree mac-address dot1d

This command sets the processing mode of the Bridge PDU based on their destination MAC address and allows you to use STP with bridges operating under the 802.1ad standard (Provider Bridges). Changes the MAC address from which BPDUs are sent and received to 01-80-C2-00-00-00. Inbound BPDU with an address inconsistent with the mode are discarded.

Default: Enabled

Format `spanning-tree mac-address dot1d`

Command Mode: Interface Config

no spanning-tree mac-address

This command disables the Bridge PDU processing mode based on their destination MAC address.

Format `no spanning-tree mac-address`

Command Mode Interface Config

spanning-tree mac-address dot1ad

This command changes the MAC address from which BPDUs are sent and received to 01-80-C2-00-00-08. In the dot1ad mode, frames are processed and transmitted from the Provider Bridge Group Address. Inbound BPDU with an address inconsistent with the mode are discarded.

Default: Disabled

Format `spanning-tree mac-address dot1ad`

Command Mode: Interface Config

no spanning-tree mac-address

This command disables the Bridge PDU processing mode based on their destination MAC address.

Format `no spanning-tree mac-address`

Command Mode Interface Config

spanning-tree mac-address auto

This command changes the MAC address with which BPDUs are received on 01-80-C2-00-00-08; on others it changes the MAC address to 01-80-C2-00-00-00.

Default: Disabled

Format `spanning-tree mac-address auto`

Command Mode: Interface Config

no spanning-tree mac-address

This command disables the Bridge PDU processing mode based on their destination MAC address.

Format `no spanning-tree mac-address`

Command Mode Interface Config

9.3 Loop Protection configuration commands

This section describes the commands used to configure loop protection. Loop protection detects physical and logical loops between Ethernet ports on a device. Loop protection must be enabled globally before it can be enabled at the interface level.

keepalive (Global Config)

This command enables loop protection for the system.

Default: disabled

Format: `keepalive`

Command mode: Global Config

no keepalive

This command disables loop protection for the system. This command also sets the transmit interval and retry count to the default value.

Format: `no keepalive`

Command mode: Global Config

keepalive (Interface Config)

This command enables keepalive on a particular interface.

Default: none

Format: `keepalive`

Command mode: Interface Config

no keepalive

This command disables keepalive on a particular interface.

Format: `keepalive`

Command mode: Interface Config

keepalive action

This command configures the action to be taken on a port when a loop is detected.

Default: Disabled.

Format: `keepalive receive-action {log|disable|both}`

Command mode: Interface Config

Parameter	*Description*
log	Only logs the message. The log mode only logs the message to buffer logs without bringing the port down.
disable	Shuts down the port. This is the default.
both	Logs and disables the port.

no keepalive action

This command returns the command to the default action of disabling a port when a loop is detected.

Format: `no keepalive action`

Command mode: Interface Config

keepalive disable-timer

This command configures the time, in seconds, for which a port is down if a loop is detected. The default time is 0 so that port needs to be re-enabled manually to bring it up.

Default: 0

Format: `keep-alive disable-timer` *value*

Command mode: Global Config

Parameter	***Description***
log	Only logs the message. The log mode only logs the message to buffer logs without bringing the port down.
disable	Shuts down the port. This is the default.
both	Logs and disables the port.

no keepalive action

This command returns the command to the default action of disabling a port when a loop is detected.

Format: `no keepalive action`

Command mode: Interface Config

keepalive disable-timer

This command configures the time, in seconds, for which a port is down if a loop is detected. The default time is 0 so that port needs to be re-enabled manually to bring it up.

Default: 0

Format: `keep-alive disable-timer` *value*

Command mode: Global Config

keepalive retry

This command configures the time in seconds between transmission of keep-alive packets. Retry is an optional parameter that configures the count of keepalive packets received by the switch after which the interface will be error disabled.

Default: 5

Format: `keepalive val [retry]`

Command mode: Global Config

Parameter	***Description***
val	The time in seconds between transmission of keep-alive packets.

retry	Configures the count of keepalive packets received by the switch after which the switch will be error disabled.

show keepalive

This command displays the global keepalive configuration.

Default: none

Format: `show keepalive`

Command mode: Privileged

show keepalive statistics

This command displays the keepalive statistics for each port or a specific port.

Default: none

Format: `show keepalive statistics {`*`port-num`* `| all }`

Command mode: Privileged

Parameter	***Description***
port-num	The port number for which to show statistics.
all	Show statistics for all ports.

clear counters keepalive

This command clears keepalive statistics associated with ports (for example, number of transmitted packets, received packets, and loop packets).

Default: none

Format: `clear counters keepalive`

Command mode: Privileged

9.4 VLAN configuration commands

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

vlan database

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

Format: `vlan database`

Command mode: Privileged

network mgmt_vlan

This command configures the Management VLAN ID.

Default: 1

Format: `network mgmt_vlan` *`1-4093`*

Command mode: Privileged

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format: `no network mgmt_vlan`

Command mode: Privileged

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4093.

Format: `vlan` *`2-4094`*

Command mode: VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4093.

Format: `no vlan` *`2-4094`*

Command mode: VLAN Config

vlan acceptframe

This command sets the frame acceptance mode on an interface or range of interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. For admituntaggedonly mode, only untagged frames are accepted on this interface; tagged frames are discarded. With any option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default: all

Format: `vlan acceptframe {admituntaggedonly | vlanonly | all}`

Command mode: Interface Config

no vlan acceptframe

This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format: `no vlan acceptframe`

Command mode: Interface Config

vlan ingressfilter

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

Default: disabled

Format: `vlan ingressfilter`

Command mode: Interface Config

no vlan ingressfilter

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

Format: `no vlan ingressfilter`

Command mode: Interface Config

vlan internal allocation

Use this command to configure which VLAN IDs to use for port-based routing interfaces. When a port-based routing interface is created, an unused VLAN ID is assigned internally.

Format: `vlan internal allocation {base` *`vlan-id`* `| policy ascending | policy decending}`

Command mode: Global Config

Parameter	*Description*
base vlan-id	The first VLAN ID to be assigned to a port-based routing interface.
policy ascending	VLAN IDs assigned to port-based routing interfaces start at the base and increase in value.
policy descending	VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value.

vlan makestatic

This command changes a dynamically created VLAN (created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Format: `vlan makestatic` *`2-4094`*

Command mode: VLAN Config

vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4093.

Default: VLAN ID 1 — default
other VLANS — blank string

Format: `vlan name` *`1-4094 name`*

Command mode: VLAN Config

no vlan name

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

Format: `no vlan name` *`1-4094`*

Command mode: VLAN Config

vlan participation

This command configures the degree of participation for a specific interface or range of interfaces in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format: `vlan participation {exclude | include | auto} 1-4094`

Command mode: Interface Config

Participation options are:

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

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format: `vlan participation all {exclude | include | auto} 1-4094`

Command mode: Global Config

You can use the following participation options:

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

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default: all

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

Command mode: Global Config

The modes are defined as follows:

Mode	*Value*
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.
Admit Untagged Only mode	VLAN-tagged and priority tagged frames received on this interface are discarded.

Admit All mode	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format: `no vlan port acceptframe all`

Command mode: Global Config

vlan port ingressfilter all

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

Default: disabled

Format: vlan port ingressfilter all

Command mode: Global Config

no vlan port ingressfilter all

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

Format: `no vlan port ingressfilter all`

Command mode: Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default: 1

Format: `vlan port pvid all` *`1-4094`*

Command mode: Global Config

no vlan port pvid all

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

Format: `no vlan port pvid all`

Command mode: Global Config

vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format: `vlan port tagging all 1-4094`

Command mode: Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format: `no vlan port tagging all`

Command mode: Global Config

vlan protocol group

This command adds protocol-based VLAN groups to the system. The groupid is a unique number from 1–128 that is used to identify the group in subsequent commands.

Format: `vlan protocol group groupid`

Command mode: Global Config

vlan protocol group name

This command assigns a name to a protocol-based VLAN groups. The *groupname* variable can be a character string of 0 to 16 characters.

Format: `vlan protocol group name groupid groupname`

Command mode: Global Config

no vlan protocol group name

This command removes the name from the group identified by *groupid*.

Format: `no vlan protocol group name groupid`

Command mode: Global Config

vlan protocol group add protocol

This command adds the *protocol-list* to the protocol-based VLAN identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for *protocol-list* includes the keywords *ip*, *arp*, and *ipx* and hexadecimal or decimal values ranging from 0x0600 (1536) to 0xFFFF (65535). The protocol list can accept up to 16 protocols separated by a comma.

Default: none

Format: `vlan protocol group add protocol groupid ethertype protocol-list`

Command mode: Global Config

no vlan protocol group add protocol

This command removes the protocols specified in the *protocol-list* from this protocol-based VLAN group that is identified by this *groupid*.

Format: `no vlan protocol group add protocol groupid ethertype protocol-list`

Command mode: Global Config

protocol group

This command attaches a *vlanid* to the protocol-based VLAN identified by *groupid*. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Default: none

Format: `protocol group groupid vlanid`

Command mode: VLAN Config

no protocol group

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

Format: `no protocol group groupid vlanid`

Command mode: VLAN Config

protocol vlan group

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

Default: none

Format: `protocol vlan group groupid`

Command mode: Interface Config

no protocol vlan group

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

Format: `no protocol vlan group groupid`

Command mode: Interface Config

protocol vlan group all

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

Default: none

Format: `protocol vlan group all groupid`

Command mode: Global Config

no protocol vlan group all

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

Format: `no protocol vlan group all` *groupid*

Command mode: Global Config

show port protocol

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

Format: `show port protocol {`*groupid* `| all}`

Command mode: Privileged

Term	*Description*
Group Name	The group name of an entry in the Protocol-based VLAN table.
Group ID	The group identifier of the protocol group.
VLAN	The VLAN associated with this Protocol Group.
Protocol(s)	The type of protocol(s) for this group.
Interface(s)	Lists the unit/slot/port interface(s) that are associated with this Protocol Group.

vlan pvid

This command changes the VLAN ID on an interface or range of interfaces.

Default: 1

Format: `vlan pvid` *1-4094*

Command mode: **I**nterface config

interface range config

no vlan pvid

This command sets the VLAN ID on an interface or range of interfaces to 1.

Format: `no vlan pvid`

Command mode: Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format: `vlan tagging` *1-4094*

Command mode: Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format: `no vlan tagging 1-4094`

Command mode: Interface Config

vlan association subnet

This command associates a VLAN to a specific IP-subnet.

Format: `vlan association subnet ipaddr netmask vlanid`

Command mode: VLAN Config

no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format: `no vlan association subnet ipaddr netmask`

Command mode: VLAN Config

vlan association mac

This command associates a MAC address to a VLAN.

Format: `vlan association mac macaddr vlanid`

Command mode: VLAN database

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format: `no vlan association mac macaddr`

Command mode: VLAN table

remote-span

This command identifies the VLAN as the RSPAN VLAN and disables mac address learning for that VLAN interface.

Default: none

Format: `remote-span`

Command mode: VLAN Config

Maximum RSPAN VLAN number is 7.

no remote-span

This command clears RSPAN information for the VLAN and enables mac address learning for that VLAN interface.

Format: `no remote-span`

Command mode: VLAN Config

show vlan

This command displays information about the configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and the ports which belong to a private VLAN.

Format: `show vlan {`*`vlanid`*`|private-vlan [`*`type`*`]}`

Command mode: Privileged
User

Term	*Value*
Primary	Primary VLAN identifier. The range of the VLAN identifier: 1–40934094.
Secondary	Secondary VLAN identifier.
Type	Secondary VLAN type (community, isolated, or primary).
Ports	Ports which are associated with a private VLAN.
VLAN ID	The VLAN identifier (VID) associated with each VLAN. The range of the VLAN identifier: 1–4094.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. Default: blank. VLAN ID 1 always has a name of **Default**. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) if a RADIUS-assigned VLAN does not exist on the switch.
Interface	The interface in *unit/slot/port* format. It is possible to set the parameters for all ports by using the selectors on the top line.
Current	The degree of participation of this port in this VLAN. The permissible values are: **Include** — This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. **Exclude** — This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. **Autodetect** — To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Configured	The configured degree of participation of this port in this VLAN. The permissible values are: **Include** — This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. **Exclude** — This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. **Autodetect** — To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. **Tagged** — Transmit traffic for this VLAN as tagged frames. **Untagged** — Transmit traffic for this VLAN as untagged frames.

show vlan tag

This command displays configuration for one VLAN in short format.

Format: `show vlan tag`

Command mode: Privileged
User

show vlan internal usage

This command displays information about the VLAN ID allocation on the switch.

Format: `show vlan internal usage`
Command mode: Privileged
User

Term	*Description*
Base VLAN ID	Identifies the base VLAN ID for Internal allocation of VLANs to the routing interface.
Allocation policy	Identifies whether the system allocates VLAN IDs in ascending or descending order.

show vlan brief

This command displays a list of all configured VLANs.

Format: show vlan brief

Command mode: Privileged
User

Term	*Description*
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN identifier: 1–4094.

VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. Default: blank. VLAN ID 1 always has a name of “Default”. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format: `show vlan port {`*`unit/slot/port`*` | all}`

Command mode: Privileged
User

Term	*Value*
Interface	*unit/slot/port*. It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID Configured	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. Default: 1.
Port VLAN ID Current	The current VLAN ID that this port assigns to untagged frames or priority tagged frames received on this port. Default: 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering Configured	Possible values are: enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
Ingress Filtering Current	Shows the current ingress filtering configuration.
GVRP	Possible values are: enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.
Protected Port	Specifies if this is a protected port. If False, it is not a protected port; If true, it is.
Switchport mode	The current switchport mode for the port.
Operating parameters	The operating parameters for the port, including the VLAN, name, egress rule, and type.

Static configuration	The static configuration for the port, including the VLAN, name, and egress rule.
Forbidden VLANs	The forbidden VLAN configuration for the port, including the VLAN and name.

show vlan association subnet

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Format: `show vlan association subnet [ipaddr netmask]`

Command mode: Privileged

Term	*Description*
IP Address	The IP address assigned to each interface.
Net Mask	The subnet mask.
VLAN ID	VLAN identifier (VID).

show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format: `show vlan association mac [macaddr]`

Command mode: Privileged

Term	*Description*
MAC Address	A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
VLAN ID	VLAN identifier (VID).

9.5 Double VLAN configuration commands

This section describes the commands you use to configure double VLAN (DVLAN). Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own IEEE 802.1Q domain.

dvlan-tunnel ethertype (Interface Config mode)

This command is not available on all platforms.

This command configures the ethertype for the specified interface. The two-byte hex ethertype is used as the first 16 bits of the DVLAN tag. The ethertype may have the values of *802.1Q*, *vman*, or *custom*. If the ethertype has an optional value of custom, then it is a custom tunnel value, and ethertype must be set to a value in the range of 1 to 65535.

Default: 802.1Q

Format: `dvlan-tunnel ethertype {802.1Q | vman | custom 1-65535}`

Command mode: Global Config

Term	*Description*
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 1to 65535.
vman	Represents the commonly used value of 0x88A8.

no dvlan-tunnel ethertype (Interface Config mode)

This command is not available on all platforms. This command removes the ethertype value for the interface.

Format: `no dvlan-tunnel ethertype`

Command mode: Global Config

dvlan-tunnel ethertype primary-tpid

Use this command to create a new TPID and associate it with the next available TPID register. If no TPID registers are empty, the system returns an error to the user. Specifying the optional keyword [primary–tpid] forces the TPID value to be configured as the default TPID at index 0.

Format: `dvlan-tunnel ethertype {802.1Q | vman | custom 1–65535} [primary-tpid]`

Command mode: Global Config

Term	*Description*
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 1to 65535.
vman	Represents the commonly used value of 0x88A8.

no dvlan-tunnel ethertype primary–tpid

Use the no form of the command to reset the TPID register to 0. (At initialization, all TPID registers will be set to their default values.)

Format: `no dvlan-tunnel ethertype {802.1Q | vman | custom 1–65535} [primary-tpid]`

Command mode: Global Config

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Default: disabled

Format: `mode dot1q-tunnel`

Command mode: Interface Config

no mode dot1q-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format: `no mode dot1q-tunnel`

Command mode: Interface Config

mode dvlan-tunnel

Use this command to enable Double VLAN Tunneling on the specified interface.

When you use the mode dvlan-tunnel command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

Default: disabled

Format: `mode dvlan-tunnel`

Command mode: Interface Config

no mode dvlan-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format: `no mode dvlan-tunnel`

Command mode: Interface Config

show dot1q-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format: `show dot1q-tunnel [interface {`*`unit/slot/port`*` | all}]`

Command mode: Privileged
User

Term	*Value*
Interface	The interface in unit/slot/port format
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 1 to 65535.

9.6 Private VLAN configuration commands

This section describes the commands you use for private VLANs. Private VLANs provides Layer 2 isolation between ports that share the same broadcast domain. In other words, it allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network.

switchport private-vlan

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Format: `switchport private-vlan {host-association primary-vlan-id secondary-vlan-id | mapping primary-vlan-id {add | remove} secondary-vlan-list}`

Command mode: Interface Config

Term	*Value*
host-association	Defines the VLAN association for community or host ports.
mapping	Defines the private VLAN mapping for promiscuous ports.
primary-vlan-id	Primary VLAN ID of a private VLAN.
secondary-vlan-id	Secondary (isolated or community) VLAN ID of a private VLAN.
add	Associates the secondary VLAN with the primary one.
remove	Deletes the secondary VLANs from the primary VLAN association.
secondary-vlan- list	A list of secondary VLANs to be mapped to a primary VLAN.

no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format: `no switchport private-vlan {host-association|mapping}`

Command mode: Interface Config

switchport mode private-vlan

This command configures a port as a promiscuous or host private VLAN port. Note that the properties of each mode can be configured even when the switch is not in that mode. However, they will only be applicable once the switch is in that particular mode.

Default: general

Format: `switchport mode private-vlan {host|promiscuous}`

Command mode: Interface Config

Term	*Value*
host	Configures an interface as a private VLAN host port. It can be either isolated or community port depending on the secondary VLAN it is associated with.
promiscuous	Configures an interface as a private VLAN promiscuous port. The promiscuous ports are members of the primary VLAN.

no switchport mode private-vlan

This command removes the private-VLAN association or mapping from the port.

Format: `no switchport mode private-vlan`

Command mode: Interface Config

private-vlan

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format: `private-vlan {association [add|remove] secondary-vlan-list|community|isolated|primary}`

Command mode: VLAN Config

Parameter	*Description*
association	Associates the primary and secondary VLAN.
secondary-vlan-list	A list of secondary VLANs to be mapped to a primary VLAN.
community	Designates a VLAN as a community VLAN.
isolated	Designates a VLAN as the isolated VLAN.
primary	Designates a VLAN as the primary VLAN.

no private-vlan

This command restores normal VLAN configuration.

Format: `no private-vlan {association}`

Command mode: VLAN Config

9.7 Switch Ports configuration

This section describes the commands used for switch port mode.

switchport mode

Use this command to configure the mode of a switch port as access, trunk or general.

In Trunk mode, the port becomes a member of all VLANs on switch unless specified in the allowed list in the *switchport trunk allowed vlan* command. The PVID of the port is set to the Native VLAN as specified in the switchport trunk native vlan command. It means that trunk ports accept both tagged and

untagged packets, where untagged packets are processed on the native VLAN and tagged packets are processed on the VLAN ID contained in the packet. MAC learning is performed on both tagged and untagged packets. Tagged packets received with a VLAN ID to which the port is not a member are discarded and MAC learning is not performed. The Trunk ports always transmit packets untagged on native VLAN.

In Access mode, the port becomes a member of only one VLAN. The port sends and receives untagged traffic. It can also receive tagged traffic. The ingress filtering is enabled on port. It means that when the VLAN ID of received packet is not identical to Access VLAN ID, the packet is discarded.

In General mode, the user can perform custom configuration of VLAN membership, PVID, tagging, ingress filtering etc. This is legacy behavior of switch port configuration. Legacy CLI commands are used to configure port in general mode.

Default: General mode

Format: `switchport mode {access | trunk | general}`

Command mode: Interface Config

no switchport mode

This command resets the switch port mode to its default value.

Format: `no switchport mode`

Command mode: Interface Config

switchport trunk allowed vlan

Use this command to configure the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. Default: all VLANs.

The VLANs list can be modified using the add or remove options or replaced with another list using the vlan-list, all, or except options. If all is chosen, all VLANs are added to the list of allowed vlan. The except option provides an exclusion list.

Trunk ports accept tagged packets, where tagged packets are processed on the VLAN ID contained in the packet, if this VLAN is in the allowed VLAN list. Tagged packets received with a VLAN ID to which the port is not a member are discarded and MAC learning is not performed. If a VLAN is added to the system after a port is set to the Trunk mode and it is in the allowed VLAN list, this VLAN is assigned to this port automatically.

Default: All

Format: `switchport trunk allowed vlan {`*`vlan-list`*` | all | {add `*`vlan-list`*`} | {remove `*`vlan-list`*`}| {except `*`vlan-list`*` }}`

Command mode: Interface Config

Parameter	***Description***
all	Specifies all VLANs from 1 to 4093. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
add	Adds the defined list of VLANs to those currently set instead of replacing the list.
remove	Removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to

	4093; extended-range VLAN IDs of the form X- Y or X,Y,Z are valid in this command.
except	Lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)
vlan-list	Either a single VLAN number from 1 to 4093 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

no switchport trunk allowed vlan

This command resets the list of allowed VLANs on the trunk port to its default value.

Format: `no switchport trunk allowed vlan`

Command mode: Interface Config

switchport trunk native vlan

Use this command to configure the Trunk port Native VLAN (PVID) parameter. Any ingress untagged packets on the port are tagged with the value of Native VLAN. Native VLAN must be in the allowed VLAN list for tagging of received untagged packets. Otherwise, untagged packets are discarded. Packets marked with Native VLAN are transmitted untagged from Trunk port. Default: 1.

Default: 1 (Default VLAN)

Format: `switchport trunk native vlan` *`vlan-id`*

Command mode: Interface Config

no switchport trunk native vlan

Use this command to reset the switch port trunk mode native VLAN to its default value.

Format: `no switchport trunk native vlan`

Command mode: Interface Config

switchport access vlan

Use this command to configure the VLAN on the Access port. Only one VLAN can be assigned to the Access port. Access ports are members of VLAN 1 by default. Access ports may be assigned to a VLAN other than VLAN 1. Removing the Access VLAN on the switch makes the Access port a member of VLAN 1. Configuring an Access port to be a member of a VLAN that does not exist results in an error and does not change the configuration.

Default: 1 (Default VLAN)

Format: `switchport access vlan` *`vlan-id`*

Command mode: Interface Config

no switchport access vlan

This command resets the switch port access mode VALN to its default value.

Format: `no switchport access vlan`

Command mode: Interface Config

show interfaces switchport

Use this command to display the switchport status for all interfaces or a specified interface.

Format: `show interfaces switchport` *unit/slot/port*

Command mode: Privileged

show interfaces switchport

Use this command to display the Switchport configuration for a selected mode per interface. If the interface is not specified, the configuration for all interfaces is displayed.

Format: `show interfaces switchport {access | trunk | general}` [*unit/slot/port*]

Command mode: Privileged

9.8 Voice VLAN Configuration Commands

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default: disabled

Format: `voice vlan`

Command mode: Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format: `no voice vlan`

Command mode: Global Config

voice vlan (Interface Config mode)

Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

Default: disabled

Format: `voice vlan {vlanid` *id* `| dot1p` *priority* `| none | untagged}`

Command mode: Interface Config

You can configure Voice VLAN in one of four different ways:

Parameter	*Description*
vlan-id	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4093 (the max supported by the platform).
dot1p	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid priority range is 0 to 7.
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format: `no voice vlan`

Command mode: Interface Config

voice vlan data priority

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN interface or range of interfaces being configured.

Default: trust

Format: `voice vlan data priority {untrust | trust}`

Command mode: Interface Config

show voice vlan

Format: `show voice vlan [interface {unit/slot/port | all}]`

Command mode: Privileged

When the *interface* parameter is not specified, only the global mode of the Voice VLAN is displayed.

Parameter	*Description*
Administrative Mode	The Global Voice VLAN mode.

When the *interface* is specified:

Parameter	*Description*
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN identifier
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

9.9 Provider Bridge configuration commands[1]

Provider bridge commands configure the switch to use IEEE802.1ad stacked VLANs. Service providers use stacked VLANs — in which 801.Q VLAN tags are encapsulated in a second layer of 802.1Q tags (802.1Q-in- Q) — to enable a single VLAN to support customers who have multiple internal VLANs.

Provider bridge commands include data tunneling commands and L2 protocol tunneling commands.

- "Data Tunneling Configuration Commands" define service instances and apply them to specific ports.
- "L2 Protocol Tunneling Configuration Commands" enable using Layer 2 protocols across customer networks at different sites that are connected through a service provider network.

9.9.1 Data Tunneling configuration commands

To enable a VLAN on the switch to be bridged throughout the service provider network, you define service instances. A service instance definition includes the service name, the type of forwarding to use, and QoS information. A service instance is also associated with a unique service VLAN (or *SVLAN*), which is identified by the service VLAN ID (or *S-VID*).

The administrator can subscribe individual ports to a service. When a port subscribes to a service, a VLAN is created on the switch (if it does not already exist) and the subscribing port is configured as a participant in the SVLAN. The service provider port (called the Network-to-Network, or NNI, port) is also configured as a participant in the SVLAN in order to transmit and receive upstream/downstream traffic.

A subscription includes match criteria such as the customer VLAN ID, such as C-VID, priority, S-VID. When an incoming packet on UNI-P matches the subscription criteria on the port, the switch adds the service VLAN tag to the packet and, optionally, re-marks the C-VID/removes the C-tag before forwarding/redirecting to the service provider network. When an incoming packet on UNI-S matches the subscription criteria on the port, the switch may remark S-VID and/or remarks C-VID/removes C-tag to the packet before forwarding/redirecting to the service provider network. CLI supports up to 4K service subscriptions per switch/port.

When a TLS service is subscribed on a port, then the port's P-VID is set to be the S-VID of the TLS service. The P-VID of the NNI port is set to the Management VLAN. The default management VLAN is 1. Creation and participation behavior of VLANs on the switch is the same for all types of services (TLS, E-LAN, E-Tree, E- Line) of services.

VLANs and participation of ports (customer and service provider ports) is configured automatically based on service and subscription configuration. It is recommended that administrators do not create or change VLANs and port VLAN participations on any ports. Manual configuration of VLANs and port participations may result in undefined behavior.

dot1ad mode

This command enables UNI/NNI mode and sets the dot1ad type for an interface or range of interfaces. UNI–P is for a port-based service interface and UNI–S is for a service-based interface. A match based on S–VID/C– VID and C–VID/Priority can be configured on an UNI–S port. A UNI–P port may be

[1]This functionality is available with an OSPF license. To activate the license, please contact the technical support.

configured with C–VID/ Priority/Untagged-based match criteria. Dot1ad services cannot be subscribed on a switch port. When mode is set to switchport, the port can be used for normal switching/routing traffic.

Default: none

Format: `dot1ad mode {uni-p | uni-s | nni | switchport}`

Command mode: Interface Config

Example:

The following shows an example of the command.

```
(Switch)(Config)(interface 1/0/6)#dot1ad mode nni
```

dot1ad service

This command configures a service of a given type by name. This command allows configuration of the S–VID and NNI port association at the service level.

Format: `dot1ad service` *`service-name`* `svid` *`svid`* `{e–lan | e-line | e–tree | tls} [nni` *`port list`*`]`

Command mode: Global Config

Parameter	*Description*
service-name	The user-assigned service name.
svid	The service VLAN ID (S-VID).
e-lan | e-line | e- tree | tls	These parameters define the type of traffic associated with the service instance. • **e-lan** — A switched or general service is one in which the traffic associated with that service is forwarded based on a standard L2 switching lookup using the S-VID and destination MAC as lookups in the FDB. **A port can be a member of multiple E-LAN services. If a switched service is assigned to multiple UNI ports, those ports will be able to forward traffic to each other as well as to the NNI ports. The same E-LAN service can also be applied on UNI-P and UNI-S ports.** • **e-line** — The e-line parameter creates a point-to-point service, in which traffic is forwarded directly to the NNI port in the upstream direction and to the associated UNI port in the downstream direction. An e-line service bypasses the standard VLAN/ MAC-based switching decisions, including the source MAC learning. Be default, system does not learn traffic belonging to the e-line service. An e-line service- instance defines a point-to-point service in which only one UNI-P or UNI-S port participates. **Note.** It is important to note that downstream broadcast and multicast traffic will still be redirected to the associated UNI port participating in the e-line service. • **e-tree** — The e-tree parameter creates a point-to-multipoint service in which the traffic associated with that service is forwarded directly to the NNI port in the upstream direction and direct to the associated UNI port(s) in the downstream direction. If an e-tree service instance is applied to multiple UNI ports, it becomes a

	point-to-multipoint service in which the participating user ports are still isolated from each other. **Note.** It is important to note that downstream broadcast, multicast, and unknown destination (DLF) traffic will still be forwarded (replicated) to all ports participating in the e-tree service. • **tls (Transparent LAN Service).** Administrators can configure a TLS on UNI-P and UNIS ports. A Transparent LAN service is used to connect the remote sites of a customer with C-Tag transparency. There are no match criteria for a TLS. – If no TLS service is configured on an UNI-P port, all packets not matching any of the service instances configured on the ports will be dropped. If a TLS service is configured, then all packets not matching the other service instances on that port will be tagged as per the TLS definition on that port. TLS service defined by the user will be used by Untagged, Priority Tagged, and C-VLAN tagged packets which do not match any other service instances on the port. – If a TLS service is configured on an UNI-S port, service VLAN tagged (including double tagged) frames that do not match other service instances on the port will be forwarded to appropriate NNI port(s) based on the S-VID associated with the service without any VLAN modification. Untagged and priority tagged packets that do not match other service instances on the port wil be dropped.
port-list	NNI port list.

no dot1ad service

Use the no form of the command to delete a service.

Format: `no dot1ad service` *`service-name`*

Command mode: Global Config

subscribe match untagged–pkt

Use this command to configure the match VLAN assignment for untagged packets (UNI–P ports only) on an interface or range of interfaces. Upstream traffic goes to configured NNI ports based on a switching or redirection action, depending upon the service subscribed for.

Format: `subscribe` *`service-name subscription-name`* `match untagged–pkt [assign–cvid` *`cvid`*`] [nni` *`port-list`*`]`

Command mode: Interface Config

no subscribe match untagged–pkt

Use the no form of the command to unsubscribe the untagged packets.

Format: `no subscribe` *`service-name subscription-name`* `match untagged–pkt [assign–cvid` *`cvid`*`] [nni` *`port-list`*`]`

Command mode: Interface Config

subscribe match priority

Use this command to configure the VLAN assignment criteria for priority tagged packets on an interface or range of interfaces. Upstream traffic goes to configured NNI ports based on a switching or redirection action, depending upon the service subscribed for.

Format: `subscribe` *`service-name subscription-name`* `match priority` *`pri`* `[assign-cvid` *`cvid`*`] [nni` *`port-list`*`]`

Command mode: Interface Config

subscribe match cvid

Use this command to configure the match VLAN assignment criteria for C–tagged packets. Upstream traffic goes to configured NNI ports based on a switching or redirection action, depending upon the service subscribed for. This command is applicable only on UNI–P ports.

Format: `subscribe` *`service-name subscription-name`* `match cvid` *`cvid`* `[[remark-cvid]` *`cvid]`* `|` `[remove-ctag]] [nni` *`port-list`*`]`

Command mode: Interface Config

subscribe match cvid priority

Use this command to configure the match VLAN assignment criteria for C–tagged packets based on both C– VID and, optionally, the Priority value in the C–tag. Upstream traffic goes to configured NNI ports based on a switching or redirection action, depending upon the service subscribed for. This command is applicable only on UNI–P ports.

Format: `subscribe` *`service-name subscription-name`* `match cvid` *`cvid`* `[priority` *`pri`* `[[remark-cvid]` *`cvid`*`] | [remove-ctag]] [nni` *`port-list`*`]`

Command mode: Interface Config

subscribe match svid

Use this command to configure the match VLAN assignment criteria for single S–tagged packets. Upstream traffic goes to configured NNI ports based on a switching or redirection action, depending upon the service subscribed for.

Format: `subscribe` *`service-name subscription-name`* `match svid` *`svid`* `[nni` *`port-list`*`]`

Command mode: Interface Config

subscribe match svid cvid

Use this command to configure the match VLAN assignment criteria for double–tagged packets. Upstream traffic goes to configured NNI ports based on a switching or redirection action, depending upon the service subscribed for.

Format: `subscribe` *`service-name subscription-name`* `match svid` *`svid`* `[cvid` *`cvid`* `[[remark-cvid` *`cvid`*`] | [remove-ctag]]] [nni` *`port list`*`]`

Command mode: Interface Config

subscribe

Use this command to subscribe for a TLS service on the port. Upstream traffic goes to configured NNI ports based on a switching decision.

Format: `subscribe` *`service-name subscription-name`* `[nni` *`port list`*`]`

Command mode: Interface Config

show dot1ad service

Use this command to display the specified service or all the services information (i.e. service name, service type and the S–VID) configured on the CPE.

Format: `show dot1ad service [[service-name] [unit/slot/port]]`

Command mode: Privileged

show dot1ad service-subscription

This command output shows all the services subscribed on the given LAN interfaces.

Format: `show dot1ad service-subscription {unit/slot/port | all | service-name}`

Command mode: Privileged

Parameter	*Description*
unit/slot/port	Shows all subscriptions on the specified unit/slot/port.
all	Shows subscriptions to all services.
service-name	Shows all subscriptions to the specified service name.
e-lan | e-line | e- tree | tls	These parameters define the type of traffic associated with the service instance. • **e-lan** — A switched or general service is one in which the traffic associated with that service is forwarded based on a standard L2 switching lookup using the S-VID and destination MAC as lookups in the FDB. **A port can be a member of multiple E-LAN services. If a switched service is assigned to multiple UNI ports, those ports will be able to forward traffic to each other as well as to the NNI ports. The same E-LAN service can also be applied on UNI-P and UNI-S ports.** • **e-line** — The e-line parameter creates a point-to-point service, in which traffic is forwarded directly to the NNI port in the upstream direction and to the associated UNI port in the downstream direction. An e-line service bypasses the standard VLAN/ MAC-based switching decisions, including the source MAC learning. Be default, system does not learn traffic belonging to the e-line service. An e-line service- instance defines a point-to-point service in which only one UNI-P or UNI-S port participates. Note. It is important to note that downstream broadcast and multicast traffic will still be redirected to the associated UNI port participating in the e-line service. • **e-tree** — The e-tree parameter creates a point-to-multipoint service in which the traffic associated with that service is forwarded directly to the NNI port in the upstream direction and direct to the associated UNI port(s) in the downstream direction. If an e-tree service instance is applied to multiple UNI ports, it becomes a point-to-multipoint service in which the participating user ports are still isolated from each other. **Note.** It is important to note that downstream broad-

	cast, multicast, and unknown destination (DLF) traffic will still be forwarded (replicated) to all ports participating in the e-tree service. • **tls** (Transparent LAN Service). Administrators can configure a TLS on UNI-P and UNIS ports. A Transparent LAN service is used to connect the remote sites of a customer with C-Tag transparency. There are no match criteria for a TLS. – If no TLS service is configured on an UNI-P port, all packets not matching any of the service instances configured on the ports will be dropped. If a TLS service is configured, then all packets not matching the other service instances on that port will be tagged as per the TLS definition on that port. TLS service defined by the user will be used by Untagged, Priority Tagged, and C-VLAN tagged packets which do not match any other service instances on the port. – If a TLS service is configured on an UNI-S port, service VLAN tagged (including double tagged) frames that do not match other service instances on the port will be forwarded to appropriate NNI port(s) based on the S-VID associated with the service without any VLAN modification. Untagged and priority tagged packets that do not match other service instances on the port wil be dropped.
port-list	NNI port list.

9.9.2 L2 Protocol Tunneling configuration commands

Layer 2 tunneling can be used to extend a network to remote sites across a service provider network. These commands configure layer 2 tunneling on switch interfaces.

To configure L2 protocol tunneling on an interface, you configure it as 802.1ad network-to-network interface (NNI) or user-to-network interface (UNI). Then, you configure the action (tunnel, terminate, discard, or discard- shutdown) the interface takes when it receives a PDU with a specified combination of a destination reserved MAC address and a protocol ID. If the interface is configured to tunnel the protocol/MAC address PDUs, then it appropriately tags the packet with a service definition (S-tag) and optionally with the customer's VLAN ID (C- tag), and forwards it to the NNI port.

dot1ad l2tunnel

This command configures an action (tunnel or terminate) for the given reserved MAC address on a particular service.

All reserved MAC addresses in the range 01:80:C2:00:00:00 to 01:80:C2:00:00:3F are configured with the 'terminate' action by default. When a reserved MAC is configured with the 'terminate' action, it is not visible under any 'show' or 'show running-config' commands.

Default: terminate

Format: `dot1ad l2tunnel vlan` *`vlan id`* `mac-address` *`reserved-mac`* `proto col-id` *`proto-id`* `{tunnel | terminate | discard [shutdown]}`

Command mode: Global Config

Parameter	*Description*
protocol-id	The protocol ID field that has to be matched in the in-

	gress packet to perform protocol tunneling. Protocol-id range is from 0x0001 to 0xffff.
reserved-mac	The destination mac-address field in the ingress packet that has to be matched for which the protocol tunneling needs to be configured. MAC address range is from 01:80:c2:00:00:00 to 01:80:c2:00:00:3F.
tunnel | terminate | discard [shutdown	The action to be taken on any packets that match the MAC-address/protocol-id combination. • **tunnel** — The packet is double-tagged with the service definition (S-VID) and customer VLAN ID (C-VID) and the packet is forwarded to the NNI port based on the S-VID. This action is taken whether or not the protocol has been enabled on the interface. • **terminate** — If the protocol has been enabled on the interface, then the control PDU is handed to the protocol processing application. If the protocol has not been enabled, then the control packet is dropped. • **discard [shutdown]** —The packet is discarded, regardless of whether the protocol is enabled on the interface. Use the optional shutdown keyword to shut down the interface and generate an SNMP trap.
vlan id	The service VLAN identifier.

no dot1ad l2tunnel

This command removes any dot1ad protocol processing from the port.

Format: `no dot1ad l2tunnel vlan` *`vlan id`* `MAC-address` *`reserved MAC`* `protocol-id` *`proto-id`*

Command mode: Global Config

show dot1ad mode

This command displays the port-type (UNI-P, UNI-S, NNI, or switch port), and the preserve C-tag's priority capability.

Format: `show dot1ad mode {all |` *`unit/slot/port`*`}`

Command mode: Privileged

show dot1ad l2tunnel

This command display the L2 reserved MAC filtering configuration.

Format: `show dot1ad l2tunnel {all | mac-address` *`mac-addr`* `| protocol-id` *`proto-id`*`} | vlan` *`vlan- id`*`}`

Command mode: Privileged

Both MAC–address and protocol–id can be used for indexing while displaying entries.

9.10 Provisioning (IEEE 802.1p) configuration commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

vlan port priority all

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

Format: `vlan port priority all` *priority*

Command mode: Global Config

vlan priority

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

Default: 0

Format: `vlan priority` *priority*

Command mode: Interface Config

9.11 Cut-Through (ASF) configuration commands

The Cut-through Mode (or Alternative Store and Forward Mode, ASF) feature allows the switch to operate in a mode such that the egress pipeline begins transmitting a packet before the ingress pipeline has completely received the entire packet. Enabling this mode decreases latency for large packets.

Alternate Store and forward (ASF) reduces latency for larger packets. In this mode, the MMU is allowed to forward a packet to the egress port before it has been entirely received in the Cell Buffer Pool (CBP) memory.

cut-through mode

Use this command to enable or disable cut-through mode on the switch. If you change the mode, you must reload the switch for the mode to take effect.

Default: disabled

Format: `cut-through mode`

Command mode: global configuration.

no cut-through mode

This command resets the cut-through mode to the default value.

Format: `no cut-through mode`

Command mode: global configuration.

show cut-through mode

Use this command to view the current and configured status of cut-through mode.

Format: `show cut-through mode`

Command mode: Global Config

Example:

The following shows example CLI display output for the command.

```
(Routing) #show cut-through

mode Current mode :Disable
Configured mode :Enable (This mode is effective on next reload)
```

9.12 Asymmetric Flow Control configuration

When in asymmetric flow control mode, the switch responds to PAUSE frames received from a peer by stopping packet transmission, but the switch does not initiate MAC control PAUSE frames.

When you configure the switch in asymmetric flow control (or no flow control mode), the device is placed in egress drop mode. Egress drop mode maximizes the throughput of the system at the expense of packet loss in a heavily congested system, and this mode avoids head-of-line blocking.

flowcontrol {symmetric|asymmetric}

Use this command to enable or disable the symmetric or asymmetric flow control on the switch. Asymmetric here means that Tx Pause can never be enabled. Only Rx Pause can be enabled.

Default: flow management disabled.

Format: `flowcontrol {symmetric|asymmetric}`

Command mode: Global Config

no flowcontrol {symmetric|asymmetric}

Use the no form of this command to disable symmetric or asymmetric flow control.

Format: `no flowcontrol {symmetric|asymmetric}`

Command mode: Global Config

flowcontrol

Use this command to enable or disable the symmetric flow control on the switch.

Default: flow management disabled.

Format: `flowcontrol`

Command mode: Global Config

no flowcontrol

Use the **no** form of this command to disable the symmetric flow control.

Format: `no flowcontrol`

Command mode: Global Config

show flowcontrol

Use this command to display the IEEE 802.3 Annex 31B flow control settings and status for a specific interface or all interfaces. The command also displays 802.3 Tx and Rx pause counts. Priority Flow Control frames counts are not displayed. If the port is enabled for priority flow control, operational flow control status is displayed as **Inactive**. Operational flow control status for stacking ports is always displayed as **N/A**.

Format: show flowcontrol [*unit/slot/port*]

Command mode: Privileged

9.13 Protected Ports configuration commands

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected (Global Config)

Use this command to create a protected port group. The groupid parameter identifies the set of protected ports. Use the name name pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. Default: blank.

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default: not secured

Format: `switchport protected` *`groupid`* `name` *`name`*

Command mode: Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The groupid parameter identifies the set of protected ports. The name keyword specifies the name to remove from the group.

Format: `no switchport protected` *`groupid`* `name`

Command mode: Global Config

switchport protected (Interface Config mode)

Use this command to add an interface to a protected port group. The *groupid* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default: not secured

Format: `switchport protected` *`groupid`*

Command mode: Interface Config

no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Format: `no switchport protected` *`groupid`*

Command mode: Interface Config

show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format: `show switchport protected` *`groupid`*

Command mode: Privileged
User

Term	*Value*
Group ID	The number that identifies the protected port group.
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. Default: blank.
List of Physical Ports	List of ports, which are configured as protected for the group identified with *groupid*. If no port is configured as protected for this group, this field is blank.

show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the *groupid*.

Format: `show interfaces switchport` *`unit/slot/port groupid`*

Command mode: Privileged
User

Term	*Value*
Name	A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. Default: blank. This field is optional.

Protected	Indicates whether the interface is protected or not. Values: TRUE or FALSE.

9.14 GARP configuration commands

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

set garp timer join

This command sets the GVRP join time per GARP for one interface, a range of interfaces, or all interfaces. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or reregistering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds).

Default: 20

Format: `set garp timer join` *`10-100`*

Command mode: Interface Config
Global Config

no set garp timer join

This command sets the GVRP join time to the default and only has an effect when GVRP is enabled.

Format: `no set garp timer join`

Command mode: Interface Config
Global Config

set garp timer leave

This command sets the GVRP leave time for one interface, a range of interfaces, or all interfaces or all ports and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds. The leave time must be greater than or equal to three times the join time.

Default: 60

Format: `set garp timer leave` *`20-600`*

Command mode: Interface Config
Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format: `no set garp timer leave`

Command mode: Interface Config
Global Config

set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants will need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode), or on a single port or a range of ports (Interface Config mode) and it only has an effect only when GVRP is enabled. The leave all time must be greater than the leave time.

Default: 1000

Format: `set garp timer leaveall` *`200-6000`*

Command mode: Interface Config
Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format: `no set garp timer leaveall`

Command mode: Interface Config
Global Config

show garp

This command displays GARP information.

Format: `show garp`

Command mode: Privileged
User

Term	*Value*
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

9.15 GVRP configuration commands

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

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

set gvrp adminmode

This command enables GVRP on the system.

Default: disabled

Format: `set gvrp adminmode`

Command mode: Privileged

no set gvrp adminmode

This command disables GVRP.

Format: `no set gvrp adminmode`

Command mode: Privileged

set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode), a range of ports (Interface Range mode), or all ports (Global Config mode).

Default: disabled

Format: `set gvrp interfacemode`

Command mode: Interface Config
Interface Range
Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format: `no set gvrp interfacemode`

Command mode: Interface Config
Global Config

show gvrp configuration

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

Format: `show gvrp configuration {`*`unit/slot/port`* `| all}`

Command mode: Privileged
User

Term	***Value***
Interface	unit/slot/port
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis.

	Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

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

Format: `show mac-address-table gmrp`

Command mode: Privileged

Term	*Value*
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
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:).

9.16 Port-Based Network Access Control configuration commands

This section describes the commands you use to configure port-based network access control (IEEE 802.1X). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

aaa authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- ias. Uses the internal authentication server users database for authentication. This method can be used in conjunction with any one of the existing methods like **local**, **radius**, etc.
- local. Uses the local username database for authentication.

- none. Uses no authentication.
- radius. Uses the list of all RADIUS servers for authentication.

Format: `aaa authentication dot1x default {[ias]|[`*`method1 [method2 [method3]]]`*`}`

Command mode: Global Config

clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format: `clear dot1x statistics {`*`unit/slot/port`* `| all}`

Command mode: Privileged

clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format: `clear dot1x authentication-history [`*`unit/slot/port`*`]`

Command mode: Privileged

clear radius statistics

This command is used to clear all RADIUS statistics.

Format: `clear radius statistics`

Command mode: Privileged

dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Default: disabled

Format: `dot1x eapolflood`

Command mode: Global Config

no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format: `no dot1x eapolflood`

Command mode: Global Config

dot1x dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default: disabled

Format: `dot1x dynamic-vlan enable`

Command mode: Global Config

no dot1x dynamic-vlan enable

Use this command to prevent the switch from creating VLANs when a RADIUS-assigned VLAN does not exist in the switch.

Format: `no dot1x dynamic-vlan enable`

Command mode: Global Config

dot1x guest-vlan

This command configures VLAN as guest vlan on an interface or a range of interfaces. The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Default: disabled

Format: `dot1x guest-vlan` *`vlan-id`*

Command mode: Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default: disabled

Format: `no dot1x guest-vlan`

Command mode: Interface Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format: `dot1x initialize` *`unit/slot/port`*

Command mode: Privileged

dot1x max-req

This command sets the maximum number of times the authenticator state machine on an interface or range of interfaces will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The count value must be in the range 1 - 10.

Default: 2

Format: `dot1x max-req` *`count`*

Command mode: Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format: `no dot1x max-req`

Command mode: Interface Config

dot1x max-users

Use this command to set the maximum number of clients supported on an interface or range of interfaces when MAC-based dot1x authentication is enabled on the port. The maximum users supported per port is dependent on the product. The count value is in the range 1 - 48.

Default: 48

Format: `dot1x max-users` *`count`*

Command mode: Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format: `no dot1x max-users`

Command mode: Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified interface or range of interfaces. Use the *force-unauthorized* parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the force-authorized parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the auto parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Default: auto

Format: `dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}`

Command mode: Interface Config

no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format: `no dot1x port-control`

Command mode: Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select `force-unauthorized`to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select force-authorized to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select auto to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Default: auto

Format: `dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}`

Command mode: Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format: `no dot1x port-control all`

Command mode: Global Config

dot1x mac-auth-bypass

If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones — to authenticate to the network using the client MAC address as an identifier.

Default: disabled

Format: `dot1x mac-auth-bypass`

Command mode: Interface Config

no dot1x mac-auth-bypass

This command sets the MAB mode on the ports to the default value.

Format: `no dot1x mac-auth-bypass`

Command mode: Interface Config

dot1x re-authenticate

This command begins the reauthentication sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format: `dot1x re-authenticate` *`unit/slot/port`*

Command mode: Privileged

dot1x re-authentication

This command enables reauthentication of the supplicant for the specified interface or range of interfaces.

Default: disabled

Format: `dot1x re-authentication`

Command mode: Interface Config

no dot1x re-authentication

This command disables reauthentication of the supplicant for the specified port.

Format: `no dot1x re-authentication`

Command mode: Interface Config

dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default: disabled

Format: `dot1x system-auth-control`

Command mode: Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format: `no dot1x system-auth-control`

Command mode: Global Config

dot1x system-auth-control monitor

Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Default: disabled

Format: `dot1x system-auth-control monitor`

Command mode: Global Config

no dot1x system-auth-control monitor

This command disables the 802.1X Monitor mode on the switch.

Format: `no dot1x system-auth-control monitor`

Command mode: Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on an interface or range of interfaces. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	*Value*
guest-vlan- period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauth-timeout must be a value in the range 1 - 65535.
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of

	time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The tx-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The server-timeout must be a value in the range 1 - 65535.

Default: guest-vlan-period: 90 seconds
reauth-period: 3600 seconds
quiet-period: 60 seconds
tx-period: 30 seconds
supp-timeout: 30 seconds
server-timeout: 30 seconds

Format: `dot1x timeout {{guest-vlan-period` *`seconds`*`} |{reauth-period` *`seconds`*`} | {quiet-period` *`seconds`*`} | {tx-period` *`seconds`*`} | {supp-timeout` *`seconds`*`} | {server-timeout` *`seconds`*`}}`

Command mode: Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format: `no dot1x timeout {guest-vlan-period | reauth-period | quiet-period | tx-period | supp- timeout | server-timeout}`

Command mode: Interface Config

dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface or range of interfaces. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID. The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default: 0

Format: `dot1x unauthenticated-vlan` *`vlan id`*

Command mode: Interface Config

no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format: `no dot1x unauthenticated-vlan`

Command mode: Interface Config

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The *user* parameter must be a configured user.

Format: `dot1x user` *user* {*unit/slot/port* | `all`}

Command mode: Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format: `no dot1x user` *user* {*unit/slot/port* | `all`}

Command mode: Global Config

authentication enable

This command globally enables the Authentication Manager. Interface configuration takes effect only if the Authentication Manager is enabled with this command.

Default: disabled

Format: `authentication enable`

Command mode: Global Config

no authentication enable

This command disables the Authentication Manager.

Format: `no authentication enable`

Command mode: Global Config

authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format: `authentication order {dot1x [mab [captive-portal] | captive-portal] | mab [dot1x [captive-portal]| captive-portal] | captive-portal}`

Command mode: Interface Config

no authentication order

This command returns the port to the default authentication order.

Format: `no authentication order`

Command mode: Interface Config

authentication priority

This command sets the priority for the authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. The authentication priority decides if a previously authenticated client is reauthenticated with a higher-priority method when the same is received. Captive portal is always the last method in the list.

Default: `authentication order dot1x mab captive portal`

Format: `authentication priority {dot1x [mab [captive portal] | captive portal] | mab [dot1x [captive portal]| captive portal] | captive portal}`

Command mode: Interface Config

no authentication priority

This command returns the port to the default order of priority for the authentication methods.

Format: `no authentication priority`

Command mode: Interface Config

authentication timer restart

This command sets the time, in seconds, after which reauthentication starts. (The default time is 300 seconds.) The timer restarts the authentication only after all the authentication methods fail. At the expiration of this timer, authentication is reinitiated for the port.

Format: `authentication timer restart <300-65535>`

Command mode: Interface Config

no authentication timer restart

This command sets the reauthentication value to the default value of 3600 seconds.

Format: `no authentication timer restart`

Command mode: Interface Config

show authentication authentication-history

Use this command to display information about the authentication history for a specified interface.

Format: `show authentication authentication-history unit/slot/port`

Command mode: Privileged

The following information is displayed for each interface.

Term	*Value*
Time Stamp	The time of the authentication.
Interface	The interface.
MAC-Address	The MAC address for the interface.
Auth Status Method	The authentication method and status for the interface.

show authentication interface

Use this command to display authentication method information either for all interfaces or a specified port.

Format: `show authentication interface {all | unit/slot/port }`

Command mode: Privileged

The following information is displayed for each interface.

Term	*Value*
Interface	The interface for which authentication configuration information is being displayed.
Authentication Restart timer	The time, in seconds, after which reauthentication starts.
Configured method order	The order of authentication methods used on a port.
Enabled method order	The order of authentication methods used on a port.
Configured method priority	The priority for the authentication methods used on a port.
Enabled method priority	The priority for the authentication methods used on a port.
Number of authenticated clients	The number of authenticated clients.
Logical Interface	The logical interface.
Client MAC addr	The MAC address for the client.
Authenticated Method	The current authentication method.
Auth State	If the authentication was successful.
Auth Status	The current authentication status.

Term	*Value*
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication log-in list, if any.
Method 3	The third method in the specified authentication login list, if any.

show authentication statistics

Use this command to display the authentication statistics for an interface.

Format: `show authentication statistics unit/slot/port`

Command mode: Privileged

The following information is displayed for each interface.

show authentication methods

Use this command to display information about the authentication methods.

Format: `show authentication methods`

Command mode: Privileged

Term	*Value*
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication log-in list, if any.
Method 3	The third method in the specified authentication login list, if any.

show authentication statistics

Use this command to display the authentication statistics for an interface.

Format: show authentication statistics *unit/slot/port*

Command mode: Privileged

The following information is displayed for each interface.

Term	*Value*
Port	The port for which data is displayed.
802.1X attempts	The number of Dot1x authentication attempts for the port.
802.1X failed attempts	The number of failed Dot1x authentication attempts for the port.
Mab attempts	The number of MAB (MAC authentication bypass) authentication attempts for the port.
Mab failed attempts	The number of failed MAB authentication attempts for the port.
Captive-portal attempts	The number of captive portal (Web authorization) authentication attempts for the port.
Captive-portal failed attempts	The number of failed captive portal authentication attempts for the port.

clear authentication statistics

Use this command to clear the authentication statistics on an interface.

Format: `clear authentication authentication-history {unit/slot/port] | all}`

Command mode: Privileged

clear authentication authentication-history

Use this command to clear the authentication history log for an interface.

Format: `clear authentication authentication-history {unit/slot/port | all}`

Command mode: Privileged

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format: show dot1x [{*summary* {*unit/slot/port* | all} | detail *unit/slot/port* | statistics *unit/ slot/port*]

Command mode: Privileged

If you do not use the optional parameters unit/slot/port or vlanid, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Term	*Value*
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.

If you use the optional parameter summary {unit/slot/port | all}, the dot1x configuration for the specified port or all ports are displayed.

Term	*Value*
Interface	The interface for which the configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are: force-unauthorized | force-authorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are: authorized | unauthorized.
Reauthentication Enabled	Indicates whether reauthentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are: authorized | unauthorized.

If you use the optional parameter 'detail unit/slot/port', the detailed dot1x configuration for the specified port is displayed.

Term	*Value*
Port	The interface for which the configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are: Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are: force-unauthorized | force-authorized | auto | mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine.

	Possible values are: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are: Request, Response, Success, Fail, Timeout, Idle and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds in the range of 0 and 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Configured MAB Mode	The administrative mode of the MAC authentication bypass feature on the switch.
Operational MAB Mode	The operational mode of the MAC authentication bypass feature on the switch. MAB might be administratively enabled but not operational if the control mode is not MAC based.
vlan-id	The VLAN assigned to the port by the radius server. This only valid when the port control mode is not MAC-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are: RADIUS, Unauthenticated VLAN, Guest VLAN, default, or Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds in the range of 1 and 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.
EAPOL Flood Mode Enabled	Indicates whether the EAPOL flood support is enabled on the switch. Possible values are: TRUE or FALSE.
Control Direction	The control direction for the specified port or ports. Possible values are: both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are: Default and Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port-control mode is not MAC-based.

For each client authenticated on the port, the *show dot1x detail unit/slot/port* command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Term	***Value***
Supplicant MAC Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are: Request, Response, Success, Fail, Timeout, Idle and Initialize.
VLAN-Assigned	The VLAN assigned to the client by the radius server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter *statistics unit/slot/port*, the following dot1x statistics for the specified port appear.

Term	***Value***
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.

EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x authentication-history

This command displays 802.1X authentication events and information during successful and unsuccessful Dot1x authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

Format: `show dot1x authentication-history {`*`unit/slot/port`* `| all} [failed-auth-only] [detail]`

Command mode: Privileged

Term	*Value*
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
MAC-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port on authentication.
VLAN Assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Monitor Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

show dot1x clients

This command displays 802.1X client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

Format: `show dot1x clients {`*`unit/slot/port`* `| all}`

Command mode: Privileged

Term	*Value*
Clients Authenticated using Monitor Mode	Indicates the number of the Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of Dot1x clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with the client.
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are: RADIUS, Unauthenticated VLAN, Monitor Mode or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are: Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

show dot1x users

This command displays 802.1X port security user information for locally configured users.

Format: `show dot1x users` *`unit/slot/port`*

Command mode: Privileged

Term	*Value*
Users	Users configured locally to have access to the specified port.

9.17 802.1X Supplicant commands

The system supports 802.1X ("dot1x") supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

dot1x pae

This command sets the port's dot1x role. The port can serve as either a supplicant or an authenticator.

Format: `dot1x pae {supplicant | authenticator}`

Command mode: Interface Config

dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port's attribute needs to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

Format: `dot1x supplicant port-control {auto | force-authorized | force_unauthorized}`

Command mode: Interface Config

Term	*Value*
auto	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
force-authorized	Sets the authorization state of the port to Authorized, bypassing the authentication process.
force-unauthorized	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default: auto

Format: `no dot1x supplicant port-control`

Command mode: Interface Config

dot1x supplicant max-start

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator.

Default: 3

Format: `dot1x supplicant max-start <1-10>`

Command mode: Interface Config

no dot1x supplicant max-start

This command sets the max-start value to the default.

Format: `no dot1x supplicant max-start`

Command mode: Interface Config

dot1x supplicant timeout start-period

This command configures the start period timer interval to wait for the EAP identity request from the authenticator.

Default: 30 seconds

Format: `dot1x supplicant timeout start-period <1-65535 seconds>`

Command mode: Interface Config

no dot1x supplicant timeout start-period

This command sets the start-period value to the default.

Format: `no dot1x supplicant timeout start-period`

Command mode: Interface Config

dot1x supplicant timeout held-period

This command configures the held period timer interval to wait for the next authentication on previous authentication fail.

Default: 60 seconds

Format: `dot1x supplicant timeout held-period <1-65535 seconds>`

Command mode: Interface Config

no dot1x supplicant timeout held-period

This command sets the held-period value to the default value.

Format: `no dot1x supplicant timeout held-period`

Command mode: Interface Config

dot1x supplicant timeout auth-period

This command configures the authentication period timer interval to wait for the next EAP request challenge from the authenticator.

Default: 30 seconds

Format: `dot1x supplicant timeout auth-period <1-65535 seconds>`

Command mode: Interface Config

no dot1x supplicant timeout auth-period

This command sets the auth-period value to the default value.

Format: `no dot1x supplicant timeout auth-period`

Command mode: Interface Config

dot1x supplicant user

Use this command to map the given user to the port.

Format: `dot1x supplicant user`

Command mode: Interface Config

show dot1x statistics

This command displays the dot1x port statistics in detail.

Format: `show dot1x statistics` *`slot/port`*

Command mode: Privileged
User

Term	*Value*
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.

9.18 Task-based Authorization

Task-based authorization allows users to have different permission levels (read, write, execute, debug) at a per- component level. Task-based authorization uses the concept of components/tasks to define permission for commands for a given user.

Users are assigned to User Groups that are, in turn, associated with Task Groups. Each Task Group is then associated with one or more tasks/components. This release supports the AAA, BGP and OSPF components. Also, this feature is supported only for users who are authenticated locally via the CLI interface.

usergroup

This command creates a user group with the specified name and enters user group configuration mode.

Format: `usergroup` *`usergroup-name`*

Command mode: Global Config

no usergroup

This command removes the user group with the specified name.

Format: `no usergroup` *`usergroup-name`*

Command mode: Global Config

taskgroup

This command creates a task group with the specified name and enters task group configuration mode.

Format: `taskgroup` *`taskgroup-name`*

Command mode: Global Config

no taskgroup

This command removes the task group with the specified name.

Format: `no taskgroup` *`taskgroup-name`*

Command mode: Global Config

username usergroup

This command assigns the specified user to the specified user group.

Format: `username <`*`username`*`> usergroup` *`usergroup-name`*

Command mode: Global Config

no username usergroup

This command removes the specified user from the specified user group.

Format: `no usergroup` *`usergroup-name`*

Command mode: Global Config

description (User Group Config)

This command sets a description for the user group.

Format: `description` *`description`*

Command mode: User Group Config

no description (User Group Config)

This command removes the description from the user group.

Format: `no description`

Command mode: User Group Config

inherit usergroup

This command sets the parent user group of the current user group. The user group will have the permissions of the specified parent group.

Format: `inherit usergroup` *`usergroup-name`*

Command mode: User Group Config

no inherit usergroup

This command removes the specified parent group relationship from the user group.

Format: `no inherit usergroup` *`usergroup-name`*

Command mode: User Group Config

taskgroup (User Group Config)

This command associates the user group with the specified task group.

Format: `taskgroup` *`taskgroup-name`*

Command mode: User Group Config

no taskgroup (User Group Config)

This command removes the user group's relationship with the associated task group.

Format: no taskgroup *taskgroup-name*

Command mode: User Group Config

description (Task Group Config)

This command sets a description for the task group.

Format: `description` *`description`*

Command mode: Task Group Config

no description (Task Group Config)

This command removes the description from the task group.

Format: `no description`

Command mode: Task Group Config

inherit taskgroup

This command sets the parent task group of the current task group. The task group will have the permissions of the specified parent task group.

Format: `inherit taskgroup` *`taskgroup-name`*

Command mode: Task Group Config

no inherit taskgroup

This command removes the specified parent group relationship from the user group.

Format: `no inherit taskgroup` *`taskgroup-name`*

Command mode: Task Group Config

task [read] [write] [debug] [execute]

This command associates the task group with the specified set of task permissions.

Default: No permissions

Format: `task [read] [write] [debug] [execute] {aaa | ospf | bgp}`

Command mode: Task Group Config

no task {aaa | ospf | bgp}

This command removes all relationships with the associated task.

Format: no task {aaa | ospf | bgp}

Command mode: Task Group Config

show aaa usergroup

This command displays a list of user groups and their configuration.

Format: `show aaa usergroup [usergroup-name]`

Command mode: Privileged

show aaa taskgroup

This command displays a list of task groups and their configuration.

Format: `show aaa taskgroup [taskgroup-name]`

Command mode: Privileged

show aaa userdb

This command displays a list of users and list of groups the users participate in.

Format: `show aaa userdb [username]`

Command mode: Privileged

9.19 Storm Control configuration commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

The system provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per- port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Using the “no” version of the “storm-control” command (not stating a “level”) disables that form of storm-control but maintains the configured “level” (to be active the next time that form of storm-control is enabled).

The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512 bytes packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default: disabled

Format: `storm-control broadcast`

Command mode: Global Config
Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format: `no storm-control broadcast`

Command mode: Global Config
Interface Config

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.

Default: none

Format: `storm-control broadcast action {shutdown | trap}`

Command mode: Global Config
Interface Config

no storm-control broadcast action

This command configures the broadcast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format: `no storm-control broadcast action`

Command mode: Global Config
Interface Config

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.

Default: 5

Format: `storm-control broadcast level` *`0-100`*

Command mode: Global Config
Interface Config

no storm-control broadcast level

This command sets 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.

Format: `no storm-control broadcast level`

Command mode: Global Config
Interface Config

storm-control broadcast rate

Use this command to configure the broadcast 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, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default: 0

Format: `storm-control broadcast rate` *`0-33554431`*

Command mode: Global Config
Interface Config

no storm-control broadcast rate

This command sets 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.

Format: `no storm-control broadcast rate`

Command mode: Global Config
Interface Config

storm-control multicast

This command enables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default: disabled

Format: `storm-control multicast`

Command mode: Global Config
Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format: `no storm-control multicast`

Command mode: Global Config
Interface Config

storm-control multicast action

This command configures the multicast 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 multicast packets at a rate above the threshold is diagnostically disabled. The option trap sends trap messages approximately every 30 seconds until multicast storm control recovers.

Default: none

Format: `storm-control multicast action {shutdown | trap}`

Command mode: Global Config
Interface Config

no storm-control multicast action

This command returns the multicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format: `no storm-control multicast action`

Command mode: Global Config
Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default: 5

Format: `storm-control multicast level` *`0-100`*

Command mode: Global Config
Interface Config

no storm-control multicast level

This command sets 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.

Format: `no storm-control multicast level` *`0-100`*

Command mode: Global Config
Interface Config

storm-control multicast rate

Use this command to configure the multicast 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, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default: 0

Format: `storm-control multicast rate` *`0-33554431`*

Command mode: Global Config
Interface Config

no storm-control multicast rate

This command sets 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.

Format: `no storm-control multicast rate`

Command mode: Global Config
Interface Config

storm-control unicast

This command enables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default: disabled

Format: storm-control unicast

Command mode: Global Config
Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format: `no storm-control unicast`

Command mode: Global Config
Interface Config

storm-control unicast action

This command configures the unicast 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 unicast packets at a rate above the threshold is diagnostically disabled. The option trap sends trap messages approximately every 30 seconds until unicast storm control recovers.

Default: none

Format: `storm-control unicast action {shutdown | trap}`

Command mode: Global Config
Interface Config

no storm-control unicast action

This command returns the unicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format: `no storm-control unicast action`

Command mode: Global Config
Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default: 5

Format: `storm-control unicast level` *`0-100`*

Command mode: Global Config
Interface Config

no storm-control unicast level

This command sets 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.

Format: `no storm-control unicast level`

Command mode: Global Config
Interface Config

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, the rate of unicast traffic is limited to the configured threshold.

Default: 0

Format: `storm-control unicast rate 0-33554431`

Command mode: Global Config
Interface Config

no storm-control unicast rate

This command sets 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.

Format: `no storm-control unicast rate`

Command mode: Global Config
Interface Config

show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters.

Use the all keyword to display the per-port configuration parameters for all interfaces, or specify the *unit/slot/port* to display information about a specific interface.

Format: `show storm-control [all | unit/slot/port]`

Command mode: Privileged

Term	*Value*
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

9.20 Link Dependency configuration commands

The following commands configure link dependency. Link dependency allows the link status of specified ports to be dependent on the link status of other ports. Consequently, if a port that is depended on by other ports loses link, the dependent ports are administratively disabled or administratively enabled so that the dependent ports links are brought down or up respectively.

no link state track

This command clears link-dependency options for the selected group identifier.

Format: `no link state track group-id`

Command mode: Global Config

link state group

Use this command to indicate if the downstream interfaces of the group should mirror or invert the status of the upstream interfaces. The default configuration for a group is down (that is, the downstream interfaces will mirror the upstream link status by going down when all upstream interfaces are down). The action up option causes the downstream interfaces to be up when no upstream interfaces are down.

Default: Down

Format: `link state group` *`group-id`* `action {up | down}`

Command mode: Global Config

no link state group

Use this command to restore the link state to down for the group.

Format: `no link state group` *`group-id`* `action`

Command mode: Global Config

link state group downstream

Use this command to add interfaces to the downstream interface list. Adding an interface to a downstream list brings the interface down until an upstream interface is added to the group. The link status then follows the interface specified in the upstream command. To avoid bringing down interfaces, enter the upstream command prior to entering the downstream command.

Format: `link state group` *`group-id`* `downstream`

Command mode: Interface Config

no link state group downstream

Use this command to remove the selected interface from the downstream list.

Format: `no link state group` *`group-id`* `downstream`

Command mode: Interface Config

link state group upstream

Use this command to add interfaces to the upstream interface list. Note that an interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same link state group or as a downstream interface in a different link state group, if either configuration creates a circular dependency between groups.

Format: `link state group` *`group-id`* `upstream`

Command mode: Interface Config

no link state group upstream

Use this command to remove the selected interfaces from upstream list.

Format: `no link state group` *`group-id`* `upstream`

Command mode: Interface Config

show link state group

Use this command to display information for all configured link-dependency groups or a specified link-dependency group.

Format: `show link state group` *`group-id`*

Command mode: Privileged

show link state group detail

Use this command to display detailed information about the state of upstream and downstream interfaces for a selected link-dependency group. Group Transitions is a count of the number of times the downstream interface has gone into its “action” state as a result of the upstream interfaces link state.

Format: `show link state group` *`group-id`* `detail`

Command mode: Privileged

9.21 Link Local Protocol Filtering configuration commands

Link Local Protocol Filtering (LLPF) allows the switch to filter out multiple proprietary protocol PDUs, such as Port Aggregation Protocol (PAgP), if the problems occur with proprietary protocols running on standards-based switches. If certain protocol PDUs cause unexpected results, LLPF can be enabled to prevent those protocol PDUs from being processed by the switch.

llpf

Use this command to block LLPF protocol(s) on a port.

Default: Enabled for the blockudld parameter; disabled for all others.

Format: `llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall}`

Command mode: Interface Config

no llpf

Use this command to unblock LLPF protocol(s) on a port.

Format: `no llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall }`

Command mode: Interface Config

show llpf interface

Use this command to display the status of LLPF rules configured on a particular port or on all ports.

Format: `show llpf interface [all |` *`unit/slot/port`*`]`

Command mode: Privileged

Term	*Value*
Block ISDP	Shows whether the port blocks ISDP PDUs.
Block VTP	Shows whether the port blocks VTP PDUs.
Block DTP	Shows whether the port blocks DTP PDUs.
Block UDLD	Shows whether the port blocks UDLD PDUs.

Block PAGP	Shows whether the port blocks PAgP PDUs.
Block SSTP	Shows whether the port blocks SSTP PDUs.
Block All	Shows whether the port blocks all proprietary PDUs available for the LLDP feature.

9.22 MVR configuration commands

This section lists the Multicast VLAN Registration (MVR) commands.

mvr

Use this command to enable MVR. This is disabled by default.

Default: disabled

Format: `mvr`

Command mode: interface configuration, global configuration

no mvr

Use this command to disable MVR.

Format: `no mvr`

Command mode: interface configuration, global configuration

mvr group

Use this command to add an MVR membership group.

Format: `mvr group`

Command mode: Global Config

no mvr group

Use this command to disable an MVR membership group.

Format: `no mvr group`

Command mode: Global Config

mvr immediate

Use this command to enable MVR Immediate Leave mode. If the interface is configured as source port, MVR Immediate Leave mode cannot be enabled. MVR Immediate Leave mode disabled by default.

Default: disabled

Format: `mvr immediate`

Command mode: Interface Config

no mvr immediate

Use this command to disable MVR Immediate Leave mode.

Format: `mvrm immediate`

Command mode: Interface Config

mvr mode

Use this command to change the MVR mode type. Compatible is the default mode type.

Format: `mvr mode [compatible | dynamic]`

Command mode: Global Config

no mvr mode

Use this command to set the MVR mode type to the default value of compatible.

Format: `no mvr mode`

Command mode: Global Config

mvr querytime

Use this command to set the MVR query response time in units of tenths of a second. The query time is the maximum time to wait for an IGMP membership report on a receiver port before removing the port from the multicast group. The query time only applies to receiver ports and is specified in tenths of a second. The default is 5.

Format: `mvr querytime *1-100*`

Command mode: Global Config

no mvr querytime

Use this command to set the MVR query response time to the default value.

Format: `no mvr querytime`

Command mode: Global Config

mvr type

Use this command to set the MVR port type. The default is none.

Format: `mvr type [receiver | source]`

Command mode: Interface Config

no mvr type

Use this command to reset the MVR port type to None.

Format: `no mvr type`

Command mode: Interface Config

mvr vlan

Use this command to set the MVR multicast VLAN.

Default: 1

Format: `mvr vlan *1-4093*`

Command mode: Global Config

no mvr vlan

Use this command to set the MVR multicast VLAN to the default value.

Format: `no mvr vlan`

Command mode: Global Config

mvr vlan group

Use this command to make a port participate in a specific MVR group. The default value is None.

Format: `mvr vlan mvlan group A.B.C.D.`

Command mode: Interface Config

no mvr vlan group

Use this command to remove port participation in the specific MVR group.

Format: `no mvr vlan mvlan group A.B.C.D.`

Command mode: Interface Config

show mvr

Use this command to display global MVR settings.

Format: `show mvr`

Command mode: Privileged

show mvr members

Use this command to display the allocated MVR membership groups.

Format: `show mvr members [A.B.C.D.]`

Command mode: Privileged

show mvr interface

Use this command to display the configuration of MVR-enabled interfaces.

Format: `show mvr interface [interface-id [members [vlan vlan-id]]]`

Command mode: Privileged

show mvr traffic

Use this command to display global MVR statistics.

Format: `show mvr traffic`

Command mode: Privileged

debug mvr trace

Use this command to enable MVR debug tracing. The default value is disabled.

Format: `debug mvr trace`

Command mode: Privileged

no debug mvr trace

Use this command to disable MVR debug tracing.

Format: `no debug mvr trace`

Command mode: Privileged

debug mvr packet

Use this command to enable MVR receive/transmit packets debug tracing. If it is executed without specifying the arguments, both receive and transmit packets debugging is enabled. The default is enabled.

Format: `debug mvr packet [receive | transmit]`

Command mode: Privileged

no debug mvr packet

Use this command to disable MVR receive/transmit packet debug tracing.

Format: `no debug mvr packet [receive | transmit]`

Command mode: Privileged

9.23 LAG (802.3ad) configuration commands

This section describes the commands you use to configure port-channels, which is defined in the 802.3ad specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols. A static port-channel interface does not require a partner system to be able to aggregate its member ports.

If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

port-channel

This command configures a new port-channel (LAG) and generates a logical *unit/slot/port* number for the port-channel. The name field is a character string which allows the dash "-" character as well as alphanumeric characters. Use the show port channel command to display the *unit/slot/port* number for the logical interface. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Before you include a port in a port-channel, set the port physical mode. For more information, see "speed" on page 427.

Format: `port-channel` *name*

Command mode: Global Config

addport

This command adds one port to the port-channel (LAG). The first interface is a logical *unit/slot/port* number of a configured port-channel. You can add a range of ports by specifying the port range when you enter Interface Config mode for example: interface 1/0/1-1/0/4. Instead of unit/slot/port, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

Format: `addport` *`logical unit/slot/port`*
Command mode: Interface Config

deleteport (Interface Config mode)

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical *unit/slot/port* number of a configured port-channel (or range of port-channels). Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `deleteport` *`logical unit/slot/port`*
Command mode: Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical *unit/slot/port* number of a configured port-channel. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `deleteport {`*`logical unit/slot/port`*` | all}`
Command mode: Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of key is 0 to 65535. This command can be used to configure a single interface or a range of interfaces.

Default: 0x8000
Format: `lacp admin key` *`key`*
Command mode: Interface Config

This command is applicable only to port-channel interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format: `no lacp admin key`
Command mode: Interface Config

lacp collector max-delay

Use this command to configure the port-channel collector max delay. This command can be used to configure a single interface or a range of interfaces. The valid range of delay is 0-65535.

Default: 0x8000
Format: `lacp collector max delay` *`delay`*
Command mode: Interface Config

This command is applicable only to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format: `no lacp collector max delay`
Command mode: Interface Config

lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. The valid range for key is 0-65535.

Default: Internal Interface Number of this Physical Port
Format: `lacp actor admin key` *`key`*
Command mode: Interface Config

This command is applicable only to port-channel interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format: `no lacp actor admin key`
Command mode: Interface Config

lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format: `lacp actor admin state individual`
Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format: `no lacp actor admin state individual`
Command mode: Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format: `lacp actor admin state longtimeout`

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format: `no lacp actor admin state longtimeout`

Command mode: Interface Config

This command is applicable only to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format: `lacp actor admin state passive`

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format: `no lacp actor admin state passive`

Command mode: Interface Config

lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. This command can be used to configure a single interface or a range of interfaces.

Default: 0x07

Format: `lacp actor admin state {individual|longtimeout|passive}`
Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Both the no port lacptimeout 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.

Format: `no lacp actor admin state {individual|longtimeout|passive}`

Command mode: Interface Config

lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port for an interface or range of interfaces. The valid range for *priority* is 0 to 65535.

Default: 0x80

Format: `lacp actor port priority` *`0-65535`*

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format: `no lacp actor port priority`

Command mode: Interface Config

lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. This command can be used to configure a single interface or a range of interfaces. The valid range for *key* is 0 to 65535.

Default: 0x0

Format: `lacp partner admin key` *`key`*

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp partner admin key

Use this command to set the administrative value of the Key for the protocol partner to the default.

Format: `no lacp partner admin key`

Command mode: Interface Config

lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format: `lacp partner admin state individual`

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format: `no lacp partner admin state individual`

Command mode: Interface Config

lacp partner admin state longtimeout

Use this command to set LACP partner admin state to longtimeout.

Format: `lacp partner admin state longtimeout`

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format: `no lacp partner admin state longtimeout`

Command mode: Interface Config

This command is applicable only to physical interfaces.

lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format: `lacp partner admin state passive`

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format: `no lacp partner admin state passive`

Command mode: Interface Config

lacp partner port id

Use this command to configure the LACP partner port id. This command can be used to configure a single interface or a range of interfaces. The valid range for port-id is 0 to 65535.

Default: 0x80

Format: `lacp partner port-id` *`port-id`*

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format: `no lacp partner port-id`

Command mode: Interface Config

lacp partner port priority

Use this command to configure the LACP partner port priority. This command can be used to configure a single interface or a range of interfaces. The valid range of priority is 0 to 65535.

Default: 0x0

Format: `lacp partner port priority` *`priority`*

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format: `no lacp partner port priority`

Command mode: Interface Config

lacp partner system-id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range of system-id is 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF.

Default: 00:00:00:00:00:00

Format: `lacp partner system-id` *`system-id`*

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp partner system-id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format: `no lacp partner system-id`
Command mode: Interface Config

lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range of priority is 0 to 65535.

Default: 0x0

Format: `lacp partner system priority` *`0-65535`*

Command mode: Interface Config

This command is applicable only to physical interfaces.

no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format: `no lacp partner system priority`

Command mode: Interface Config

interface lag

Use this command to enter Interface Config for the specified LAG.

Format: `interface lag` *`Lag-interface-number`*

Command mode: Global Config

port-channel static

This command enables the static mode on a port-channel (LAG) interface or range of interfaces. By default the static mode for a new port-channel is enabled, which means the port-channel is static. If the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel is enabled, which means the port-channel is static. You can only use this command on port-channel interfaces.

Default: enabled

Format: `port-channel static`

Command mode: Interface Config

no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format: `no port-channel static`

Command mode: Interface Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default: enabled

Format: `port lacpmode`

Command mode: Interface Config

no port lacpmode

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

Format: `no port lacpmode`

Command mode: Interface Config

port lacpmode enable all

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

Format: `port lacpmode enable all`

Command mode: Global Config

no port lacpmode enable all

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

Format: `no port lacpmode enable all`

Command mode: Global Config

port lacptimeout (Interface Config)

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Default: long

Format: `port lacptimeout {actor | partner} {long | short}`

Command mode: Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (actor or partner).

Format: `no port lacptimeout {actor | partner}`

Command mode: Interface Config

Both the no port lacptimeout 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 (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Default: long

Format: `port lacptimeout {actor | partner} {long | short}`

Command mode: Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

Format: `no port lacptimeout {actor | partner}`

Command mode: Global Config

Both the no port lacptimeout 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-channel adminmode

This command enables all configured port-channels with the same administrative mode setting.

Format: `port-channel adminmode all`

Command mode: Global Config

no port-channel adminmode

This command disables all configured port-channels with the same administrative mode setting.

Format: `no port-channel adminmode all`

Command mode: Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical *unit/slot/port* for a configured port-channel. The option *all* sets every configured port-channel with the same administrative mode setting. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Default: enabled

Format: `port-channel linktrap {`*`logical unit/slot/port`*` | all}`

Command mode: Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical *unit/slot/port* for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

Format: `no port-channel linktrap {`*`logical unit/slot/port`*` | all}`

Command mode: Global Config

port-channel load-balance

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port- channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

This command can be configured for a single interface, a range of interfaces, or all interfaces. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Default: 3

Format: `port-channel load-balance { dst-ip | dst-mac | enhanced | src-dst-ip | src-dst-mac | src-ip | src-mac } {`*`unit/slot/port`*` | all}`

Command mode: Global config

Interface config

Term	*Value*
src-mac	Source MAC, VLAN, EtherType, and incoming port associated with the packet.
dst-mac	Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
src-dst-mac	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
src-ip	Source IP and Source TCP/UDP fields of the packet.
dst-ip	Destination IP and Destination TCP/UDP Port fields of the packet.
src-dst-ip	Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
enhanced	Enhanced hashing mode.
unit/slot/port| all	Global Config Mode only: The interface is a logical *unit/slot/port* number of a configured port-channel. *All* applies the command to all currently configured port-channels.

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format: `no port-channel load-balance {`*`unit/slot/port`*` | all}`

Command mode: Global config

Interface config

Term	*Value*
unit/slot/ port| all	Global Config Mode only: The interface is a logical *unit/slot/port* number of a configured port-channel. *All* applies the command to all currently configured port-channels.

port-channel local-preference

This command enables the local-preference mode on a port-channel (LAG) interface or range of interfaces. By default, the local-preference mode for a port-channel is disabled. This command can be used only on port-channel interfaces.

Default: disabled

Format: `port-channel local-preference`

Command mode: Interface Config

no port-channel local-preference

This command disables the local-preference mode on a port-channel.

Format: `no port-channel local-preference`

Command mode: Interface Config

port-channel min-links

This command configures the port-channel's minimum links for lag interfaces.

Default: 1

Format: `port-channel min-links` *`1-8`*

Command mode: Interface Config

port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical *unit/slot/port* for a configured port-channel, and name is an alphanumeric string up to 15 characters. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `port-channel name {`*`logical unit/slot/port`*`}` *`name`*

Command mode: Global Config

port-channel system priority

Use this command to configure port-channel system priority. The valid range of priority is 0 to 65535.

Default: 0x8000

Format: `port-channel system priority` *`priority`*

Command mode: Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format: `no port-channel system priority`

Command mode: Global Config

show hashdest

Use this command to predict how packets are forwarded over a LAG or to the next hop device when ECMP is the destination. Given the link aggregation method, ingress physical port and values of various packet fields, this command predicts an egress physical port within the LAG or ECMP for the packet.

Format: show hashdest {lag *lag-id* | ecmp *prefix/prefix-length*} in_port *unit/slot/port* src-mac *macaddr* dst-mac *macaddr* [vlan *vlan-id*] ethertype *0xXXXX* [src-ip {*ipv4-addr* | *ipv6- addr*} dst-ip {*ipv4-addr* | *ipv6-addr*} protocol *pid* src-l4-port *port-num* dst-l4-port *port-num*]

Command mode: Privileged

Term	*Value*
lag	The LAG group for which to display the egress physical port.
ecmp	The IP address of the EMC_ group for which to display the egress physical port.
in_port	The incoming physical port for the system.
src-mac	The MAC address of the source.
dst-mac	The destination MAC address.
vlan	The VLAN ID for VLAN-tagged packets. Do not use this parameter or enter 0 for non- VLAN-tagged packets.
ethertype	The 16-bit EtherType value, in the form 0xXXXX. For layer 3 packets, hash prediction is only available for IPv4 (0x0800) and IPv6 (0x86DD).
src-ip	The source IP address, entered as x.x.x.x for IPv4 or x:x:x:x:x:x:x:x for IPv6 packets.
dst-ip	The destination IP address, entered as x.x.x.x for IPv4 or x:x:x:x:x:x:x:x for IPv6 packets.
protocol	The protocol ID.
src-l4-port	The layer 4 source port.
dst-l4-port	The layer 4 destination port.

show lacp actor

Use this command to display LACP actor attributes. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: show lacp actor {*unit/slot/port*|all}

Command mode: Global Config

The following output parameters are displayed.

Term	*Value*
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

Use this command to display LACP partner attributes. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `show lacp actor {`*`unit/slot/port`*`|all}`

Command mode: Privileged

The following output parameters are displayed.

Term	*Value*
System Priority	The administrative value of priority associated with the Partner's System ID.
System ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `show port-channel brief`

Command mode: User

For each port-channel the following information is displayed:

Term	*Value*
Logical Interface	unit/slot/port of the logic 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.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. The lag *lag-intf-num* parameter can be used to determine the specific LAG interface, and the *lag-intf-num* value should indicate the LAG port number.

Format: `show port-channel`

Command mode: Privileged

Term	*Value*
Logical Interface	The valid unit/slot/port number.
port-channel name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Shows whether the link is up or down.
Admin Mode	Possible values are: enabled or disabled. The factory default is enabled.
Type	Shows whether the port-channel is statically or dynamically maintained. • **Static** — The port-channel is statically maintained. • **Dynamic** — The port-channel is dynamically maintained.
Load Balance Option	The load balance option associated with this LAG. See the port-channel load-balance command.
Local Preference	Indicates whether the local preference mode is enabled or disabled.
Mode	A listing of the ports that are members of this port-channel (LAG), in *unit/slot/port* notation.
Mbr Ports	There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (**long** or **short**) for Device Type (**actor** or **partner**).
Port Speed	Speed of the port-channel port.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).

show port-channel system priority

Use this command to display the port-channel system priority.

Format: `show port-channel system priority`

Command mode: Privileged

show port-channel counters

Use this command to display port-channel counters for the specified port.

Format: `show port-channel` *`unit/slot/port`* `counters`

Command mode: Privileged

Term	*Value*
Local Interface	The valid slot/port number.
Channel Name	The name of this port-channel (LAG).
Link State	Shows whether the link is up or down.
Admin Mode	Possible values are: 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.

clear port-channel counters

Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

Format: `clear port-channel {lag-intf-num | unit/slot/port} counters`

Command mode: Privileged

clear port-channel all counters

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Format: `clear port-channel all counters`

Command mode: Privileged

9.24 VPC configuration commands

VPC (also known as MLAG) enables a LAG to be created across two independent switches, so that some member ports of a VPC can reside on one switch and the other members of a VPC can reside on another switch. The partner device on the remote side can be a VPC-unaware unit. To the unaware unit, the VPC appears to be a single LAG connected to a single switch.

vpc domain

Use this command to enter into VPC configuration mode and creates a VPC domain with the specified domain- id. Only one VPC domain can be created on a given device. The domain-id of the VPC domain should be equal to the one configured on the other VPC peer with which this device wants to form a VPC pair. The configured VPC domain-ids are exchanged during role election and if they are configured differently on the peer devices, the VPC does not become operational.

The administrator needs to ensure that the no two VPC domains can share the same VPC domain-id. Domain- id is used to derive the auto-generated VPC MAC address that is used in the actor ID field in the LACP PDUs and STP BPDUs sent out on VPC interfaces. When two VPC domains have the same domain-id, it leads to the same actor IDs and results in LACP convergence issues and STP convergence issues.

The range of domain id is 1-255.

Format: `vpc domain` *`domain-id`*

Command mode: Global Config

no vpc domain

Use this command to deletes the VPC domain, disable peer-keepalive, disable peer-detection, and reset the configured parameters (role priority, VPC MAC address and VPC system priority) for the VPC domain.

Format: `no vpc domain` *`domain-id`*

Command mode: Global Config

feature vpc

This command enables VPC globally. VPC role election occurs if both VPC and the keepalive state machine are enabled (see “peer-keepalive timeout” on page 606). Peer link also has to be configured for role election to occur.

Format: `feature vpc`

Command mode: Global Config

no feature vpc

This command disables VPC.

Format: `no feature vpc`

Command mode: Global Config

peer detection enable

This command starts the dual control plane detection protocol (DCPDP) on the VPC switch. The peer VPC switch’s IP address must be configured for the DCPDP to start on an VPC switch.

Default: none

Format: `peer detection enable`

Command mode: VPC Config

no peer detection enable

This command disables the dual control plane detection protocol (DCPDP) on the VPC switch.

Format: `no peer detection enable`

Command mode: VPC Config

peer detection interval

Use this command to configure the DCPDP transmission interval and reception timeout.

The configurable transmission interval range is 200 ms–4000 ms. The configurable reception timeout range is 700 ms–14000 ms. The default transmission interval is 1000 ms; the default reception timeout is 3500 ms.

Default: Transmission interval: 1000 ms
Reception timeout: 3500 ms

Format: `peer detection interval` *`msecs`* `timeout` *`seconds`*

Command mode: VPC Config

no peer detection interval

Use this command to reset the DCPDP transmission interval and reception timeout to default values.

Format: `no peer detection interval` *`msecs`* `timeout` *`seconds`*

Command mode: VPC Config

peer-keepalive destination

This command configures the IP address of the peer VPC switch, which is the destination IP address of the dual control plane detection protocol (DCPDP) on the peer VPC switch. This configuration is used by the dual control plane detection protocol (DCPDP) on the VPC switches. It also configures the source IP address of the DCPDP message, which is the self IP on the VPC switch. The UDP port on which the VPC switch listens to the DCPDP messages can also be configured with this command.

The configurable range for the UDP port 1 to 65535 (Default is 60000).

Format: `peer-keepalive destination` *`ipaddress`* `switch` *`ipaddress`* `[udp-port` *`port`*`]`

Command mode: VPC Config

no peer-keepalive destination

This command clears the configuration of the switch IP address, IP address of peer device, and the UDP port settings.

Format: `no peer-keepalive destination` *`ipaddress`* `switch` *`ipaddress`* `[udp-port` *`port`*`]`

Command mode: VPC Config

peer-keepalive enable

This command starts the keepalive state machine on the VPC device, if VPC is globally enabled.

Default: disabled

Format: `peer-keepalive enable`

Command mode: VPC Config

no peer-keepalive enable

This command stops the keepalive state machine of the VPC switch.

Format: `no peer-keepalive enable`

Command mode: VPC Config

peer-keepalive timeout

This command configures the peer keepalive timeout value (in seconds). If an VPC switch does not receive a keepalive message from the peer for the duration of this timeout value, it transitions its role (if required).

The keepalive state machine is not restarted if keepalive priority is modified post election.

The configurable range is 2 to 15 seconds. The default is 5 seconds.

Format: `peer-keepalive timeout` *`value`*

Command mode: VPC Config

no peer-keepalive timeout

This command resets the keepalive timeout to the default value of 5 seconds.

Format: `no keepalive timeout`

Command mode: VPC Config

role priority

This command configures VPC switch priority. This value is used for VPC role selection. The priority value is sent to the peer in the VPC keepalive messages. The VPC switch with lower priority becomes the Primary and the switch with higher priority becomes the Secondary. If both VPC peer switches have the same role priority, the device with the lower system MAC address becomes the Primary.

The keepalive state machine is not restarted even if the keepalive priority is modified post-election.

The priority can be between 1 and 255 seconds.

Default: 100.

Format: `role priority` *`value`*

Command mode: VPC Config

no role priority

This command resets the keepalive priority and timeout to the default value of 100.

Format: `no role priority`

Command mode: VPC Config

system-mac

Use this command to manually configure the MAC address for the VPC domain. The VPC MAC address should be configured same on both the peer devices. The specified MAC address should be a unicast MAC address in

<aa:bb:cc:dd:ee:ff> format and cannot be equal to the MAC address of either the primary VPC or secondary VPC device. The configured VPC MAC address is exchanged during role election and, if they are configured differently on the peer devices, VPC does not become operational.

The *mac-address* is used in the LACP PDUs and STP BPDUs that are sent out on VPC member ports, if VPC primary device election takes place after the VPC MAC address is configured. When the VPC MAC address is configured after the VPC primary device is elected, the operational VPC MAC address is used in the LACP PDUs and STP BPDUs instead of the configured VPC MAC address.

Format: `system-mac` *`mac-address`*

Command mode: VPC Domain

no system-mac

This command unconfigures the manually configured VPC MAC address for the VPC domain.

Format: `no system-mac`

Command mode: VPC Domain

system-priority

Use this command to manually configures a system priority for the VPC domain. The *system-priority* should be configured identically on both VPC peers. If the configured VPC system priority is different on VPC peers, the VPC will not come up.

The *system-priority* is used in the LACP PDUs that are sent out on VPC member ports if VPC primary device election takes place after the VPC system priorities are configured. When the VPC system priority is configured after the VPC primary device is elected, the operational VPC system priority is used in the LACP PDUs instead of the configured VPC system priority.

The configurable range is 1 to 65535.

Default: 32767.

Format: `system-priority` *priority*

Command mode: VPC Domain

no system-priority

This command restores the VPC system priority to the default value.

Format: `no system-priority` *priority*

Command mode: VPC Domain

vpc

This command configures a port-channel (LAG) as part of an VPC. Upon issuing this command, the port- channel is down until the port-channel member information is exchanged and agreed between the VPC peer switches.

The configurable range for the VPC id 1 to (Max number of LAG interfaces (64) -1).

Default: none

Format: `vpc` *id*

Command mode: LAG interface

no vpc

This command unconfigures a port-channel as VPC.

Format: `no vpc` *id*

Command mode: LAG interface

vpc peer-link

This command configures a port channel as the VPC peer link.

Format: `vpc peer-link`

Command mode: LAG interface

no vpc peer-link

This command unconfigures a port channel as the VPC peer link.

Format: `no vpc peer-link`

Command mode: LAG interface

show running-config vpc

Use this command to display running configuration information for virtual port channels (VPC).

Format: `show running-config vpc`

Command mode: Privileged

show vpc

This command displays information about an VPC. The configuration and operational modes of the VPC are displayed; the VPC is operationally enabled if all the preconditions are met. The port-channel that is configured as an VPC interface is also displayed with the member ports on the current switch and peer switch (with their link status).

Format: `show vpc` *id*

Command mode: User

show vpc brief

This command displays the VPC global status and current VPC operational mode (the VPC is in operational mode if the preconditions are met). The *peerlink* and *keepalive* statuses as well as the number of configured and operational VPCs and the system MAC and role are displayed.

Format: `show vpc brief`

Command mode: Privileged

show vpc consistency-parameters

Use this command to display global consistency parameters and LAG interface consistency parameters for virtual port channels (VPC) on the switch.

Format: `show vpc consistency-parameters {global | interface lag` *lag-id*`}`

Command mode: Privileged

show vpc peer-keepalive

This command displays the peer VPC switch IP address used by the dual control plane detection protocol. The port used for the DCPDP is shown. This command also displays if peer detection is enabled. If enabled, the detection status is displayed. The DCPDP message transmission interval and reception timeout are also displayed.

Format: `show vpc peer-keepalive`

Command mode: User

show vpc role

This command displays information about the keepalive status and parameters. The role of the VPC switch as well as the system MAC address and priority are displayed.

Format: `show vpc role`

Command mode: User

show vpc statistics

This command displays counters for the keepalive messages transmitted and received by the VPC switch.

Format: `show vpc statistics {peer-keepalive | peer-link}`

Command mode: User

clear vpc statistics

This command clears all the keepalive statistics.

Format: `clear vpc statistics {peer-keepalive | peer-link}`

Command mode: User

debug vpc peer-keepalive

This command enables debug traces of the keepalive state machine transitions.

Format: `debug vpc peer-keepalive`

Command mode: User

debug vpc peer-link data-message

This command enables debug traces for the control messages exchanged between the VPC devices on the peer link.

Format: `debug vpc peer-link data-message`

Command mode: User

debug vpc peer-link control-message async

This command enables debug traces for the asynchronous reliable control messages exchanged between the MLAG devices on the peer link. For error, only the errors in the communication are traced. For msg, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format: `debug vpc peer-link control-message async {error | msg [receive | transmit]}`

Command mode: User

debug vpc peer-link control-message bulk

This command enables debug traces for the periodic control messages exchanged between the MLAG devices on the peer link. For error, only the errors in the communication are traced. For msg, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format: `debug vpc peer-link control-message bulk {error | msg [receive | transmit]}`

Command mode: User

debug vpc peer-link control-message ckpt

This command enables debug traces for the checkpointing control messages exchanged between the MLAG devices on the peer link. For *error*, only the errors in the communication are traced. For *msg*, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format: `debug vpc peer-link control-message ckpt {error | msg [receive | transmit]}`

Command mode: User

debug vpc peer detection

This command enables debug traces for the dual control plane detection protocol. Traces are seen when the DCPDP transmits or receives detection packets to or from the peer VPC switch.

Format: `debug vpc peer detection`

Command mode: User

9.25 Port Mirroring configuration commands

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

monitor session source

The commands described below add a mirrored port (source port) to a session identified with *session-id*. The *session-id* parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is 7. Use the *source interfaceunit/slot/port* parameter to specify the interface to monitor. Use rx to monitor only ingress packets, or use tx to monitor only egress packets. If you do not specify an {rx | tx} option, the destination port monitors both ingress and egress packets.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored).

Remote port mirroring can be configured with the remote vlan vlan-id parameter.

The source and destination cannot be configured as remote on the same device.

If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLANand this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

If you specify a VLAN interface as the source, TX traffic from the switch CPU will not be mirrored on that VLAN. To mirror this traffic, you should specify the CPU interface as the source port (`monitor session-id source interface cpu`).

Default: none

Format: `monitor session` *`session-id`* `source {interface {`*`unit/slot/port`* `| cpu | lag } | vlan` *`vlan- id`* `| remote vlan` *`vlan-id`* `}[{rx | tx}]`

Command mode: Global Config

no monitor session source

This command removes the specified mirrored port from the selected port mirroring session.

Default: none

Format: `no monitor session` *`session-id`* `source {interface {`*`unit/slot/port`* `| cpu | lag } | vlan| remote vlan}`

Command mode: Global Config

monitor session destination

The commands described below add a mirrored port (source port) to a session identified with *session-id*. The *session-id* parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is 7. Use the destination interface *unit/slot/port* to specify the interface to receive the monitored traffic.

Remote port mirroring is configured by giving the RSPAN VLAN ID. Remote RSPAN mirroring can be configured with the *remote vlan vlan-id* parameter.

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.

This port must be configured with RSPAN VLAN membership.

On the intermediate switch: RSPAN VLAN should be created, the ports connected towards Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on the interface on the intermediate switch connected towards the Destination switch.

Default: none

Format: `monitor session` *`session-id`* `destination {interface` *`unit/slot/port`* `|remote vlan` *`vlan- id`* `reflector-port` *`unit/slot/port`*`}`

Command mode: Global Config

no monitor session destination

This command removes the specified probe port from the selected port mirroring session.

Format: `no monitor session` *`session-id`* `destination {interface` *`unit/slot/port`* `|remote vlan` *`vlan- id`* `reflector-port` *`unit/slot/port`*`}`

Command mode: Global Config

monitor session filter

This command attaches an IP/MAC ACL to a selected monitor session defined as *session-id*. Use the *filter* parameter to filter a specified access group either by IP address or MAC address.

An IP/MAC ACL can be attached to a session by giving the access list number/name.

Default: none

Format: `monitor session` *`session-id`* `filter {ip access-group` *`acl-id/aclname`* `| mac access-group` *`acl-name`*`}`

Command mode: Global Config

no monitor session filter

This command removes the specified IP/MAC ACL from the selected monitoring session.

Format: `no smonitor session` *`session-id`* `filter {ip access-group | mac access-group }`

Command mode: Global Config

monitor session mode

This command enables the selected port mirroring session.

Default: none

Format: `monitor session session-id mode`

Command mode: Global Config

no monitor session mode

This command disables the selected port mirroring session.

Format: no monitor session *session-id* mode

Command mode: Global Config

no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs and set the value to default.

Format: no monitor session *session-id*

Command mode: Global Config

no monitor

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

This is a stand-alone "no" command. This command does not have a "normal" form.

Default: none

Format: `no monitor`

Command mode: Global Config

show monitor session

This command displays the Port monitoring information for a particular mirroring session.

Format: `show monitor session {session-id {1-7} | all}`

Command mode: Privileged

Term	*Value*
Session ID	An integer value used to identify the session in the range of 1 to 7.
Admin Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with session-id. Possible values are: enabled and disabled
Probe Port	Probe port (destination port) for the session identified with session-id. If probe port is not set then this field is blank.
Src RVLAN	All member ports of this VLAN are mirrored. If the source VLAN is not configured, this field is blank.

Mirrored Port	The port that is configured as a mirrored port (source port) for the session identified with session-id. If no source port is configured for the session, this field is blank.
Ref. Port	This port carries all the mirrored traffic at the source switch.
Src RVLAN	The source VLAN is configured at the destination switch. If the remote VLAN is not configured, this field is blank.
Dst RVLAN	The destination VLAN is configured at the source switch. If the remote VLAN is not configured, this field is blank.
Type	The type of the mirroring packets. Possible values are: tx for transmitted packets and rx for receiving packets.
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.

show vlan remote-span

This command displays the configured RSPAN VLAN.

Format: `show vlan remote-span`

Command mode: Privileged

9.26 Static MAC Filtering configuration commands

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

macfilter

This command adds a static MAC filter entry for the MAC address macaddr on the VLAN vlanid. The value of the macaddr parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The vlanid parameter must identify a valid VLAN.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

For current platforms, you can configure the following combinations:

- Unicast MAC and source port;
- Multicast MAC and source port;
- Multicast MAC and destination port (only);
- Multicast MAC and source ports and destination ports.

Format: `macfilter` *`macaddr vlanid`*

Command mode: Global Config

no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address macaddr on the VLAN vlanid. The value of the macaddr parameter should be defined as a 6-bit hexadecimal number in the b1:b2:b3:b4:b5:b6 format.

The *vlanid* parameter must identify a valid VLAN.

Format: no macfilter *macaddr vlanid*

Command mode: Global Config

macfilter adddest

Use this command to add the interface or range of interfaces to the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The value of the *macaddr* parameter should be defined as a 6-bit hexadecimal number in the b1:b2:b3:b4:b5:b6 format. The vlanid parameter must identify a valid VLAN.

Configuring a destination port list is only valid for multicast MAC addresses.

Format: `macfilter adddest` *macaddr*

Command mode: Interface Config

no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given macaddr and VLAN of vlanid. The value of the macaddr parameter should be defined as a 6-bit hexadecimal number in the b1:b2:b3:b4:b5:b6 format. The vlanid parameter must identify a valid VLAN.

Format: `no macfilter adddest` *macaddr*

Command mode: Interface Config

macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Configuring a destination port list is only valid for multicast MAC addresses.

Format: `macfilter adddest all` *macaddr*

Command mode: Global Config

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The value of the *macaddr* parameter should be defined as a 6-bit hexadecimal number in the b1:b2:b3:b4:b5:b6 format. The vlanid parameter must identify a valid VLAN.

Format: `no macfilter adddest all` *macaddr*

Command mode: Global Config

macfilter addsrc

This command adds the interface or range of interfaces to the source filter set for the MAC filter with the MAC address of macaddr and VLAN of vlanid. The value of the macaddr parameter should be defined as a 6-bit hexadecimal number in the b1:b2:b3:b4:b5:b6 format. The vlanid parameter must identify a valid VLAN.

Format: `macfilter addsrc macaddr vlanid`

Command mode: Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. The value of the macaddr parameter should be defined as a 6-bit hexadecimal number in the b1:b2:b3:b4:b5:b6 format. The *vlanid* parameter must identify a valid VLAN.

Format: no macfilter addsrc *macaddr vlanid*

Command mode: Interface Config

macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and *vlanid*. You must specify the *macaddr* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The vlanid parameter must identify a valid VLAN.

Format: `macfilter addsrc all macaddr vlanid`

Command mode: Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. You must specify the macaddr parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *vlanid* parameter must identify a valid VLAN.

Format: no `macfilter addsrc all macaddr vlanid`

Command mode: Global Config

show mac-address-table static

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

Format: `show mac-address-table static {macaddr vlanid | all}`

Command mode: Privileged

Term	*Value*
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set's slot and port(s).

Only multicast address filters will have destination port lists.

show mac-address-table staticfiltering

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

Format: `show mac-address-table staticfiltering`

Command mode: Privileged

Term	*Value*
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. 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.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

9.27 DHCP L2 Relay Agent configuration commands

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

dhcp l2relay

This command enables the DHCP Layer 2 Relay agent for an interface a range of interfaces in, or all interfaces. The subsequent commands mentioned in this section can only be used when the DHCP L2 relay is enabled.

Format: `dhcp l2relay`

Command mode: Global Config
Interface Config

no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

Format: `no dhcp l2relay`

Command mode: Global Config
Interface Config

dhcp l2relay circuit-id subscription

This command sets the Option-82 Circuit ID for a given service subscription identified by *subscription-string* on a given interface. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When *circuit-id* is enabled using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 circuit-id as the incoming interface number.

Default: disabled

Format: `dhcp l2relay circuit-id subscription subscription-string`

Command mode: Interface Config

no dhcp l2relay circuit-id subscription

This command resets the Option-82 Circuit ID for a given service subscription identified by *subscription-string* on a given interface.

Format: `no dhcp l2relay circuit-id subscription` *`subscription-string`*

Parameter	***Description***
vlan–list	The identifier of the VLAN. Range of values: 1–4094. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Format: `no dhcp l2relay circuit-id vlan` *`vlan-list`*

Command mode: Global Config

dhcp l2relay remote-id subscription

This command sets the Option-82 *Remote-ID* string for a given service subscription identified by subscription-string on a given interface or range of interfaces. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. The *remoteid-string* is a character string. When *remote-id* string is set using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 *Remote-id* as the configured *remote-id* string.

Default: empty string

Format: `dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*

Command mode: Interface Config

no dhcp l2relay remote-id subscription

This command resets the Option-82 Remote-ID string for a given service subscription identified by subscription-string on a given interface.

Format: `no dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*

Command mode: Interface Config

Parameter	***Description***

vlan–list	The identifier of the VLAN. Range of values: 1–4094. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay remote-id vlan

This parameter clears the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format: `no dhcp l2relay remote-id vlan` *`vlan-list`*

Command mode: Global Config

dhcp l2relay subscription

This command enables relaying DHCP packets on an interface or range of interfaces that fall under the specified service subscription. The *subscription-string* is a character string that needs to be matched with configured DOT1AD subscription string for correct operation.

Default: disabled (i.e. no DHCP packets are relayed)

Format: `dhcp l2relay subscription-name` *`subscription-string`*

Command mode: Interface Config

no dhcp l2relay subscription

This command disables relaying DHCP packets on the interface or range of interfaces that fall under the specified service subscription.

Format: `no dhcp l2relay subscription-name` *`subscription-string`*

Command mode: Interface Config

dhcp l2relay trust

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

Default: untrusted
Format: `dhcp l2relay trust`

Command mode: Interface Config

no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format: `no dhcp l2relay trust`

Command mode: Interface Config

dhcp l2relay vlan

Use this command to enable the DHCP L2 Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default: disabled

Format: `dhcp l2relay vlan` *`vlan-list`*

Command mode: Global Config

dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription- name).

Format: `dhcp l2relay remote-id` *`remote-id-string`* `vlan` *`vlan-list`*

Command mode: Global Config

Parameter	*Description*
vlan–list	The identifier of the VLAN. Range of values: 1–4094. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay vlan

Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Format: `no dhcp l2relay vlan` *`vlan-list`*

Command mode: Global Config

show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Format: `show dhcp l2relay all`

Command mode: Privileged

show dhcp l2relay circuit-id vlan

This command displays DHCP circuit-id vlan configuration.

Format: `show dhcp l2relay circuit-id vlan` *`vlan-list`*

Command mode: Privileged
Interface Config

dhcp l2relay circuit-id vlan

This parameter sets the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format: `dhcp l2relay circuit-id vlan` *`vlan-list`*

Command mode: Global Config

Parameter	*Description*
vlan–list	VLAN identifier in the range form 1 to 4094. Use a hyphen (-) for a range or a comma (,) to separate individual VLAN IDs. Spaces and zeros are not permitted.

show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Format: `show dhcp l2relay interface {all | ` *`interface-num`*`}`

Command mode: Privileged

show dhcp l2relay remote-id vlan

This command displays DHCP Remote-id vlan configuration.

Format: `show dhcp l2relay remote-id vlan` *vlan-list*

Command mode: Privileged

Parameter	*Description*
vlan–list	VLAN identifier in the range form 1 to 4094. Use a hyphen (-) for a range or a comma (,) to separate individual VLAN IDs. Spaces and zeros are not permitted.

show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Format: `show dhcp l2relay stats interface {all | interface-num}`

Command mode: Privileged

show dhcp l2relay subscription interface

This command displays DHCP L2 Relay configuration specific to a service subscription on an interface.

Format: `show dhcp l2relay subscription interface {all|interface-num}`

Command mode: Privileged

show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format: `show dhcp l2relay agent-option vlan vlan-range`

Command mode: Privileged

show dhcp l2relay vlan

This command displays DHCP vlan configuration.

Format: `show dhcp l2relay vlan vlan-list`

Command mode: Privileged

Parameter	*Description*
vlan–list	VLAN identifier in the range form 1 to 4094. Use a hyphen (-) for a range or a comma (,) to separate individual VLAN IDs. Spaces and zeros are not permitted.

clear dhcp l2relay statistics interface

Use this command to reset the DHCP L2 relay counters to zero. Specify the port with the counters to clear, or use the all keyword to clear the counters on all ports.

Format: `clear dhcp l2relay statistics interface {unit/slot/port | all}`

Command mode: Privileged

9.28 DHCP Client configuration commands

The system can include vendor and configuration information in DHCP client requests relayed to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

dhcp client vendor-id-option

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the switch.

Format: `dhcp client vendor-id-option` *`string`*

Command mode: Global Config

no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the switch.

Format: `no dhcp client vendor-id-option`

Command mode: Global Config

dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the switch.

Format: `dhcp client vendor-id-option-string` *`string`*

Command mode: Global Config

no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format: `no dhcp client vendor-id-option-string`

Command mode: Global Config

show dhcp client vendor-id-option

This command displays the configured administration mode of the VendorID Option and the VendorID String to be included in Option-60 in DHCP requests.

Format: `show dhcp client vendor-id-option`

Command mode: Privileged

9.29 DHCP Snooping configuration commands

This section describes commands you use to configure DHCP Snooping.

ip dhcp snooping

Use this command to enable DHCP Snooping globally.

Default: disabled

Format: `ip dhcp snooping`

Command mode: Global Config

no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Format: `no ip dhcp snooping`

Command mode: Global Config

ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default: disabled

Format: `ip dhcp snooping vlan` *`vlan-list`*

Command mode: Global Config

no ip dhcp snooping vlan

Use this command to disable DHCP snooping on the specified VLANs.

Format: `no ip dhcp snooping vlan` *`vlan-list`*

Command mode: Global Config

ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default: enabled

Format: `ip dhcp snooping verify mac-address`

Command mode: Global Config

no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format: `no ip dhcp snooping verify mac-address`

Command mode: Global Config

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.

Default: local

Format: `ip dhcp snooping database {local|tftp://hostIP/filename}`

Command mode: Global Config

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.

Default: 300 seconds

Format: `ip dhcp snooping database write-delay in seconds`

Command mode: Global Config

no ip dhcp snooping database write-delay

Use this command to set the *write delay* value to the default value.

Format: `no ip dhcp snooping database write-delay`

Command mode: Global Config

ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format: `ip dhcp snooping binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Command mode: Global Config

no ip dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format: `no ip dhcp snooping binding` *`mac-address`*

Command mode: Global Config

ip dhcp filtering trust

Use this command to enable trusted mode on the interface if the previously saved configuration or applied script contains this command.

Format: `ip dhcp filtering trust` *`interface id`*

Command mode: Global Config

no ip dhcp filtering trust

Use this command to disable trusted mode on the interface.

Format: `no ip dhcp filtering trust` *`interface id`*

Command mode: Global Config

ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format: `ip verify binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Command mode: Global Config

no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

Format: `no ip verify binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Command mode: Global Config

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.

Default: disabled (no limit)

Format: `ip dhcp snooping limit {rate pps [`*`burst interval seconds`*`]}`

Command mode: Interface Config

no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format: `no ip dhcp snooping limit`

Command mode: Interface Config

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.

Default: disabled

Format: `ip dhcp snooping log-invalid`

Command mode: Interface Config

no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format: `no ip dhcp snooping log-invalid`

Command mode: Interface Config

ip dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default: disabled

Format: `ip dhcp snooping trust`

Command mode: Interface Config

no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format: no ip dhcp snooping trust

Command mode: Interface Config

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.

Default: the source ID is the IP address

Format: `ip verify source {port-security}`

Command mode: Interface Config

no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable *port-security* alone if it is configured.

Format: `no ip verify source`

Command mode: Interface Config

show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format: `show ip dhcp snooping`

Command mode: Privileged

User

Term	*Value*
Interface	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.

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.

Format: `show ip dhcp snooping binding [{static/dynamic}] [interface unit/slot/port] [vlan id]`

Command mode: Privileged

User

Term	*Value*
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 (sec)	The remaining lease time for the entry.

show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistence.

Format: `show ip dhcp snooping database`

Command mode: Privileged
User

Term	*Value*
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

show ip dhcp snooping interfaces

Use this command to show the DHCP Snooping status of the interfaces.

Format: `show ip dhcp snooping interfaces`

Command mode: Privileged

show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format: `show ip dhcp snooping statistics`

Command mode: Privileged
User

Term	*Value*
Interface	The IP address of the interface in *unit/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 HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format: `clear ip dhcp snooping binding [interface unit/slot/port]`

Command mode: Privileged

User

clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format: `clear ip dhcp snooping statistics`

Command mode: Privileged
User

show ip verify source

Use this command to display the IPSG configurations on all ports.

Format: `show ip verify source`

Command mode: Privileged
User

Term	*Value*
Interface	The IP address of the interface in *unit/slot/port* format.
Filter Type	Is one of two values: • ip-mac: User has configured IP and MAC address filtering on this interface. • ip: Only IP address filtering on this interface.
IP Address	IP 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.

show ip verify interface

Use this command to display the IPSG filter type for a specific interface.

Format: `show ip verify interface unit/slot/port`

Command mode: Privileged
User

Term	*Value*
Interface	The IP address of the interface in *unit/slot/port* format.
Filter Type	Is one of two values: • ip-mac: User has configured IP and MAC address filtering on this interface. • ip: Only IP address filtering on this interface.

show ip source binding

Use this command to display the IPSG bindings.

Format: `show ip source binding [{dhcp-snooping|static}] [interface unit/slot/port] [vlan id]`

Command mode: Privileged
User

Term	*Value*
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 unit/slot/port format.

9.30 Dynamic ARP Inspection configuration commands

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

ip arp inspection vlan

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default: disabled

Format: `ip arp inspection vlan vlan-list`

Command mode: Global Config

no ip arp inspection vlan

Use this command to disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Format: `no ip arp inspection vlan vlan-list`

Command mode: Global Config

ip arp inspection validate

Use this command to enable additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables src-mac and dst-mac validations, and a second command enables IP validation only, the src-mac and dst-mac validations are disabled as a result of the second command.

Default: disabled

Format: `ip arp inspection validate {[src-mac] [dst-mac] [ip]}`

Command mode: Global Config

no ip arp inspection validate

Use this command to disable the additional validation checks on the received ARP packets.

Format: `no ip arp inspection validate {[src-mac] [dst-mac] [ip]}`

Command mode: Global Config

ip arp inspection vlan logging

Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default: enabled

Format: `ip arp inspection vlan vlan-list logging`

Command mode: Global Config

no ip arp inspection vlan logging

Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format: `no ip arp inspection vlan vlan-list logging`

Command mode: Global Config

ip arp inspection trust

Use this command to configure an interface or range of interfaces as trusted for Dynamic ARP Inspection.

Default: enabled

Format: `ip arp inspection trust`

Command mode: Interface Config

no ip arp inspection trust

Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format: `no ip arp inspection trust`

Command mode: Interface Config

ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface or range of interfaces. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections. The maximum pps value shown in the range for the rate option might be more than the hardware allowable limit. Therefore you need to understand the switch performance and configure the maximum rate pps accordingly.

The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.

Default: 15 pps for rate and 1 second for burst-interval

Format: `ip arp inspection limit {rate pps [burst interval seconds] | none}`

Command mode: Interface Config

no ip arp inspection limit

Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format: `no ip arp inspection limit`

Command mode: Interface Config

ip arp inspection filter

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Default: No ARP ACL is configured on a VLAN

Format: `ip arp inspection filter acl-name vlan vlan-list [static]`

Command mode: Global Config

no ip arp inspection filter

Use this command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format: `no ip arp inspection filter acl-name vlan vlan-list [static]`

Command mode: Global Config

arp access-list

Use this command to create an ARP ACL.

Format: `arp access-list acl-name`

Command mode: Global Config

no arp access-list

Use this command to delete a configured ARP ACL.

Format: `no arp access-list acl-name`

Command mode: Global Config

permit ip host mac host

Use this command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format: `permit ip host` *`sender-ip`* `mac host` *`sender-mac`*

Command mode: ARP Access-list Config

no permit ip host mac host

Use this command to delete a rule for a valid IP and MAC combination.

Format: `no permit ip host sender-ip mac host sender-mac`

Command mode: ARP Access-list Config

show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the vlan-list argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the source mac validation, destination mac validation and invalid IP validation information.

Format: `show ip arp inspection [{interfaces` *`unit/slot/port`*`| vlan` *`vlan-list`*`]`

Command mode: Privileged
User

Term	*Value*
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is 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 packets 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.

show ip arp inspection statistics

Use this command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format: `show ip arp inspection statistics [vlan vlan-list]`

Command mode: Privileged
User

Term	*Value*
VLAN	The VLAN ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

clear ip arp inspection statistics

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Default: none

Format: `clear ip arp inspection statistics`

Command mode: Privileged

show ip arp inspection interfaces

Use this command to display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a *unit/slot/port* interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format: `show ip arp inspection interfaces [unit/slot/port]`

Command mode: Privileged
User

Term	*Value*
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is 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.

show arp access-list

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format: `show arp access-list [acl-name]`

Command mode: Privileged
User

9.31 IGMP Snooping configuration commands

This section describes the commands you use to configure IGMP snooping. The software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

This note clarifies the prioritization of 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.

set igmp

This command enables IGMP Snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum ERROR.

- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default: disabled

Format: `set igmp [vlan_id]`

Command mode: Global Config
Interface Config
VLAN Config

no set igmp

This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN.

Format: `no set igmp [vlan_id]`

Command mode: Global Config
Interface Config
VLAN Config

set igmp header-validation

This command enables header validation for IGMP messages. When header validation is enabled, IGMP Snooping checks:

- The time-to-live (TTL) field in the IGMP header and drops packets where TTL is not equal to 1. The TTL field should always be set to 1 in the headers of IGMP reports and queries.
- The presence of the router alert option (9404) in the IP packet header of the IGMPv2 message and drops packets that do not include this option.
- The presence of the 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.

Default: enabled

Format: `set igmp header-validation`

Command mode: Global Config

no set igmp header-validation

This command disables header validation for IGMP messages.

Format: `no set igmp header-validation`

Command mode: Global Config

set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port- channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default: disabled

Format: `set igmp interfacemode`

Command mode: Global Config

no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format: `no set igmp interfacemode`

Command mode: Global Config

set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface, a range of interfaces, or a VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default: disabled

Format: `set igmp fast-leave [vlan_id]`

Command mode: Interface Config
Interface Range Config
VLAN Config

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format: `no set igmp fast-leave [vlan_id]`

Command mode: Interface Config
Interface Range Config
VLAN Config

set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface, a range of interfaces, or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default: 260 seconds

Format: `set igmp groupmembership-interval [vlan_id] 2-3600`

Command mode: Interface Config
Global Config
VLAN Config

no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format: `no set igmp groupmembership-interval [vlan_id]`

Command mode: Interface Config
Global Config
VLAN Config

set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default: 10 seconds

Format: `set igmp maxresponse [vlan_id] 1-25`

Command mode: Global Config
Interface Config
VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format: `no set igmp maxresponse [vlan_id]`

Command mode: Global Config
Interface Config
VLAN Config

set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

Default: 0

Format: `set igmp mcrtrexpiretime [vlan_id] 0-3600`

Command mode: Global Config
Interface Config
VLAN Config

no set igmp mcrtrexpiretime

Use this 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.

Format: `no set igmp mcrtrexpiretime [vlan_id]`

Command mode: Global Config
Interface Config
VLAN Config

set igmp mrouter

This command configures the VLAN ID (*vlan_id*) that has the multicast router mode enabled.

Format: `set igmp mrouter vlan_id`

Command mode: Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (*vlan_id*).

Format: `no set igmp mrouter vlan_id`

Command mode: Interface Config

set igmp mrouter interface

This command configures the interface or range of interfaces as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default: disabled

Format: `set igmp mrouter interface`

Command mode: Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format: `no set igmp mrouter interface`

Command mode: Interface Config

set igmp report-suppression

Use this command to 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.

Default: disabled

Format: `set igmp report-suppression vlan-id`

Command mode: VLAN Config

Parameter	*Description*
vlan-id	A valid VLAN identifier. Valid values: 1 to 4094.

no set igmp report-suppression

Use this command to return the system to the default.

Format: `no set igmp report-suppression`

Command mode: VLAN Config

show igmpsnooping

This command displays IGMP Snooping information for a given *unit/slot/port* or VLAN. Configured information is displayed whether or not IGMP Snooping is enabled.

Format: `show igmpsnooping [unit/slot/port | vlan_id]`

Command mode: Privileged

When the optional arguments *unit/slot/port* or *vlan_id* are not used, the command displays the following information:

Term	*Value*
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the *unit/slot/port* values, the following information appears:

Term	*Value*
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlan_id*, the following information appears:

Term	*Value*
VLAN ID	The identifier of the VLAN.
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 amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Maximum Response Time (secs)	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time (secs)	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.
Report Suppression Mode	Indicates whether IGMP reports suppression is enabled or not.

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format: `show igmpsnooping mrouter interface` *`unit/slot/port`*

Command mode: Privileged

Term	*Value*
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.

show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format: `show igmpsnooping mrouter vlan` *`unit/slot/port`*

Command mode: Privileged

Term	*Value*
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping ssm

This command displays information about Source Specific Multicasting (SSM) by entry, group, or statistics. SSM is only available with IGMPv3 and MLDv2.

Format: `show igmpsnooping ssm {entries | groups | stats}`

Command mode: Privileged

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format: `show mac-address-table igmpsnooping`

Command mode: Privileged

Term	*Value*
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

9.32 IGMP Snooping Querier configuration commands

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

This note clarifies the prioritization of 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.

set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default: disabled

Format: `set igmp querier [vlan-id] [address ipv4_address]`

Command mode: Global Config
VLAN Mode

no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional address parameter to reset the querier address to 0.0.0.0.

Format: `no set igmp querier [vlan-id] [address]`

Command mode: Global Config
VLAN Mode

set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default: 60

Format: `set igmp querier query-interval 1-1800`

Command mode: Global Config

no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format: `no set igmp querier query-interval`

Command mode: Global Config

set igmp querier timer expiry

Use this command to 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.

Default: 125 seconds

Format: `set igmp querier timer expiry` *`60-300`*

Command mode: Global Config

no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format: `no set igmp querier timer expiry`

Command mode: Global Config

set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default: 1

Format: `set igmp querier version` *`1-2`*

Command mode: Global Config

no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format: `no set igmp querier version`

Command mode: Global Config

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.

Default: disabled

Format: `set igmp querier election participate`

Command mode: VLAN Config

no set igmp querier election participate

Use this 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.

Format: `no set igmp querier election participate`

Command mode: VLAN Config

show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping is enabled.

Format: `show igmpsnooping querier [{detail | vlan vlanid}]`

Command mode: Privileged

When the optional argument *vlanid* is not used, the command displays the following information.

Term	*Value*
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.
Expiry Interval	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.

Term	*Value*
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.

9.33 MLD Snooping configuration 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.

This note clarifies the prioritization of 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.

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.

MLD Snooping supports the following activities:

- Validation of address version, payload length consistencies and discarding of the frame upon error.
- Maintenance of the forwarding table entries based on the MAC address versus the IPv6 address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default: disabled

Format: `set mld vlanid`

Command mode: Global Config
Interface Config
VLAN Mode

no set mld

Use this command to disable MLD Snooping on the system.

Format: set mld *vlanid*

Command mode: Global Config
Interface Config
VLAN Mode

set mld interfacemode

Use this command to enable MLD Snooping on all interfaces. 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.

Default: disabled

Format: `set mld interfacemode`

Command mode: Global Config

no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Format: `no set mld interfacemode`

Command mode: Global Config

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.

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 connectedto the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group.

Default: disabled

Format: `set mld fast-leave` *`vlanid`*

Command mode: Interface Config
VLAN Mode

no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface.

Format: `no set mld fast-leave` *`vlanid`*

Command mode: Interface Config
VLAN Mode

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.

Default: 260 seconds

Format: `set mld groupmembership-interval` *`vlanid 2-3600`*

Command mode: Interface Config
Global Config
VLAN Mode

no set groupmembership-interval

Use this command to set the MLDv2 Group Membership Interval time to the default value.

Format: `no set mld groupmembership-interval`

Command mode: Interface Config
Global Config
VLAN Mode

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.

Default: 10 seconds

Format: `set mld maxresponse` *`1-65`*

Command mode: Global Config
Interface Config
VLAN Mode

no set mld maxresponse

Use this command to set the max response time (on the interface or VLAN) to the default value.

Format: `no set mld maxresponse`

Command mode: Global Config
Interface Config
VLAN Mode

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.

Default: 0

Format: `set mld mcrtexpiretime` *`vlanid 0-3600`*

Command mode: Global Config
Interface Config

no set mld mcrtexpiretime

Use this 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.

Format: `no set mld mcrtexpiretime` *`vlanid`*

Command mode: Global Config
Interface Config

set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format: `set mld mrouter vlanid`

Command mode: Interface Config

no set mld mrouter

Use this command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

Format: `no set mld mrouter vlanid`

Command mode: Interface Config

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.

Default: disabled

Format: `set mld mrouter interface`

Command mode: Interface Config

no set mld mrouter interface

Use this command to disable the status of the interface as a statically configured multicast router-attached interface.

Format: `no set mld mrouter interface`

Command mode: Interface Config

show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Format: `show mldsnooping [unit/slot/port | vlanid]`

Command mode: Privileged

When the optional arguments *unit/slot/port* or *vlanid* are not used, the command displays the following information.

Term	*Value*
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 *unit/slot/port* values, the following information appears:

Term	*Value*

MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the interface.
Fast Leave Mode	Indicates 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:

Term	***Value***
VLAN Admin Mode	Indicates whether MLD Snooping is active on the VLAN.

show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

Format: `show mldsnooping mrouter interface` *`unit/slot/port`*

Command mode: Privileged

Term	***Value***
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.

show mldsnooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

Format: `show mldsnooping mrouter vlan` *`unit/slot/port`*

Command mode: Privileged

Term	***Value***
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show mldsnooping ssm entries

Use this command to display the source specific multicast forwarding database built by MLD snooping.

A given {Source, Group, VLAN} combination can have few interfaces in INCLUDE mode and few interfaces in EXCLUDE mode. In such instances, two rows for the same {Source, Group, VLAN} combinations are displayed.

Format: `show mldsnooping ssm entries`

Command mode: Privileged

Term	*Value*
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. 1) If Source Filter Mode is “Include,” specifies the list of interfaces on which a 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 a 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.
Interfaces	Shows the list of interfaces on which the incoming packet is routing.

show mldsnooping ssm stats

Use this command to display the statistics of MLD snooping’s SSMFDB. This command takes no options.

Format: `show mldsnooping ssm stats`

Command mode: Privileged

Term	*Value*
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.

show mldsnooping ssm groups

Use this command to display the MLD SSM group membership information.

Format: `show mldsnooping ssm groups`

Command mode: Privileged

Term	*Value*
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.

show mac-address-table mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format: `show mac-address-table mldsnooping`

Command mode: Privileged

Term	*Value*
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:).

clear mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

Format: clear mldsnooping

Command mode: Privileged

9.34 MLD Snooping Querier configuration 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.

This note clarifies the prioritization of 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.

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.

Default: disabled

Format: `set mld querier [vlan-id] [address ipv6_address]`

Command mode: Global Config
VLAN Mode

no set mld querier

Use this command to disable MLD Snooping Querier on the system. Use the optional parameter address to reset the querier address.

Format: `no set mld querier [vlan-id][address]`

Command mode: Global Config
VLAN Config

set mld querier query_interval

Use this command to set the MLD Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default: 60 seconds

Format: `set mld querier query_interval 1-1800`

Command mode: Global Config

no set mld querier query_interval

Use this command to set the MLD Querier Query Interval time to its default value.

Format: `no set mld querier query_interval`

Command mode: Global Config

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.

Default: 60 seconds

Format: `set mld querier timer expiry` *`60-300`*

Command mode: Global Config

no set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period to its default value.

Format: `no set mld querier timer expiry`

Command mode: Global Config

set mld 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.

Default: disabled

Format: `set mld querier election participate`

Command mode: VLAN Config

no set mld querier election participate

Use this 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.

Format: `no set mld querier election participate`

Command mode: VLAN Config

show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Format: `show mldsnooping querier [{detail | vlan` *`vlanid`*`}]`

Command mode: Privileged

When the optional arguments *vlandid* are not used, the command displays the following information.

Term	***Value***
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	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 information appears:

Term	***Value***
VLAN Admin Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates 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 IPv4 header while sending out MLD queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The 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.

When the optional argument *detail* is used, the command shows the global information and the information for all Querier-enabled VLANs.

9.35 Port Security configuration 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.

To enable the SNMP trap specific to port security, see the snmp-server enable traps violation command.

port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default: disabled

Format: `port-security`

Command mode: Global Config (to enable port locking globally)
Interface Config (to enable port locking on an interface or range of interfaces)

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format: `no port-security`

Command mode: Global Config
Interface Config

port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port. Valid value range: 0–600.

Default: 600

Format: `port-security max-dynamic` *`maxvalue`*

Command mode: Interface Config

no port-security max-dynamic

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

Format: `no port-security max-dynamic`

Command mode: Interface Config

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port. Valid value range: 0–20.

Default: 1

Format: `port-security max-static` *`maxvalue`*

Command mode: Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format: `no port-security max-static`

Command mode: Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The *vid* is the VLAN ID.

Format: `port-security mac-address` *`mac-address vid`*

Command mode: Interface Config

no port-security mac-address

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

Format: `no port-security mac-address` *`mac-address vid`*

Command mode: Interface Config

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format: `port-security mac-address move`

Command mode: Interface Config

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.

Format: `port-security mac-address sticky [<mac-address><vid>]`

Command mode: Global Config
Interface Config

no port-security mac-address sticky

The **no** form removes the sticky mode. The sticky MAC address can be deleted by using the command *"no port- security mac-address <mac-address><vid>"*.

Format: `no port-security mac-address sticky [<mac-address><vid>]`

Command mode: Global Config
Interface Config

mac-address-table limit

This command sets the MAC limit for the corresponding vlan-id.

Default: disabled

Format: `mac-address-table limit [action shutdown] [notification trap] [maximum-num] [vlan vlan-id]`

Command mode: Global Config

Parameter	*Description*
[action shutdown]	After the MAC limit has been reached, the action will shut down the ports participating in the VLAN.
[notification trap]	Enables snmp-server enable traps violation on the ports participating in the VLAN.
[maximum-num]	MAC limit to be configured.
[vlan vlan]	VLAN on which the MAC limit is to be applied.

no mac-address-table limit

This command removes the MAC limit for the corresponding *vlan-id*.

Default: disabled

Format: `no mac-address-table limit [action shutdown] [notification trap] [maximum-num] [vlan vlan-id]`

Command mode: Global Config

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 or on all interfaces. Instead of unit/slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. Lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Format: show port-security [{*unit/slot/port* | all}]
Command mode: Privileged

Term	*Value*
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:

Term	*Value*
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	Shows, whether violation traps are enabled.
Sticky Mode	The administrative mode of the port security Sticky Mode feature on the interface.

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `show port-security dynamic` *`unit/slot/port`*

Command mode: Privileged

Term	*Value*
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for port. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `show port-security static {`*`unit/slot/port`* `|` `lag` *`lag-intf-num`*`}`

Command mode: Privileged

Parameter	*Description*
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.

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `show port-security violation {`*`unit/slot/port`* `|` `lag` *`lag-id`*`}`

Command mode: Privileged

Term	*Value*
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.

show mac-address-table limit

This command displays the VLAN port security configuration.

Format: `show mac-address-table limit [vlan-id]`

Command mode: Privileged

Term	*Value*
VLAN ID	The VLAN ID on which MAC locking has been configured.

9.36 LLDP (802.1AB) configuration commands

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

lldp transmit

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default: enabled

Format: `lldp transmit`

Command mode: Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format: `no lldp transmit`

Command mode: Interface Config

lldp receive

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default: enabled

Format: `lldp receive`

Command mode: Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format: `no lldp receive`

Command mode: Interface Config

lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *interval-seconds* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The *hold-value* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The reinit-seconds is the delay before reinitialization, and the range is 1-0 seconds.

Default: interval — 30 seconds
hold — 4 seconds
reinit—2 seconds

Format: `lldp timers [interval *interval-seconds*] [hold *hold-value*] [reinit *reinit-seconds*]`

Command mode: Global Config

no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format: `no lldp timers [interval] [hold] [reinit]`

Command mode: Global Config

lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs from an interface or range of interfaces. Use *sys-name* to transmit the system name TLV. Use *sys-desc* to transmit the system description TLV. Use *sys-cap* to transmit the system capabilities TLV. Use *port-desc* to transmit the port description TLV.

Default: no optional TLVs are included

Format: `lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Command mode: Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format: `no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Command mode: Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. This command can be used to configure a single interface or a range of interfaces.

Format: `lldp transmit-mgmt`
Command mode: Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format: `no lldp transmit-mgmt`

Command mode: Interface Config

lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default: disabled

Format: `lldp notification`

Command mode: Interface Config

no lldp notification

Use this command to disable notifications.

Default: disabled

Format: `no lldp notification`

Command mode: Interface Config

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The *interval* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default: 5

Format: `lldp notification-interval` *`interval`*

Command mode: Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format: `no lldp notification-interval`

Command mode: Global Config

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format: `clear lldp statistics`

Command mode: Privileged

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format: `clear lldp remote-data`

Command mode: Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format: `show lldp`

Command mode: Privileged

Term	*Value*
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before reinitialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format: `show lldp interface {`*`unit/slot/port`* `| all}`

Command mode: Privileged

Term	*Value*
Interface	The interface in *unit/slot/port* format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format: `show lldp statistics {`*`unit/slot/port`* `| all}`

Command mode: Privileged

Term	*Value*
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Term	*Value*
Interface	The interface in *unit/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.

show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format: `show lldp remote-device {`*`unit/slot/port`* `| all}`

Command mode: Privileged

show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format: `show lldp remote-device detail` *unit/slot/port*

Command mode: Privileged

Term	*Value*
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 alphanumeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format: `show lldp local-device {`*unit/slot/port* `|` `all}`
Command mode: Privileged

Term	*Value*
Interface	The interface in *unit/slot/port* format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format: `show lldp local-device detail` *unit/slot/port*

Command mode: Privileged

Term	*Value*
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 alphanumeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

9.37 LLDP-MED configuration commands

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

lldp med

Use this command to enable MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default: disabled

Format: `lldp med`

Command mode: Interface Config

no lldp med

Use this command to disable MED.

Format: `no lldp med`

Command mode: Interface Config

lldp med confignotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default: disabled

Format: `lldp med confignotification`

Command mode: Interface Config

no ldp med confignotification

Use this command to disable notifications.

Format: `no lldp med confignotification`

Command mode: Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from this interface or a range of interfaces.

Default: By default, the capabilities and network policy TLVs are included

Format: `lldp med transmit-tlv [capabilities] [network-policy]`

Command mode: Interface Config

Term	*Value*
capabilities	Transmit the LLDP capabilities TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format: `no lldp med transmit-tlv [capabilities] [network-policy]`

Command mode: Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports.

Format: `lldp med all`

Command mode: Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format: `lldp med confignotification all`

Command mode: Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. *[count]* is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default: 3

Format: `lldp med faststartrepeatcount [count]`

Command mode: Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format: `no lldp med faststartrepeatcount`

Command mode: Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default: By default, the capabilities and network policy TLVs are included

Format: `lldp med transmit-tlv all [capabilities] [network-policy]`

Command mode: Global Config

no lldp med transmit-tlv

Use this command to remove a TLV.

Format: `no lldp med transmit-tlv all [capabilities] [network-policy]`

Command mode: Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format: `show lldp med`

Command mode: Privileged

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. *unit/slot/port* indicates a specific physical interface. all indicates all valid LLDP interfaces.

Format: `show lldp med interface {unit/slot/port | all}`

Command mode: Privileged

show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits.

unit/slot/port indicates a specific physical interface.

Format: `show lldp med local-device detail unit/slot/port`

Command mode: Privileged

show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format: `show lldp med remote-device {`*`unit/slot/port`* `| all}`

Command mode: Privileged

Term	*Value*
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.

show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format: `show lldp med remote-device detail` *`unit/slot/port`*

Command mode: Privileged

9.38 DoS (Denial of Service) configuration commands

This section describes the commands you use to configure Denial of Service (DoS) Control. The 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.

dos-control all

This command enables Denial of Service protection checks globally.

Default: disabled

Format: `dos-control all`

Command mode: Global Config

no dos-control all

This command disables Denial of Service prevention checks globally.

Format: `no dos-control all`

Command mode: Global Config

dos-control sipdip

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control sipdip`

Command mode: Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format: `no dos-control sipdip`

Command mode: Global Config

dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If packets ingress having a TCP Header Size smaller then 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.

Default: disabled (20)

Format: `dos-control firstfrag [0-255]`

Command mode: Global Config

no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of disabled.

Format: `no dos-control firstfrag`

Command mode: Global Config

dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack 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.

Default: disabled

Format: dos-control tcpfrag

Command mode: Global Config

no dos-control tcpfrag

This command disables TCP Fragment Denial of Service protection.

Format: `no dos-control tcpfrag`

Command mode: Global Config

dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control tcpflag`

Command mode: Global Config

no dos-control tcpflag

This command disables TCP Flag Denial of Service protections.

Format: `no dos-control tcpflag`

Command mode: Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. 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.

Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which wouldrender the application inoperable.

Default: disabled

Format: `dos-control l4port`

Command mode: Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format: `no dos-control l4port`

Command mode: Global Config

dos-control smacdmac

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control smacdmac`

Command mode: Global Config

no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Format: `no dos-control smacdmac`

Command mode: Global Config

dos-control tcpport

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control tcpport`

Command mode: Global Config

no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format: `no dos-control tcpport`

Command mode: Global Config

dos-control udpport

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) DoS protection. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control udpport`

Command mode: Global Config

no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format: `no dos-control udpport`

Command mode: Global Config

dos-control tcpflagseq

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control tcpflagseq`

Command mode: Global Config

no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format: `no dos-control tcpflagseq`

Command mode: Global Config

dos-control tcpoffset

This command enables TCP Offset Denial of Service protection. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control tcpoffset`

Command mode: Global Config

no dos-control tcpoffset

This command disables TCP Offset Denial of Service protection.

Format: `no dos-control tcpoffset`

Command mode: Global Config

dos-control tcpsyn

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control tcpsyn`

Command mode: Global Config

no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format: `no dos-control tcpsyn`

Command mode: Global Config

dos-control tcpsynfin

This command enables TCP SYN and FIN Denial of Service protection. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control tcpsynfin`

Command mode: Global Config

no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format: `no dos-control tcpsynfin`

Command mode: Global Config

dos-control tcpfinurgpsh

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control tcpfinurgpsh`

Command mode: Global Config

no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format: `no dos-control tcpfinurgpsh`
Command mode: Global Config

dos-control icmpv4

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default: disabled (512)

Format: `dos-control icmpv4 [0-16376]`

Command mode: Global Config

no dos-control icmpv4

This command disables Maximum ICMPv6 Packet Size Denial of Service protections.

Format: `no dos-control icmpv4`

Command mode: Global Config

dos-control icmpv6

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default: disabled (512)

Format: `dos-control icmpv6 0-16376`

Command mode: Global Config

no dos-control icmpv6

This command disables Maximum ICMPv6 Packet Size Denial of Service protections.

Format: `no dos-control icmpv6`

Command mode: Global Config

dos-control icmpfrag

This command enables ICMP Fragment Denial of Service protection. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default: disabled

Format: `dos-control icmpfrag`

Command mode: Global Config

no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format: `no dos-control icmpfrag`

Command mode: Global Config

show dos-control

This command displays Denial of Service configuration information.

Format: `show dos-control`

Command mode: Privileged

Term	*Value*
First Fragment Mode	The administrative mode of First Fragment DoS prevention. When enabled, this causes the switch to drop packets that have a TCP header smaller then the configured Min TCP Hdr Size.
Min TCP Hdr Size	The minimum TCP header size the switch will accept if First Fragment DoS prevention is enabled.
ICMPv4 Mode	The administrative mode of ICMPv4 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 Payload Size.
Max ICMPv4 Payload Size	The maximum ICMPv4 payload size to accept when ICMPv4 DoS protection is enabled.

ICMPv6 Mode	The administrative mode of ICMPv6 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Payload Size.
Max ICMPv6 Payload Size	The maximum ICMPv6 payload size to accept when ICMPv6 DoS protection is enabled.
ICMPv4 Fragment Mode	The administrative mode of ICMPv4 Fragment DoS prevention. When enabled, this causes the switch to drop fragmented ICMPv4 packets.
TCP Port Mode	The administrative mode of TCP Port DoS prevention. When enabled, this causes the switch to drop packets that have the TCP source port equal to the TCP destination port.
UDP Port Mode	The administrative mode of UDP Port DoS prevention. When enabled, this causes the switch to drop packets that have the UDP source port equal to the UDP destination port.
SIPDIP Mode	The administrative mode of SIP=DIP DoS prevention. Enabling this causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
SMACDMAC Mode	The administrative mode of SMAC=DMAC DoS prevention. Enabling this causes the switch to drop packets that have a source MAC address equal to the destination MAC address.
TCP FIN&URG& PSH Mode	The administrative mode of TCP FIN & URG & PSH DoS prevention. Enabling this causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0.
TCP Flag & Sequence Mode	The administrative mode of TCP Flag DoS prevention. Enabling this causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0.
TCP SYN Mode	The administrative mode of TCP SYN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN set.
TCP SYN & FIN Mode	The administrative mode of TCP SYN & FIN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN and FIN set.
TCP Fragment Mode	The administrative mode of TCP Fragment DoS prevention. Enabling this causes the switch to drop 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.
TCP Offset Mode	The administrative mode of TCP Offset DoS prevention. Enabling this causes the switch to drop packets that have a TCP header Offset equal to 1.

9.39 MAC Database configuration commands

This section describes the commands you use to configure and view information about the MAC databases.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The seconds parameter must be within the range of 10 to 1,000,000 seconds.

Default: 300

Format: `bridge aging-time` *`10-1,000,000`*

Command mode: Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Format: `no bridge aging-time`

Command mode: Global Config

show forwardingdb agetime

This command displays the timeout for address aging.

Default: all

Format: `show forwardingdb agetime`

Command mode: Privileged

Term	*Value*
Address Aging Timeout	Displays the system's address aging timeout value in seconds.

show mac-address-table multicast

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

Format: `show mac-address-table multicast` *`macaddr`*
Command mode: Privileged

Term	*Value*
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.

show mac-address-table stats

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

Format: `show mac-address-table stats`

Command mode: Privileged

Term	*Value*
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.

9.40 ISDP configuration commands

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

isdp run

This command enables ISDP on the switch.

Default: disabled

Format: `isdp run`

Command mode: Global Config

no isdp run

This command disables ISDP on the switch.

Format: `no isdp run`

Command mode: Global Config

isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default: 180 seconds

Format: `isdp holdtime` *`10-255`*

Command mode: Global Config

isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default: 60 seconds

Format: `isdp timer 5-254`

Command mode: Global Config

isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default: disabled

Format: `isdp advertise-v2`

Command mode: Global Config

no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format: `no isdp advertise-v2`

Command mode: Global Config

isdp enable

This command enables ISDP on an interface or range of interfaces.

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.

Default: disabled

Format: `isdp enable`

Command mode: Interface Config

no isdp enable

This command disables ISDP on the interface.

Format: `no isdp enable`

Command mode: Interface Config

clear isdp counters

This command clears ISDP counters.

Format: `clear isdp counters`

Command mode: Privileged

clear isdp table

This command clears entries in the ISDP table.

Format: `clear isdp table`

Command mode: Privileged

show isdp

This command displays global ISDP settings.

Format: `show isdp`

Command mode: Privileged

Term	*Value*
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.
Version 2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
Neighbors table time since last change	The amount of time that has passed since the ISPD neighbor table changed.
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.

show isdp interface

This command displays ISDP settings for the specified interface.

Format: `show isdp interface {all | unit/slot/port}`

Command mode: Privileged

Term	*Value*
Interface	The *unit/slot/port* of the specified interface.
Mode	ISDP mode enabled/disabled status for the interface(s).

show isdp entry

This command displays ISDP entries. If the device id is specified, then only entries for that device are shown.

Format: `show isdp entry {all | deviceid}`

Command mode: Privileged

Term	*Value*
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (unit/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 software version that the neighbor is running.
Entry Last Changed Time	The version of the advertisement packet received from the neighbor.
Version	The time when the entry was last changed.

show isdp traffic

This command displays ISDP statistics.

Format: `show isdp traffic`

Command mode: Privileged

Term	*Value*
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 Checksum Error	Number of packets received with a checksum error.
ISDP Transmission Failure	Number of packets which failed to transmit.
ISDP Invalid Format	Number of invalid packets received.
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database.
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

debug isdp packet

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Format: `debug isdp packet [{receive | transmit}]`

Command mode: Privileged

no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format: `no debug isdp packet [{receive | transmit}]`

Command mode: Privileged

9.41 EFM OAM (Ethernet in the First Mile Operations and Maintenance Protocol) configuration commands[1]

This section describes the commands used to configure the Ethernet in the First Mile (EFM) Operations and Maintenance (OAM) protocol. Network administrators use these commands to view link operation data, such as remote fault indication and remote loopback control, which enable monitoring, testing, and troubleshooting OAM-enabled links in the network.

ethernet oam

This command is used to enable the Ethernet OAM on an interface or range of interfaces.

Default: disabled

Format: `ethernet oam`

Command mode: Interface Config

no ethernet oam

This command is used to disable the Ethernet OAM on an interface or range of interfaces.

Format: `no ethernet oam timeout`

Command mode: Interface Config

ethernet oam timeout

This command sets the link lost timer value to 2-30 seconds on an interface or range of interfaces. If any OAM PDUs are not received from the remote DTE within this time period, then the local client executes the Fault state of the Discovery state machine.

Default: 5 seconds

Format: `ethernet oam timeout` *`2-30`*

Command mode: Interface Config

[1] This functionality is available with an EFM OAM license. To activate the license, please contact the technical support.

no ethernet oam timeout

This command sets the link lost timer value to the default.

Format: `no ethernet oam timeout`

Command mode: Interface Config

ethernet oam min-rate

This command sets the minimum transmission rate (pdu_timer) in seconds for sending periodic OAM PDUs on an interface or range of interfaces. The range is 1 to 10.

Default: 1

Format: `ethernet oam min-rate` *`1-10`*

Command mode: Interface Config

no ethernet oam min-rate

This command sets the minimum transmission rate (pdu_timer) in seconds for sending periodic OAM PDUs to the default.

Format: `no ethernet oam min-rate`

Command mode: Interface Config

ethernet oam max-rate

This command sets the maximum transmission rate (pdu_timer) in seconds on an interface or range of interfaces when one OAM PDU is sent per second. The range is 1 to 10.

Default: 1

Format: `ethernet oam max-rate` *`1-10`*

Command mode: Interface Config

no ethernet oam max-rate

This command sets the maximum transmission rate (pdu_timer) to the default.

Format: `no ethernet oam max-rate`

Command mode: Interface Config

ethernet oam mode

This command set the OAM interface mode as Active or Passive on a specified interface or range of interfaces.

Default: passive

Format: `ethernet oam mode {active | passive}`

Command mode: Interface Config

ethernet oam remote-loopback

This command configures Remote Loopback timeout support on an interface or range of interfaces.

Default: remote loopback support is enabled

Format: `ethernet oam remote-loopback [supported] [timeout 1-100]`

Command mode: Interface Config

Term	*Value*
supported	Enables remote loopback. By default, it is enabled. Default: enabled.
timeout	Sets the time in seconds after which remote loopback times-out. The range is 10–100 seconds; 50 seconds is the default.

ethernet oam remote-loopback start

This command starts the remote loopback in the specified OAM interface.

Per IEEE 802.3ah, an OAM entity should be in Active mode to start the remote loopback facility.

Format: `ethernet oam remote-loopback start unit/slot/port`

Command mode: Privileged
User

ethernet oam remote-loopback stop

This command stops the remote loopback in the specified OAM interface.

Format: `ethernet oam remote-loopback stop unit/slot/port`

Command mode: Privileged
User

ethernet oam link-monitor supported

This command enables support for link monitoring on the current interface or range of interfaces.

Default: enabled

Format: `ethernet oam link-monitor supported`

Command mode: Interface Config

no ethernet oam link-monitor supported

This command disables support for link monitoring on the current interface.

Format: `no ethernet oam link-monitor supported`

Command mode: Interface Config

ethernet oam link-monitor

This command starts or stops Link Monitoring on the current OAM-enabled interface.

Default: disabled
Format: `ethernet oam link-monitor {on | off}`

Command mode: Interface Config

ethernet oam link-monitor frame

This command configures the Errored Frame Event properties. This command is used to configure high and low thresholds for error frames that trigger an error-frame link event. The window value provides the time in seconds during which the threshold values must be violated in order for a trap to be generated

Format: `ethernet oam link-monitor frame {threshold {high (1-65535 | none) | low 1-65535}|window 10-60}`

Command mode: Interface Config

Term	*Value*
threshold	Errored frame threshold high and low values in number of frames. Default: 1.
window	Event window size in number of seconds from 10-60. Default is 1.

no ethernet oam link-monitor frame

This command resets the errored frame event properties to their default values.

Default: errored frame event properties are disabled.

Format: `no ethernet oam link-monitor frame {threshold {high | low} |window}`

Command mode: Interface Config

ethernet oam link-monitor frame-period

This command configures the Errored Frame Period Event Properties. This command is used to configure high and low thresholds for the error-frame period that triggers an error-frame-period link event. The window value provides the time in seconds during which the threshold values must be violated in order for a trap to be generated

Format: `ethernet oam link-monitor frame-period {threshold {high (1-65535 | none) | low 1-65535}|window 1-65535}`

Command mode: Interface Config

Term	*Value*
threshold	Errored frame threshold high and low values in number of frames. Default: 1.
window	Polling event window size in number of frames from 1 to 65535. Default value is 1000.

no ethernet oam link-monitor frame-period

This command resets the errored frame period event properties to their default values.

Format: `no ethernet oam link-monitor frame-period {threshold {high | low} |window}`

Command mode: Interface Config

ethernet oam link-monitor frame-seconds

This command configures the Errored Frame Seconds Event Properties. This command is used to configure high and low thresholds for the error-frame seconds that triggers an error-frame-seconds link event. The window value provides the time in seconds during which the threshold values must be violated in order for a trap to be generated

Format: `ethernet oam link-monitor frame-seconds {threshold {high (1-65535 | none) | low 1- 65535} |window 10-900}`

Command mode: Interface Config

Term	*Value*
threshold	Errored frame threshold high and low values in number of frames. Default: 1.
window	Polling event window size in number of frames from 1 to 65535. Default value is 1000.

no ethernet oam link-monitor frame-seconds

This command resets the errored frame seconds event properties.

Format: `no ethernet oam link-monitor frame-seconds {threshold {high | low} |window}`

Command mode: Interface Config

show ethernet oam statistics

This command shows the OAM statistics for the specified OAM interface.

Format: `show ethernet oam statistics [interface unit/slot/port | all]`

Command mode: Privileged
User

show ethernet oam interface

This command shows the OAM interfaces.

Format: `show ethernet oam interface`

Command mode: Privileged

show ethernet oam discovery

This command shows the OAM entity discovery information on the specified OAM interface.

Format: `show ethernet oam discovery [interface unit/slot/port | all]`

Command mode: Privileged

show ethernet oam status

This command displays OAM status information for the specified interface.

Format: `show ethernet oam status [interface unit/slot/port | all]`

Command mode: Privileged
User

show ethernet oam mode

This command displays the interface information for a specified OAM interface.

Format: `show ethernet oam mode` *`unit/slot/port`*`|all`

Command mode: Privileged
User

show ethernet oam link-monitor

This command displays the Ethernet OAM (Dot3ah) Link-Monitoring information for an OAM-enabled interface.

Format: `show ethernet oam link-monitor` *`unit/slot/port`*

Command mode: Privileged
User

show ethernet oam summary

This command displays the Ethernet OAM (Dot3ah) summary of the protocol information.

Format: `show ethernet oam summary [`*`unit/slot/port`* `| all]`

Command mode: Privileged
User

debug dot3ah packet

Use this command to turn on dot3ah packet debug trace on the console. This will allow you to see whether the OAM packet is transmitted or received on an EFM-OAM/Dot3ah-enabled interface.

Format: `debug dot3ah packet`

Command mode: Privileged
User

clear ethernet oam statistics

This command clears the Ethernet OAM (Dot3ah) protocol statistics information on the interface(s).

Format: `show ethernet oam statistics [`*`unit/slot/port`* `| all]`

Command mode: Privileged
User

loopback-test

This command performs loopback testing on a specified port or all ports connected to the switch except those on which OAM is enabled. The test includes MAC-level and PHY-level testing. The status and statistics information returned depends on results received from MAC level or PHY level loop testing provided by hardware.

Format: `loopback-test [mac | phy]` *`unit/slot/port`*

Command mode: Privileged
User

Term	*Value*
Mac	MAC level loop testing.
Phy	Physical level loop testing.

9.42 CFM (Connectivity Fault Management) configuration commands[1]

Ethernet CFM (Connectivity Fault Management), IEEE802.1ag – Provides monitoring, troubleshooting for Ethernet networks, allowing you to control the connection, isolate problem areas of the network and identify clients that have network restrictions.

The protocol operates with the following concepts:

- Maintenance Domain (MD) – a network section owned and operated by one operator;
- Maintenance Association (MA) – set of endpoints (MEP), each of which has the same MAID (Maintenance Association Identifier) identifying the type of service;
- Maintenance association End Point (MEP) – service endpoint located on its border;
- Maintenance domain Intermediate Point (MIP) – intermediate point of the domain.

ethernet cfm domain

Use this command to enter the maintenance domain config mode where you can create maintenance associations and configure per-maintenance domain parameters.

Format: `ethernet cfm domain` *`domain-name`* `level` *`0-7`*

Command mode: Global Config

Parameter	*Description*
domain-name	The identifier, unique over the domain.
level	The maintenance domain unique identifier. Range of values: 0–7.

service vlan

Use this command to enter the maintenance association config mode where you can create maintenance end points and configure per-maintenance domain parameters.

Format: `service` *`service-name`* `vlan` *`vlanID`*

Command mode: Maintenance Domain Config

Parameter	*Description*
service-name	A character string that uniquely identifies a maintenance association in a maintenance domain. You can use up to 45 alphanumeric characters in the name.
vlanID	The maintenance association VLAN ID. Range of values: 1–409. Default: zero (0). The VLAN ID represents a service instance that is monitored by this maintenance association.

ethernet cfm enable

Use this command to enable the administrative state of CFM on the switch.

Default: disabled

Format: `ethernet cfm enable`

Command mode: Global Config

[1] This functionality is available with an CFM license. To activate the license, please contact the technical support.

no ethernet cfm enable

Use the no version of the command to reset the administrative mode of CFM to the default value.

Format: `no ethernet cfm enable`

Command mode: Global Config

ethernet cfm cc level vlan interval

Use this command to configure the Continuity Check Message (CCM) transmit interval.

Format: `ethernet cfm cc level 0-7 vlan vlan-list interval secs`

Command mode: Maintenance Association

Parameter	*Description*
level	A character string that uniquely identifies a maintenance association in a maintenance domain. You can use up to 45 alphanumeric characters in the name.
vlan–list	The maintenance association VLAN ID. Range of values: 1–409. Default: zero (0). The VLAN ID represents a service instance that is monitored by this maintenance association.
secs	The time in seconds between CCM frames transmission, used by all MEPs in the given Maintenance Association. Possible values are: •10 — Set CCM interval to 10 msecs •100 — Set CCM interval to 100 msecs •1000 — Set CCM interval to 1000 msecs •10000 — Set CCM interval to 10000 msecs •3,3 — Set CCM interval to 3.3 msecs •60000 — Set CCM interval to 60000 msecs •600000 — Set CCM interval to 600000 msecs

ethernet cfm mep archive-hold-time

Use this command to configure the number seconds that data from a missing maintenance point (mep) is kept before it is purged. The range is 1–65535 seconds.

Default: `600`

Format: `ethernet cfm mep archive-hold-time seconds`

Command mode: Global Config

no ethernet cfm mep archive-hold-time

Use the no version of the command to reset the archive hold time to the default value.

Format: `no ethernet cfm mep archive-hold-time`

Command mode: Global Config

ethernet cfm mep level

Use this command to configure a Maintenance End Point (MEP) level on an interface or range of interfaces. MEPs are configured per Maintenance Association and per Maintenance Domain.

Format: `ethernet cfm mep level` *`0-7`* `direction {up|down} mpid` *`1–8191`* `vlan` *`vlan–list`*

Command mode: Interface Config

Parameter	*Description*
level	Domain level. Range of values: 0–7. Default: zero (0).
direction	Direction for MEP. Possible values are: • **up** – upward • **down** - downward.
mpid	The Maintenance End Point Identifier. Creates MEPs associated with this Maintenance Association.
vlan–list	The identifier of the VLAN. Range of values: 1–40934. Separate nonconsecutive IDs with a comma (,) and no spaces and no zeros in between the range. Use a dash (–) for the range.

no ethernet cfm mep level

Use the no version of the command to delete a MEP.

Format: `no ethernet cfm mep level` *`0-7`* `direction {up|down} mpid` *`1–8191`* `vlan` *`vlan–list`*

Command mode: Interface Config

Parameter	*Description*
level	Domain level. Range of values: 0–7. Default: zero (0).
mpid	The Maintenance End Point Identifier. Creates MEPs associated with this Maintenance Association.
vlan–list	The identifier of the VLAN. Range of values: 1–40934. Separate nonconsecutive IDs with a comma (,) and no spaces and no zeros in between the range. Use a dash (–) for the range.

ethernet cfm mep enable

Use this command to enable the administrative state of MEP on an interface or range of interfaces. By default, MEPs are disabled. When enabled, MEP starts transmitting Continuity Check (CC) messages periodically.

Default: `disabled`

Format: `ethernet cfm mep enable level` *`0-7`* `vlan` *`vlan–list`* `mpid` *`1-8191`*

Command mode: Interface Config

Parameter	*Description*
level	Domain level. Range of values: 0–7. Default: zero (0).
mpid	The Maintenance End Point Identifier. Creates MEPs associated with this Maintenance Association.
vlan–list	The identifier of the VLAN. Range of values: 1–40934. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no ethernet cfm mep enable

Use the no version of the command to disable MEP.

Format: `no ethernet cfm mep enable level 0-7 vlan vlan-list mpid 1-8191`

Command mode: Interface Config

ethernet cfm mep active

Use this command to set the Maintenance End Point (MEP) active mode on an interface or range of interfaces. The active mode is either True or False.

Default: False.

Format: `ethernet cfm mep active level 0-7 vlan vlan-list mpid 1-8191`

Command mode: Interface Config

Parameter	*Description*
level	Domain level. Range of values: 0–7. Default: zero (0).
mpid	The Maintenance End Point Identifier. Creates MEPs associated with this Maintenance Association.
vlanID	The identifier of the VLAN. Range of values: 1–409. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no ethernet cfm mep active

Use the no version of the command to deactivate MEP.

Format: `no ethernet cfm mep active level 0-7 vlan vlan-list mpid 1-8191`

Command mode: Interface Config

ethernet cfm mip level

Use this command to configure the Maintenance Intermediate Point (MIP) level. MIPs are configured per Maintenance Domain per interface or range of interfaces.

Format: `ethernet cfm mip level 0-7`

Command mode: Interface Config

Parameter	*Description*
level	Domain level. Range of values: 0–7. Default: 0

ping ethernet cfm mac

Use this command to generate a loopback message from the configured MEP. This is triggered from the MA configuration mode.

Format: `ping ethernet cfm mac` *`mac-address`* `domain` *`domain-name`* `level` *`0-7`* `vlan` *`vlan–list`* `mpid` *`1- 8191`* `count` *`1-255`*

Command mode: Privileged

Parameter	*Description*
mac-address	The destination MAC address for which the connectivity needs to be verified.
domain	The name of the domain.
level	The maintenance domain level. Range of values: 0–7. Default: zero (0).
mpid	The Maintenance End Point Identifier (MEP ID) from which the loopback message needs to be transmitted. Range of values: 1–8191.
vlanID	The identifier of the VLAN. Range of values: 1–409. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.
count	The number of LBM to transfer. Range of values: 1–255. Default: 5.

ping ethernet cfm remote–mpid

Use this command to generate a loopback message from the configured MEP. This is triggered from the MA configuration mode.

Format: `ping ethernet cfm remote-mpid` *`1-8191`* `domain` *`domain-name`* `level` *`0-7`* `vlan` *`vlanID`* `mpid` *`1- 8191`* `count` *`1-255`*

Command mode: Privileged

Parameter	*Description*
remote–mpid	The destination Maintenance End Point Identifier (MEP ID) for which the connectivity needs to be verified. Range of values: 1–8191.
domain	The domain name.
level	Domain level. Range of values: 0–7. Default: zero (0).
vlanID	The identifier of the VLAN. Range of values: 1–409. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.
mpid	The Maintenance End Point Identifier (MEP ID) from which the loopback message needs to be transmitted. Range of values: 1–8191.
count	The number of LBM to transfer. Range of values: 1–255. Default: 5.

traceroute ethernet cfm mac

Use this command to generate a Link Trace message from the configured MEP. This is triggered from the MA configuration mode.

Format: `traceroute ethernet cfm mac mac-address [domain domain-name | level 0-7] vlan vlanID mpid 1-8191 ttl 1-255`

Command mode: Privileged

Parameter	*Description*
mac-address	The destination MAC address for which the connectivity needs to be verified.
level	Domain level. Range of values: 0–7. Default: zero (0).
mpid	The Maintenance End Point Identifier (MEP ID) from which the Link Trace message needs to be transmitted. Range of values: 1–8191.
vlanID	The identifier of the VLAN. Range of values: 1–40934. Separate nonconsecutive IDs with a comma (,) and no spaces and no zeros in between the range. Use a dash (–) for the range.
ttl	The number of hops the LTM is expected to be transmitted. Range of values: 1–255. Default: 64.

traceroute ethernet cfm remote–mpid

Use this command to generate a Link Trace message from the configured MEP. This is triggered from the MA configuration mode.

Format: `traceroute ethernet cfm remote-mpid 1-8191 [domain domain-name | level 0-7] vlan vlanID mpid 1-8191 ttl 1-255`

Command mode: Privileged

Parameter	*Description*
remote-mpid	The destination Maintenance End Point Identifier (MEP ID) for which the connectivity needs to be verified.
domain	The name of the domain.
level	Domain level. Range of values: 0–7. Default: zero (0).
vlanID	The identifier of the VLAN. Range of values: 1–4094. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.
mpid	The Maintenance End Point Identifier (MEP ID) from which the Link Trace message (LTM) needs to be transmitted. Range of values: 1–8191.
ttl	The number of hops remaining to the LTM. The number is decremented by 1 by each LinkTrace responder that handles the LTM. Range of values: 1–255. Default: 65. If the LTM TTL is 0 or 1, the LTM is not forwarded to the next hop, and if 0, no LTR is generated.

show ethernet cfm domain

Use this command to display the configured parameters in the Maintenance Domain.

Format: `show ethernet cfm domain` *`domain-name`*

Command mode: Privileged

Parameter	*Description*
domain-name	The name of the domain.
Level	The maintenance domain level.
total Services	The number of service instances.
VLAN	The identifier of the VLAN. Range of values: 1–4094
service-name	A character string that uniquely identifies a maintenance association in a maintenance domain.
CC–Interval	CCM Interval. The time interval in seconds between successive transmissions of CCM.

show ethernet cfm domain brief

Use this command to display a summary of the configured parameters in the Maintenance Domain.

Format: `show ethernet cfm domain brief`

Command mode: Privileged

Parameter	*Description*
CFM Feature	Indicates whether the Connectivity Fault Management (CFM) is enabled or disabled.
MEP Archive Hold Time	The number of seconds that data from a missing maintenance point (MEP) is kept before it is purged. Valid values: from 1 to 65535 seconds.
domain-name	The name of the domain.
level	Domain level.
Services	The number of service instances.

show ethernet cfm maintenance-points local domain

Use this command to display the local maintenance points' configured maintenance *domain name* in the maintenance association.

Format: `show ethernet cfm maintenance-points local domain` *`domain–name`*

Command mode: Privileged

Parameter	*Description*
domain-name	The maintenance domain name.
MPID	MEP ID
Level	Domain level.
Type	Type of service point: MEP or MIP.
VLAN	MA, defined by VLAN ID. Range of values: 1–4094.
Port	The interface index of a physical port or a port channel, to which the MEP is attached.
Direction	Direction for MEP. Possible values are:

	• **up** – upward • **down** - downward.
CC Transmit	If enabled, the MEP will generate CCM messages.
MEP–Active	Indicates the administrative status of the MEP. **True** indicates that MEP is functioning normally. **False** indicates that MEP has stop functioning. Default: **True**.
Operational Status	If value set to **True**, MEP is promptly enabled.
MAC	MEP MAC address.

show ethernet cfm maintenance-points local interface

Use this command to display the *unit/slot/port* interface for the local maintenance points.

Format: `show ethernet cfm maintenance-points local interface [unit/slot/port]`

Command mode: Privileged

Parameter	*Description*
MPID	MEP ID
Level	Domain level.
Type	Type of service point: MEP or MIP.
VLAN	MA, defined by VLAN ID. Range of values: 1–4094.
Port	The interface index of a physical port or a port channel, to which the MEP is attached.
Direction	Direction for MEP. Possible values are: • **up** – upward • **down** - downward.
CC Transmit	If enabled, the MEP will generate CCM messages.
MEP–Active	Indicates the administrative status of the MEP. **True** indicates that MEP is functioning normally. **False** indicates that MEP has stop functioning. Default: **True**.
Operational Status	If value set to **True**, MEP is promptly enabled.
MAC	MEP MAC address.

show ethernet cfm errors

Use this command to display MEP errors on a particular maintenance domain.

Format: `show ethernet cfm errors`

Command mode: Privileged

Parameter	*Description*
Level	The maintenance domain level.
SVID	The 12-bit service VLAN ID.
MPID	MEP ID
DefRDICcm	An integer value specifying the highest priority maintenance end point defect that is generated since the last

	notification.
DefMACStatus	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.
DefRemoteCCM	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.
DefErrorCCM	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.
DefXconCCM	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.

show ethernet cfm errors domain

Use this command to display MEP errors on a particular maintenance domain.

Format: `show ethernet cfm errors domain` *`domain-name`*

Command mode: Privileged

Parameter	***Description***
domain–name	The name of the domain.
Level	Domain level.
SVID	The 12-bit service VLAN ID.
MPID	MEP ID
DefRDICcm	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.
DefMACStatus	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.
DefRemoteCCM	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.
DefErrorCCM	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.
DefXconCCM	An integer value specifying the highest priority maintenance end point defect that is generated since the last notification.

show ethernet cfm errors level

Use this command to display MEP errors on a particular maintenance domain.

Format: `show ethernet cfm errors level` *`level`*

Command mode: Privileged

Parameter	***Description***
Level	Domain level. Range of values: 0–7.

SVID	The 12-bit service VLAN ID.
MPID	MEP ID
DefRDICcm	Remote Defect Indication used by a MEP to communicate to its peer MEPs that a defect condition has been encountered. A MEP that is in a defect condition transmits frames with ETH-RDI information. A MEP, upon receiving frames with ETH-RDI information, determines that is peer MEP has encountered a defect condition.
DefMACStatus	MAC status defect. This occurs if a port on which the transmitting MEP resides has no ability to pass ordinary data, or the MEP's primary VLAN is down. The defect is identified when the last CCM received by the local MEP from some remote MEP indicated that the transmitting MEP's associated MAC is reporting an error status via the Port Status TLV or the Interface Status TLV.
DefRemoteCCM	Remote MEP defect. If no CCM frames from a peer MEP are received within the interval equal to 3.5 times the receiving MEP's CCM transmission period, loss of continuity with the peer MEP is detected.
DefErrorCCM	Indicates the MEP received a CCM frame with an incorrect value of time interval.
DefXconCCM	A cross connect defect. If there is an incompatibility in one of the expected parameters in the CCM frame, for example, domain level, domain name type, service name type, service ID, etc.

show ethernet cfm maintenance-points remote domain

Use this command to display the configured *domain name* in the remote maintenance end point.

Format: `show ethernet cfm maintenance-points remote domain` *`domain–name`*

Command mode: Privileged

Parameter	***Description***
domain–name	Domain name
MEP ID	MEP ID
RMEP ID	Identifier of Remote Maintenance Association End Point (RMEP) of remote MEP.
Level	Domain level.
MAC	Remote MEP MAC address.
VLAN	MA, defined by VLAN ID. Range of values: 1–4094
Expiry Timer (sec)	The expiration time to record the last CCM message on this RMEP.
Service ID	VLAN ID service name.

show ethernet cfm maintenance-points remote level

Use this command to display the configured maintenance domain *level* in the remote maintenance end point.

Format: `show ethernet cfm maintenance-points remote level` *`level`*

Command mode: Privileged

Parameter	*Description*
domain–name	Domain name
MEP ID	MEP ID
RMEP ID	Identifier of Remote Maintenance Association End Point (RMEP) of remote MEP.
Level	Domain level.
MAC	Remote MEP MAC address.
VLAN	MA, defined by VLAN ID. Range of values: 1–4094
Expiry Timer (sec)	The expiration time to record the last CCM message on this RMEP.
Service ID	VLAN ID service name.

show ethernet cfm maintenance-points remote detail mac

Use this command to display the configured remote maintenance end point's MAC address *mac-addr*.

Format: `show ethernet cfm maintenance-points remote detail mac` *mac–addr*

Command mode: Privileged

Parameter	*Description*
mac–addr	6 bit MAC address.
MEP ID	MEP ID
RMEP ID	Identifier of Remote Maintenance Association End Point (RMEP ID) of remote MEP.
Level	Domain level.
VLAN	MA, defined by VLAN ID. Range of values: 1–4094
MAC	Remote MEP MAC address.
Expiry Timer (sec)	The expiration time to record the last CCM message on this RMEP.
Service ID	Service identifier.

show ethernet cfm maintenance-points remote detail mpid

Use this command to display the configured remote maintenance end point's MEP ID.

Format: `show ethernet cfm maintenance-points remote detail mpid` *1-8191*

Command mode: Privileged

Parameter	*Description*
mac–addr	6 bit MAC address.
MEP ID	MEP ID
RMEP ID	Identifier of Remote Maintenance Association End Point (RMEP ID) of remote MEP.
Level	Domain level.
MAC	Remote MEP MAC address.

VLAN	MA, defined by VLAN ID. Range of values: 1–4094
Expiry Timer (sec)	The expiration time to record the last CCM message on this RMEP.
Service ID	Service identifier.

show ethernet cfm traceroute-cache

The link trace triggered for an MP can be traced by displaying the link trace database either giving the transaction ID or the sequence number returned during triggering.

Format: `show ethernet cfm traceroute–cache [sequence–num` *`sequence–num`*`]`

Command mode: Privileged

Parameter	*Description*
sequence–num	The sequence number.

show ethernet cfm statistics

Use this command to display the statistics supported by the CFM component per MEP.

Format: `show ethernet cfm statistics [domain` *`domain-name`* `| level` *`0-7`*`]`

Command mode: Privileged

Parameter	*Description*
Out–of–sequence CCMs received	The total number of out-of-order sequence CCM's received.
CCMs transmitted	The total number of CCMs transmitted.
In–order Loopback Replies received	The total number of in–order Loopback Replies (LBRs) received.
Out–of–order Loopback Replies received	The total number of out–of–order LBRs received.
Bad MSDU Loopback Replies received	The total number of bad MSDU LBRs received.
Loopback Replies transmitted	The total number of Linktrace Replies (LTRs) transmitted.
Unexpected LTRs received	The total number of unexpected Linktrace Replies (LTRs) received.

clear ethernet cfm maintenance-points remote

Use this command to clear the specified remote maintenance end point domain name or level from the local database.

Format: clear ethernet cfm maintenance-points remote {domain *domain-name* | level *level*}

Command mode: Privileged

clear ethernet cfm traceroute-cache

Use this command to clear the Ethernet CFM traceroute cache.

Format: `clear ethernet cfm traceroute-cache`

Command mode: Privileged

9.43 Interface Error Disable and Auto Recovery configuration commands

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. Auto Recovery re-enables the interface after the expiry of configured time interval.

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.

Default: none

Format: `errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp- mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service | link-flap}`

Command mode: Global Config

no errdisable recovery cause

Use this 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.

Format: `no errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp-mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service service | link-flap}`

Command mode: Global Config

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).

Default: 300

Format: `errdisable recovery interval` *`30-86400`*

Command mode: Global Config

no errdisable recovery interval

Use this command to reset the auto recovery interval to the factory default value of 300.

Format: `no errdisable recovery interval`

Command mode: Global Config

show errdisable recovery

Use this command to display the errdisable configuration status of all configurable causes.

Format: `show errdisable recovery`

Command mode: Privileged

The information presented below is displayed.

Parameter	*Description*
arp-inspection	Enable/Disable status of arp-inspection auto recovery.
bpdguard	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.

show interfaces status err-disabled

Use this command to display the interfaces that are error disabled and the amount of time remaining for auto recovery.

Format: `show interfaces status err-disabled`

Command mode: Privileged

The information presented below is displayed.

Parameter	*Description*
interface	An interface that is error disabled.
Errdisable Reason	The cause of the interface being error disabled.
Auto-Recovery Time Left	The amount of time left before auto recovery begins.

9.44 UDLD (UniDirectional Link Detection) configuration commands[1]

The purpose of the UniDirectional Link Detection (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. Use the UDLD commands to detect 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.

[1] This functionality is available with an UDLD license. To activate the license, please contact the technical support.

udld enable (Global Config)

This command enables UDLD globally on the switch.

Default: disabled

Format: `udld enable`

Command mode: Global Config

no udld enable (Global Config)

This command disables udld globally on the switch.

Format: `no udld enable`

Command mode: Global Config

udld message time

This command configures the interval between UDLD probe messages on ports that are in the advertisement phase. The range is from 7 to 90 seconds.

Default: 15 seconds

Format: `udld message time` *`interval`*

Command mode: Global Config

udld timeout interval

This command configures the time interval after which UDLD link is considered to be unidirectional. The range is from 5 to 60 seconds.

Default: 5 seconds

Format: `udld timeout interval` *`interval`*

Command mode: Global Config

udld reset

This command resets all interfaces that have been shutdown by UDLD.

Default: none

Format: `udld reset`

Command mode: Privileged

udld enable (Interface Config)

This command enables UDLD on the specified interface.

Default: disabled

Format: `udld enable`

Command mode: Interface Config

no udld enable (Interface Config)

This command disables UDLD on the specified interface.

Format: `no udld enable`

Command mode: Interface Config

udld port

This command selects the UDLD mode operating on this interface. If the keyword **aggressive** is not entered, the port operates in normal mode.

Default: normal

Format: `udld port [aggressive]`

Command mode: Interface Config

show udld

This command displays the global settings of UDLD.

Format: `show udld`

Command mode: User
Privileged

Parameter	*Description*
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 a decision that the link is unidirectional.

show udld

This command displays the UDLD settings for the specified *unit/slot/port*. If the all keyword is entered, it displays information for all ports.

Format: `show udld {`*`unit/slot/port`*` | all}`

Command mode: User
Privileged

Parameter	*Description*
Port	The identifying port of the interface.
Admin Mode	The administrative mode of UDLD configured on this interface. This is either **Enabled** or **Disabled**.
UDLD Mode	The UDLD mode configured on this interface. This is either **Normal** or **Aggressive**.
UDLD Status	The status of the link as determined by UDLD. Possible values are: • **Undetermined**: UDLD has not collected enough information to determine the state of the port. • **Not applicable**: UDLD is disabled, either globally or on the port. • **Shutdown**: UDLD has detected a unidirectional link and shutdown the port. That is, the port is in an errDisabled state. • **Bidirectional**: UDLD has detected a bidirectional link. • **Undetermined (Link Down)**: The port would transition into this state when the port link physically goes down due to any reasons other than the port been put into D-Disable mode by the UDLD protocol on the switch.

10 DATA CENTER CONFIGURATION COMMANDS[1]

The data center commands allow network operators to deploy lossless Ethernet capabilities in support of a converged network with Fiber Channel and Ethernet data, as specified by the FC-BB-5 working group of ANSI T11. This capability allows operators to deploy networks at a lower cost while still maintaining the same network management operations that exist today.

10.1 DCBX Protocol configuration 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.

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 of the 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.

CIN is Cisco Intel Nuova DCBX (version 1.0). CEE is converged enhanced Ethernet DCBX (version 1.06).

Default: auto

Format: `lldp dcbx version { auto | cin | cee | ieee }`

Command mode: Global Config

Term	*Value*
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

no lldp dcbx version

Use the **no** form of the command to reset the DCBX version to the default value of **auto**.

Format: `no lldp dcbx version`

Command mode: Global Config

[1] This functionality is available with an Data Center license. To activate the license, please contact the technical support.

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.

Default: Transmission of all TLVs is enabled by default.

Format: `lldp tlv-select dcbxp [ ets-config | ets-recommend | pfc | application-priority]`

Command mode: Interface Config
Global Config

Term	*Value*
ets-config	Transmit the ETS configuration TLV.
ets-recommend	Transmit the ETS recommendation TLV.
pfc	Transmit the PFC configuration TLV.
application- priority	Transmit the application priority TLV.

no lldp tlv-select dcbxp

Use the **no lldp tlv-select dcbxp** command to disable LLDP from sending all or individual DCBX TLVs, even if LLDP is enabled for transmission on the given interface.

Format: `no lldp tlv-select dcbxp [ ets-config | ets-recommend | pfc | application-priority]`

Command mode: Interface Config
Global Config

lldp dcbx port-role

Use the **lldp dcbx port-role** command in Interface Config to configure the port role. Possible values are: 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.

Default: The default port role is ***manual***.

Format: `lldp dcbx port-role {auto-up|auto-down|manual |configuration-source}`

Command mode: Interface Config

Term	*Value*
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.
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-upstream 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.
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.

no lldp dcbx port-role

Use the *no lldp dcbx port-role* command in Interface Config to configure the port role to manual.

show lldp tlv-select

Use the *show lldp tlv-select* command in Privileged mode to display the per interface TLV configuration.

Format: `show lldp tlv-select {interface all | unit/slot/port }`

Command mode: Privileged

Parameter	*Description*
all	All interfaces.
unit/slot/port	Physical interface identifier.

show lldp dcbx interface

Use the *show lldp dcbx interface* command in Privileged mode to display the local DCBX control status of an interface.

Format: `show lldp dcbx interface all | unit/slot/port <detail>`

Command mode: Privileged

Parameter	*Description*
unit/slot/port	Physical interface identifier.
all	All interfaces.
Detail	Display detailed DCBX information.
Status	Displays a status summary.
trafficclass	The traffic class can range from 0 to 6.
traffic class group	The Traffic Class Group value can range from 0 to 2.

no classofservice traffic-class-group

Use the *no classofservice traffic-class-group* command in Global Config or Interface Config mode to restore the default mapping for each of the Traffic Classes.

Format: `no classofservice traffic-class-group`

Command mode: Global Config

Interface Config

traffic-class-group max-bandwidth

Use the *traffic-class-group max-bandwidth* command in Global Config or Interface Config mode to specify the maximum transmission bandwidth limit for each Traffic Class Group (TCG). Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Default: Max-bandwidth is zero for all TCG.

Format: `traffic-class-group max-bandwidth` *`bw-0 bw-1 … bw-n`*

Command mode: Global Config

Interface Config

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces.

Each bw-x value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command, and each is independent of the others. The number n is platform-dependent and corresponds to the number of supported traffic classes groups. The default maximum bandwidth value for each TCG is 0, meaning no upper limit is enforced, which allows the TCG queue to consume any available nonguaranteed bandwidth of the interface.

If a nonzero value is specified for any bw-x maximum bandwidth parameter, it must not be less than the current minimum bandwidth value for the corresponding queue. A bw-x maximum bandwidth parameter value of 0 may be specified at any time without restriction.

The maximum bandwidth limits may be used with either a weighted or strict priority scheduling scheme.

A value of 0 (the default) implies an unrestricted upper transmission limit, which is similar to 100%, although there may be subtle operational differences depending on how the device handles ano limit case versus limit to 100%.

no traffic-class-group max-bandwidth

Use the *no traffic-class-group max-bandwidth* command in Global Config or Interface Config mode to restore the default for each queue's maximum bandwidth value.

Format: `no traffic-class-group max-bandwidth`

Command mode: Global Config

Interface Config

traffic-class-group min-bandwidth

Use the *traffic-class-group min-bandwidth* command in Global Config or Interface Config mode to specify the minimum transmission bandwidth guarantee for each interface TCG. The total number of TCG supported per interface is platform specific.

Default: Min-bandwidth is zero for all TCG.

Format: `traffic-class-group min-bandwidth bw-0 bw-1 … bw-n`

Command mode: Global Config

Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces.

Each bw-x value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command, and their combined sum must not exceed 100%. The number n is platform dependent and corresponds to the number of supported Traffic Class Groups. The default minimum bandwidth value for each TCG is 0, meaning no bandwidth is guaranteed (best effort).

If the value of any bw-x minimum bandwidth parameter is specified as greater than the current maximum bandwidth value for the corresponding TCG, then its corresponding maximum bandwidth automatically increases the maximum to the same value.

no traffic-class-group min-bandwidth

Use the *no traffic-class-group min-bandwidth* command in Global Config or Interface Config mode to restore the default for each queue's minimum bandwidth value.

Format: `no traffic-class-group min-bandwidth`

Command mode: Global Config

Interface Config

traffic-class-group strict

Use the *traffic-class-group strict* command in Global Config or Interface Config mode to activate the strict priority scheduler mode for each specified TCG.

Default: Weighted scheduler mode is used for all TCG

Format: `traffic-class-group strict` *tcg-id-0* [*tcg-id-1 … tcg-id-n*]

Command mode: Global Config

Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces.

At least one, but no more than n, tcg-id values are specified with this command. Duplicate tcg-id values are ignored. Each tcg-id value ranges from 0 to (n-1), where n is the total number of TCG supported per interface. The number n is platform-dependent and corresponds to the number of supported traffic classes groups.

When strict priority scheduling is used for a TCG, the minimum bandwidth setting for the TCG is ignored and packets are scheduled for transmission as soon as they arrive. A maximum bandwidth setting for the queue, if configured, serves to limit the outbound transmission rate of a strict priority TCG queue so that it does not consume the entire capacity of the interface. If multiple TCG on the same interface are configured for strict priority mode, the method of handling their packet transmission is platform specific. One typical scheme is to schedule all strict priority TCG ahead of the weighted queues, giving preference among the strict priority TCG to the one with the highest tcg-id.

no traffic-class-group strict

Use the *no traffic-class-group strict* command in Global Config or Interface Config mode to restore the default scheduler mode for each interface TCG.

Format: `no traffic-class-group strict` *tcg-id-0* [*tcg-id-1 … tcg-id-n*]

Command mode: Global Config

Interface Config

traffic-class-group weight

Use the *traffic-class-group weight* command in Global Config or Interface Config mode to specify the weight for each interface TCG.

Default: For TCG0:TCG1:TCG2, weights are in the ratio 100%:0%:0%

Format: `traffic-class-group weight` *wp-0 wp-1 … wp-n*

Command mode: Global Config

Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces.

Each wp-x (weight percentage) value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command, and their combined sum must not exceed 100%. The number n is platform-dependent and corresponds to the number of supported traffic classes groups. The default weight percentage value is in the ratio of 1:2:3 for TCG0:TCG1:TCG2, which is calculated as 100%:0%:0%.

The weight percentage is not considered for TCG that are configured for strict scheduling.

no traffic-class-group weight

Use the *no traffic-class-group weight* command in Global Config or Interface Config mode to restore the default for each queue's weight percentage value.

Format: `no traffic-class-group weight` *wp-0 wp-1 … wp-n*

Command mode: Global Config

Interface Config

show classofservice traffic-class-group

Use the *show classofservice traffic-class-group* command in Privileged mode to display the Traffic Class to Traffic Class Group mapping.

Format: `show classofservice traffic-class-group [unit/slot/port]`

Command mode: Privileged

Enhanced Transmission Selection and Traffic Class Group

classofservice traffic-class-group

Use the *classofservice traffic-class-group* command in Global Config or Interface Config mode to map the internal Traffic Class Group (TCG).

Default: All traffic classes are mapped to TCG 0.

Format: `classofservice traffic-class-group trafficclass traffic class group`

Command mode: Global Config

Interface Config

Parameter	*Description*
unit/slot/port	Optional parameter, valid only on platforms that support independent distribution of a class of services for each port. • If unit/slot/port is specified, the TCG binding tables for this interface are displayed. • If the unit/slot/port value is omitted, global configuration options are displayed (which can be replaced by specific port configurations).
Traffic Class	The traffic class queue identifier.
traffic class group	The traffic class froup identifier.

10.2 FIP Snooping configuration commands

The Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) is used to perform the functions of FC_BB_E device discovery, initialization and maintenance. FIP uses a separate EtherType from FCoE to enable the distinction of discovery, initialization, and maintenance traffic from other FCoE traffic. FIP frames (with one exception) are the standard Ethernet size (1518 Byte 802.1q frame) whereas FCoE frames are a maximum of 2240 bytes.

This document describes FIP snooping, which is a frame inspection method used by FIP Snooping Bridges to monitor FIP frames and apply policies based upon the L2 header information in those frames, following recommendations in Annex C of FC_BB_5 Rev 2.00. This allows for:

1. Auto-configuration of Ethernet ACLs based on information in the Ethernet headers of FIP frames.
2. Emulation of FC point-to-point links within the DCB Ethernet networks.
3. Enhanced FCoE security/robustness by preventing FCoE MAC spoofing.

The FIP Snooping Bridge solution supports configuration-only of perimeter port role and FCF-facing port roles and is only intended for use at the edge of the switched network.

The role of FIP Snooping-enabled ports on the switch falls under one of the following types:

1. Perimeter or Edge port (connected directly to ENode).
2. FCF facing port (that receives traffic from FCFs targeted to the ENodes).

The default port role in an FCoE enabled VLAN is as a perimeter port. FCF facing ports must be configured by the user.

feature fip-snooping

Use the feature *fip-snooping* command in Global Configuration mode to globally enable Fibre Channel over Ethernet Initialization Protocol (FIP) snooping on the switch. When FIP snooping is disabled, received FIP frames are forwarded or flooded using the normal multicast rules.

When FIP snooping is enabled, FC-BB-5 Annex D ACLs are installed on the switch and FIP frames are snooped. FIP snooping will not allow FIP or Fiber Channel over Ethernet (FCoE) frames to be forwarded over a port until the port is operationally enabled for PFC. VLAN tagging must be enabled on the interface in order to carry the dot1p values through the network.

Default: disabled

Format: `feature fip-snooping`

Command mode: Global Config

no feature fip-snooping

Use the no form of the command to return the settings to the default values and globally disable FIP snooping. When FIP snooping is globally disabled, received FIP frames are forwarded or flooded using the normal multicast rules. In addition, other FIP snooping commands are not available until the FIP snooping feature is enabled.

Format: `no feature fip-snooping`

Command mode: Global Config

Example:

The following example disables the FIP snooping feature.

```
s1(config)#no feature fip-snooping
```

fip-snooping enable

Use the *fip-snooping enable* command in VLAN Configuration mode to enable snooping of FIP packets on the configured VLANs. FIP snooping is disabled on VLANs by default.

Priority Flow Control (PFC) must be operationally enabled before FIP snooping can operate on an interface. VLAN tagging needs to be turned on in order to carry the dot1p value through the network.

This command can only be entered after FIP snooping is enabled using the *feature fip- snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Default: disabled

Format: `feature fip-snooping`

Command mode: VLAN Config

no fip-snooping enable

Use the ***no*** form of the command to return the mode to the default (off).

Format: `no feature fip-snooping`

Command mode: VLAN Config

fip-snooping fc-map

Use the *fip-snooping fc-map* command in VLAN Configuration mode to configure the FP-MAP value on a VLAN. The FC map value is used to help in securing the switch against misconfiguration.

When configured using fabric-provided MAC addresses, FCoE devices transmit frames containing the FC map value in the upper 24 bits. Only frames that match the configured FC map value are passed across the VLAN. Frames with MAC addresses that do not match the FC map value are discarded.

This command can only be entered after FIP snooping is enabled using the *feature fip- snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Default: The default FC map value is 0x0efc00.

Format: `fip-snooping fc-map` *`0x0 – 0xffffff`*

Command mode: VLAN Config

Parameter	***Description***
map value	Valid FC map values are in the range of 0x0 to 0xffffff.

no fip-snooping fc-map

The ***no*** version of the command sets the FC-MAP value for the VLAN to the default value.

Format: `no fip-snooping fc-map`

Command mode: VLAN Config

fip-snooping port-mode

To relay the FIP packets received from the hosts toward the Fibre Channel Fabric (FCF), the switch needs to know the interfaces to which the FCFs are connected. Use the *fip-snooping port-mode* command in Interface Config to configure the interface that is connected towards FCF. By default, an interface is configured to be a host-facing interface if it is not configured to be an FCF-facing interface.

It is recommended that FCF-facing ports be placed into auto-upstream mode in order to receive DCBX information and propagate it to the CNAs on the downstream (host-facing) ports.

Interfaces enabled for PFC should be configured in trunk or general mode and must be PFC-operationally enabled before FCoE traffic can pass over the port.

This command can only be entered after FIP snooping is enabled using the *feature fip- snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Default: Configuration as a host-facing interface.

Format: `fip-snooping port-mode fcf`

Command mode: Interface Config

Parameter	*Description*
fcf	Fibre Channel Fabric

show fip-snooping

Use the *show fip-snooping* command in User or Privileged mode to display information about the global FIP snooping configuration and status.

Format: `show fip-snooping`

Command mode: User

Privileged

The information presented below is displayed.

Parameter	*Description*
Global Mode	Fibre Channel Fabric
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.

show fip-snooping enode

Use the *show fip-snooping enode* command in User or Privileged mode to display information about the interfaces connected to ENodes.

This command can only be entered after FIP snooping is enabled using the *feature fip-snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Format: `show fip-snooping enode [ENode-mac]`

Command mode: User

Privileged

Parameter	*Description*
ENode-mac	MAC address of the enode to display.

The command outputs the following information.

Parameter	*Description*
Interface	The interface to which the ENode is connected.
VLAN	ID number of the VLAN to which the ENode belongs.
NameID	Name of the ENode.
FIP-MAC	MAC address of the ENode.
FCID	Fiber channel ID number of the virtual port that was created by FCF when the ENode logged into the network.
Sessions Established	Number of successful virtual connections established.

The command displays the following additional information when the optional argument is supplied.

Parameter	*Description*
Sessions Waiting	Number of virtual connections waiting for FCF acceptance.
Sessions Failed	Number of virtual sessions failed.
Max-FCoE-PDU	Maximum FCoE PDU size the ENode MAC intends to use for FCoE traffic. This is equivalent to the maximum Ethernet frame payload the ENode intends to send.
Time elapsed	Time elapsed since first successful login session snooped from the ENode.

show fip-snooping fcf

Use the **show fip-snooping fcf** command in User or Privileged mode to display information about the interfaces connected to FCFs.

This command can only be entered after FIP snooping is enabled using the *feature fip-snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Format: `show fip-snooping fcf [fcf-mac]`

Command mode: User
Privileged

The following information is displayed when no FCF mac argument is supplied.

Parameter	*Description*
Interface	Interface to which the FCF is connected.
VLAN	ID number of the VLAN to which the FCF belongs.
No. of ENodes	Total number of ENodes that are connected to the FCF.
FPMA/SPMA	Type of the MAC address for ENode as negotiated by the FCF.
FCMAP	FCMAP value used by the FCF.
FIP-MAC	MAC address of the FCF.
Fabric Name	Name of the FCF.

Below is additional information regarding the FCF that is displayed when the optional FCF MAC address argument is provided.

Parameter	*Description*
Sessions	Total number of virtual sessions accepted by FCF in the associated VLAN.
D-bit	This reflects the value of the D-bit provided by the most recently received Discovery Advertisement from the FCF. When D-bit value is zero then FIP snooping bridge verifies the periodic VN_Port FIP Keep Alive frames associated with FCF and Discovery Advertisements sent by FCF. When D-bit is set to 1, switch discards snooped VN_Port FIP Keep Alive frames associated with FCF and does not timeout the FCoE sessions established with the FCF based on FKA_VN_PERIOD*5 interval.
Available for Login	This reflects the value of the A bit provided by the most

	recently received Discovery Advertisement from the FCF. This provides the information that the transmitting FCF is available for FIP FLOGI/FDISC from ENodes. This is informational and shall have no effect on existing logins.
Priority	The Priority returned from the FCF in the Solicited Discovery Advertisement. This indicates the Priority that has been manually assigned to the FCF.
FKA-ADV	FIP keepalive interval (FKA_ADV_PERIOD) in seconds configured on the FCF multiplied by five. For example, if the FKA_ADV period configured on the FCF is 80 seconds, the value of this field is 400.
FCF Expiry Time	This is timer value to monitor the status of the FCF. FCF entry and all its associated virtual sessions will be removed when the value reaches 0. This value is reset to Configured FKA- ADV every time a Discovery Advertisement is received from the FCF-MAC.
Time elapsed	Time since FCF is Discovered.

show fip-snooping sessions

Use the show fip-snooping sessions command in User or Privileged mode to display information about the active FIP snooping sessions.

This command can only be entered after FIP snooping is enabled using the *feature fip-snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Format: `show fip-snooping sessions [[[vlan` *`vlan-id`*`] | [interface` *`interface-id`*`] | [fcf fcf- mac [enode` *`Enode-mac`*`]]] [detail]]`

Command mode: User
Privileged

Parameter	*Description*
Interface-id	ID of an interface on which FIP snooping has been enabled.
FCF-MAC	MAC address of the FCF that is part of the session.
ENode-mac	MAC address of the ENode that is part of the session.
VLAN	ID number of the VLAN that contains the session.
FCoE MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
FC-ID	Fiber Channel ID of the virtual port that was created by the FCF when the ENode VN_Port did a FLOGI/NPIV/FDISC request.

The command output format is different when the *detail* option is used. The information below is displayed.

Parameter	*Description*
VLAN	VLAN to which the session belongs.
FC-MAP	FCMAP value used by the FCF.
FCFs	Number of FCFs discovered.
ENodes	Number of ENodes discovered.

Sessions	Total virtual sessions in FCoE VLAN.
FCF Information	
Interface	Interface on which the FCF is discovered.
MAC	MAC address of the FCF.
ENodes	Total number of ENodes that are connected to the FCF.
Sessions	Total number of virtual sessions accepted by FCF in the associated VLAN.
ENode Information	
Interface	The interface to which the ENode is connected.
MAC	MAC address of the ENode.
Sessions	Total number of virtual sessions originated from ENodes to FCF in the VLAN.
Waiting	Total number of virtual connections waiting for FCF acceptance in the VLAN.
Session Information	
FCoE-MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
Request (FP, SP)	FIP session request type sent by ENode. This can be FLOGI or FDESC (NPIV FDISC). Whereas FP and SP values are the FP bit and the SP bit values in the FLOGI or NPIV FDISC request respectively.
Expiry Time	This is virtual connection/session expiry interval. This is used to monitor the status of the session. Session entry is removed when the value reaches 0. This value is reset to 450 secs (5*90 secs) every time an associated VN_Port FKA is received from the ENode. This is ignored (marked as NA) if the D-bit is set to one in the FCF Discovery Advertisements.
Mode	This is the addressing mode in use by the VN_Port at ENode. In other words, this is the type of MAC address granted (selected and returned) by FCF. This can be one of the addressing modes, i.e. FPMA or SPMA.
State	This is the state of the virtual session. The state is displayed as **Tentative** during the process of ENode login to FCF (using FLOGI or FDESC). It displays **Active** after ENode and FCF establish a successful virtual connection.
Session-Time	Time elapsed after this successful virtual session is established by ENode with FCF. The value is displayed in **xd**, **yh**, **zm** format where **x** represents number of days, **y** represents hours and **z** represents minutes elapsed following this successful virtual session. This field has no useful information for waiting sessions.

show fip-snooping statistics

Use the *show fip-snooping statistics* command in User or Privileged mode to display the statistics of the FIP packets snooped in the VLAN or on an interface. If the optional (VLAN or interface) argument is not given, this command displays the statistics for all of the FIP snooping enabled VLANs.

This command can only be entered after FIP snooping is enabled using the *feature fip-snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Format: `show fip-snooping statistics [vlan` *`vlan-id`*`] | [interface` *`interface-id`*`]`

Command mode: User

Privileged

Parameter	*Description*
vlan-id	A VLAN on which FIP snooping is enabled.
interface-id	An interface belonging to a VLAN on which FIP snooping is enabled.

The following table describes the packet counters per FIP Operation.

Packet timer	*Description*
VR	Number of VLAN Request messages received on the VLAN.
VN	Number of VLAN Notification messages received on the VLAN.
MDS	Number of Multicast Discovery Solicitation messages snooped on the VLAN.
UDS	Number of Unicast Discovery Solicitation messages snooped on the VLAN.
FLOGI	Number of Fabric Logins snooped on the VLAN.
FDISC	Number of fabric discovery logins snooped on the VLAN.
LOGO	Number of Fabric Logouts on the VLAN.
VNPort-keep-alive	Number of VN_Port keepalive messages snooped on the VLAN.
MDA	Number of Multicast Discovery Advertisement messages snooped on the VLAN.
UDA	Number of Unicast Discovery Advertisement messages snooped on the VLAN.
FLOGI_ACC	Number of Fabric Logins accepted on the VLAN.
FLOGI_RJT	Number of Fabric Logins rejected on the VLAN.
FDISC_ACC	Number of Fabric Discoveries accepted on the VLAN.
FDISC_RJT	Number of Fabric Discoveries rejected on the VLAN.
LOGO_ACC	Number of Fabric Logouts accepted on the VLAN.
LOGO_RJT	Number of Fabric Logouts rejected on the VLAN.
CVL	Number of Clear Virtual Links actions on the VLAN.

The following table describes the other interface or session-related counters.

Packet timer	*Description*
Number of Virtual Session Timeouts	Number of Virtual sessions removed due to session timer expiry.
Number of FCF Session Timeouts	Number of ACTIVE sessions timed out due to Discovery Advertisements expiry from FCFs in the VLAN.

Number of Session configuration failures	Number of sessions in the VLAN that failed to be configured in the hardware.
Number of Sessions denied with FCF limit	Number of sessions that are denied to be created for the new FCF as the number of FCFs reached the maximum allowed in the VLAN.
Number of Sessions denied with ENode limit	Number of session create requests that are denied for the new ENode as the number of ENodes reached the maximum allowed in the system.
Number of Sessions denied with System limit	Number of sessions that are denied to be created as the number of sessions reached the maximum allowed in the system.

When an interface is provided as an argument, interface applicable statistics are only displayed.

show fip-snooping vlan

Use the *show fip-snooping vlan* command in User or Privileged mode to display the FCoE VLANs information and, additionally, the FIP snooping port status when optional argument is specified.

This command can only be entered after FIP snooping is enabled using the *feature fip-snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Format: `show fip-snooping vlan [vlan-id]`

Command mode: User

Privileged

Packet timer	*Description*
vlan-id	A VLAN enabled for FIP snooping.
VLAN	VLAN in which FIP snooping is enabled/operational.
FC-MAP	FCoE mapped address prefix of the FCoE forwarder for the FCoE VLAN.
FCFs	Number of FCFs discovered.
ENodes	Number of ENodes discovered.
Sessions	Total virtual sessions in FCoE VLAN.

clear fip-snooping statistics

Use the *clear fip-snooping statistics* command in User or Privileged mode to clear the FIP Snooping statistics in the supplied VLAN or on a supplied interface. If the optional (VLAN or interface) argument is not given, this command clears the statistics on all FIP snooping-enabled VLANs.

This command can only be entered after FIP snooping is enabled using the *feature fip-snooping* command. Otherwise, it does not appear in the CLI syntax tree.

Format: `clear fip-snooping statistics [vlan vlan-id] | [interface interface-id]`

Command mode: User

Privileged

Packet timer	*Description*
vlan-id	A VLAN on which FIP snooping is enabled.
interface-id	An interface belonging to a VLAN on which FIP snooping is enabled.

10.3 OpenFlow Protocol configuration commands

The OpenFlow feature enables the switch to be managed by a centralized OpenFlow Controller using the OpenFlow protocol.

openflow enable

This command enables the OpenFlow feature.

Default: disabled

Format: `openflow enable`

Command mode: Global Config

no openflow enable

This command disables the OpenFlow feature. The OpenFlow feature can be administratively disabled at any time.

Format: `no openflow enable`

Command mode: Global Config

openflow static-ip

This command sets the IP address to be used for the OpenFlow feature. The static IP is applied only when the static IP mode is enabled. The switch must have an operational IP interface with the specified address in order for the static IP address to be used for the OpenFlow feature. If the system does not have an interface with a matching IP address then the OpenFlow feature is operationally disabled.

If the OpenFlow feature is enabled when this command is issued and the specified static IP address is not the same as the IP address already in use by the OpenFlow feature then the feature is automatically disabled and re-enabled.

Default: 0.0.0.0

Format: `openflow static-ip` *`IPv4 Address`*

Command mode: Global Config

no openflow static-ip

This command sets the OpenFlow static IP address to 0.0.0.0. Issuing this command when OpenFlow is enabled and using a static IP causes the OpenFlow feature to become operationally disabled.

Format: `no openflow static-ip`

Command mode: Global Config

openflow controller

Specify up to twenty IP addresses to which the switch should establish an OpenFlow Controllers connection. Each command invocation specifies one IP address and connection mode (TCP or SSL). If the IP Port is omitted then the default IP port number 6633 is used. The default connection mode is SSL. The controller table configured by this command is used by the switch in OpenFlow 1.0/1.3 modes.

Format: `openflow controller` *`ip-address`* [*`ip-port`*] [*`connection mode`*]

Command mode: Global Config

Packet timer	*Description*
ip-address	Specify up to five IP addresses to which the switch should establish an OpenFlow Management connection.
Ip-port	TCP port to use for an OpenFlow Management connection. If the TCP Port is omitted, then the default IP port number 6632 is used.
connection mode	TCP or SSL. Default: SSL.

no openflow controller

Delete the specified OpenFlow Controller IP address or delete all Controller addresses. If the IP Port number is omitted then all entries for the specified IP address are deleted.

Format: `no openflow controller {`*`ip-address`* [*`ip-port`*] | `all}`

Command mode: Global Config

openflow default-table

Configure 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. The parameter is applicable only when the OpenFlow variant is set to OpenFlow 1.0.

Default: full-match

Format: `openflow default-table` *`parameter`*

Command mode: Global Config

Packet timer	*Description*
Parameter	Possible values are: **full-match** or **layer-2-match**.

openflow ip-mode

This command directs the OpenFlow feature to use the configured IP address. Issuing this command when OpenFlow is already enabled causes the feature to be disabled and re-enabled with the new IP address.

Default: disabled

Format: `openflow ip-mode {auto|static|serviceport}`

Command mode: Global Config

no openflow ip-mode

This command directs the OpenFlow feature to automatically assign the IP address to itself.

Format: `no openflow ip-mode`

Command mode: Global Config

openflow passive-mode

This command enables OpenFlow passive-mode.

Default: disabled

Format: `openflow passive-mode`

Command mode: Global Config

no openflow passive-mode

This command disables OpenFlow passive-mode.

Format: `no openflow ip-mode`

Command mode: Global Config

openflow variant

This command configures the OpenFlow feature to the specified variant. You can configure the OpenFlow feature to use one of two variants: **OpenFlow 1.0** or **OpenFlow 1.3**. The OpenFlow feature is configured to **OpenFlow 1.3** by default.

Default: OpenFlow1.3

Format: `openflow variant` *`openflow10|openflow13`*

Command mode: Global Config

clear openflow ca-cert

This command erases the Certificate Authority certificates used for validating the OpenFlow Controllers from the switch. Issuing this command automatically disables and re-enables the OpenFlow feature. The new SSL certificates are reloaded from the OpenFlow Controller on the first connection to the controller or can be manually loaded with a *copy* command.

Format: `clear openflow ca-cert`

Command mode: Privileged

show openflow

This command displays the OpenFlow feature status and configuration information.

Format: `show openflow`

Command mode: Privileged

Packet timer	*Description*
Administrative Mode	The administrative mode of the OpenFlow feature.
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	The IP mode. Possible values are: **Auto**, **Static** or **ServicePort IP**.
Static IP Address	Static IP address.
openflow variant	OpenFlow Protocol Variant. Possible values are: **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.

show openflow configured controller

This command displays a list of configured OpenFlow Controllers. The switch communicates with these controllers only when the OpenFlow variant is 1.0 or 1.3.

Format: `show openflow configured controller`

Command mode: Privileged

Packet timer	***Description***
IP Address	IPv4 address of the controller.
IP Port	TCP port number for the controller connection.
connection mode	SSL or TCP Controller Connection mode.
Role	The role of the controller: Master, Equal, Slave

show openflow installed flows

This command displays the list of configured flows on the switch.

Format: `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`*`]`

Command mode: Privileged

Flow filters	
Parameter	***Description***
dest_ip	The IP address of the destination.
dest_ip_port	The port number of the destination.
dest_mac	The MAC address of the destination.
dscp	The DSCP value.
ether_type	The ethertype value.
Ingress_port	The slot and port for the ingress.
ip_proto	The IP protocol.

priority	The priority of the flow.
source_ip	The IP address of the source.
source_ip_port	The port number of the source.
source_mac	The MAC address of the source.
table	The table number.
vlan	The VLAN.
vlan_prio	The VLAN priority.
The information about set flows	
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. 0 is displayed if the flow cannot be added. 1 is displayed if the flow was added.

show openflow installed groups

Use this command to display the list of configured groups on the switch.

Format: `show openflow installed groups`

Command mode: Privileged

Packet timer	***Description***
Group Type	Type of the Group (Indirect, All, Select etc.)
Group ID	Unique ID of the Group
Reference 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.

show openflow table-status

This command displays the supported OpenFlow tables and report usage information for the tables.

Format: `show openflow table-status {openflow10|opnflow13)`

Command mode: Privileged

Packet timer	***Description***
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 the 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.

10.4 Priority-Based Flow Control configuration commands

Ordinarily, when flow control is enabled on a physical link, it applies to all traffic on the link. When congestion occurs, the hardware sends pause frames that temporarily suspend traffic flow. Pausing traffic helps prevent buffer overflow and dropped frames.

Priority-based flow control (PFC) provides a way to distinguish which traffic on physical link is paused when congestion occurs, based on the priority of the traffic. An interface can be configured to pause only high priority (i.e., loss-sensitive) traffic when necessary prevent dropped frames, while allowing traffic that has greater loss tolerance to continue to flow on the interface.

Priorities are differentiated by the priority field of the IEEE 802.1Q VLAN header, which identifies an IEEE 802.1p priority value. These priority values must be mapped to internal class-of-service (CoS) values.

To enable priority-based flow control for a particular CoS value on an interface:

1. Ensure that VLAN tagging is enabled on the interface so that the 1p priority values are carried through the network;

2. Ensure that 1p priority values are mapped to CoS values (see “classofservice dot1p-mapping”).

When priority-flow-control is disabled, the interface defaults to the IEEE 802.3x flow control setting for the interface. When priority-based flow control is enabled, the interface will not pause any CoS unless there is at least one no-drop priority.

priority-flow-control mode

Use the *priority-flow-control mode* on command in Datacenter-Bridging Config mode to enable Priority-Flow- Control (PFC) on the given interface.

PFC must be enabled before FIP snooping can operate over the interface. Use the *no* form of the command to return the mode to the default (off). VLAN tagging (trunk or general mode) must be enabled on the interface in order to carry the dot1p value through the network. Additionally, the dot1mapping to class-of-service must be set to one-to-one.

When PFC is enabled on an interface, the normal PAUSE control mechanism is operationally disabled.

Default: Priority-flow-control mode is off (disabled) by default.

Format: `priority-flow-control mode { on | off }`

Command mode: Datacenter bridge setup

Parameter	*Description*
on	Enable PFC on the interface.
off	Disable PFC on the interface.

no priority-flow-control mode

Use the no priority-flow-control mode command to return the PFC mode to the default (off).

Format: `no priority-flow-control mode`

Command mode: Datacenter bridge setup

priority-flow-control priority

Use the *priority-flow-control priority* command in Datacenter-Bridging Config mode to enable the priority group for lossless (no-drop) or lossy (drop) behavior on the selected interface. Up to two lossless priorities can be enabled on an interface. The administrator must configure the same no-drop priorities across the network in order to ensure end-to-end lossless behavior.

The command has no effect on interfaces not enabled for PFC. VLAN tagging needs to be turned on in order to carry the dot1p value through the network. Additionally, the dot1pmapping to class of service must be set to one to one.

Default: The default behavior for all priorities is drop.

Format: `priority-flow-control priority` *`priority-list`* `{drop | no-drop}`

Command mode: Datacenter-Bridging Config

Parameter	*Description*
drop	Enable lossless behavior on the selected priorities.
no-drop	Disable lossless behavior on the selected priorities.

no priority-flow-control priority

Use the *no priority-flow-control priority* command in Datacenter-Bridging Config mode to enable lossy behavior on all priorities on the interface. This has no effect on interfaces not enabled for PFC or with no lossless priorities configured.

Format: `no priority-flow-control priority`

Command mode: Datacenter bridge setup

clear priority-flow-control statistics

Use the clear priority-flow-control statistics command to clear all global and interface PFC statistics.

Format: `clear priority-flow-control statistics`

Command mode: Privileged

show interface priority-flow-control

Use the *show interface priority-flow-control* command in Privileged mode to display the PFC information of a given interface or all interfaces.

Format: `show interface [unit/slot/port] priority-flow-control`

Command mode: Privileged

Parameter	*Description*
unit/slot/port	A valid Ethernet port.

When an interface number is not provided, the following information displays for all interfaces.

Parameter	*Description*
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 through LLDP DCBX.
Configured 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 through LLDP DCBX.
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 include 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.

10.5 QCN (Quantized Congestion Notification) configuration commands

The Quantized Congestion Notification (QCN) feature is part of the Data Center Package.

qcn enable

Use the *qcn enable* command in Global Configuration mode to enable QCN on all the ports of the system. This command is master enable control. When QCN is enabled, the system recognizes the CN-TAG in received frames, the Congestion algorithm runs on the configured Congestion Points (CP) and Congestion Notification Messages (CNMs) are transmitted if congestion is detected on a CP.

Default: disabled

Format: `qcn enable`

Command mode: Global Config

no qcn enable

Use the no *qcn enable* command in Global Configuration mode to disable QCN on all the ports of the system. This command is the master disable command. When QCN is disabled, received frames with CN-TAGs are treated as normal data frames and CNMs are never generated.

Format: `no qcn enable`

Command mode: Global Config

qcn cnm-transmit-priority

Use the *qcn cnm-transmit-priority* command in Global Configuration mode to globally configure the dot1p priority of congestion notification messages (CNM) that are transmitted by the system. This command configures the dot1p priority value with which the CNM are transmitted. By default, CNMs are transmitted with dot1p priority as zero.

Default: 0

Format: `qcn cnm-transmit-priority dot1p priority`

Command mode: Global Config

Parameter	*Description*
dot1p priority	The range is 0–7.

no qcn cnm-transmit-priority

Use the *no qcn cnm-transmit-priority* command in Global Configuration mode to set to the default value the dot1p priority on CNMs that are transmitted by the system.

Format: `no qcn cnm-transmit-priority`

Command mode: Global Config

qcn cnpv-priority (datacenter bridging config)

Use the *qcn cnpv-priority* command in Data Center Bridging Configuration mode to globally configure a CP (port-queue) that is mapped to the specified dot1p priority as congestion enabled (**interior**) or congestion disabled (**disable**) or edge congestion point (**edge**) for all ports which have the defense mode configured as component.

Default: All priorities are disabled for QCN.

Format: `qcn cnpv-priority priority {interior | edge | disable}`

Command mode: Datacenter-Bridging Config

Packet timer	*Description*
cnpv-priority	The range is 0–7.
Interior (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 congestion point (ECP)	Used when the congestion point (CP) is on the edge of the congestion notification domain (CND).
Disabled for QCN	Used when it is desired that the priority be congestion unaware. This setting disables detection of congestion on the priority.

qcn cnpv-priority alternate-priority

Use the *qcn cnpv-priority alternate-priority* command in Global Configuration mode to globally configure the alternate priority for the selected cnpv-priority. When a frame is received with a dot1p priority equal to congestion notification priority value, the priority value in the frame is remarked with the alternate priority. The alternate priority is applied to incoming frames if and only if the incoming frame's dot1p priority is equal to CNPV priority of the CP and CP is configured as Edge.

Use the alternate priority setting to steer away traffic that comes from CN-unaware sources. Traffic from noncongestion aware sources is remarked when entering the CND domain so that the resources assigned to the congestion-enabled queues are not exhausted with traffic from QCN unaware sources. Since the frames are coming from non-QCN sources, they do not have a CN-TAG. If the frames are mapped to the congestion- enabled queue, then they may contribute to the congestion and, in turn, trigger generation of CNMs. This is not useful to sources that are QCN-unaware.

This configuration is applied to all ports whose defense-mode-choice is configured as component.

Format: `qcn cnpv-priority cnpv priority alternate-priority non-cnpv priority`

Command mode: Global Config

Packet timer	*Description*
cnpv priority	The range is 1–7.
non-cnpv priority	The range of alternate priority is 0–7.

no qcn cnpv-priority alternate-priority

Use the *no qcn cnpv-priority alternate-priority* command in Global Configuration mode to reset the alternate priority to the default value.

Format: `no qcn cnpv-priority cnpv priority alternate-priority`

Command mode: Global Config

qcn cnpv-priority cp-creation

Use the *qcn cnpv-priority cp-creation* command in Global Configuration mode to globally configure the default scope for the per port-priority defense mode choice when a CP is newly created. The default scope for per-port defense mode choice can be ***admin*** or ***component***.

Default: qcn cp-creation is set to enable

Format: `qcn cnpv-priority` *`cnpv-priority`* `cp-creation {enable | disable}`

Command mode: Global Config

Packet timer	***Description***
cnpv-priority	The range is 1–7.
admin scope	Is per-priority.
component scope	Is per priority level configuration.
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.

qcn cnpv-priority defense-mode-choice

Use the *qcn cnpv-priority defense-mode-choice* command in Interface Config to select the defense-mode as ***admin*** or ***component*** on an interface, namely whether interior/edge/disable and alternate priorities should use the per-priority configuration or the per-port-priority configuration.

Default: enabled

Format: `qcn cnpv-priority` *`cnpv-priority`* `defense-mode-choice {admin | component}`

Command mode: Interface Config

Packet timer	***Description***
cnpv-priority	The range is 1–7.
admin scope	Is per-priority.
component scope	Is per priority level configuration.

qcn cnpv-priority

Use the *qcn cnpv-priority* command in Interface Config mode to configure a CP (port-queue) that is mapped to the specified dot1p priority.

This configuration is applied if the defense mode choice is configured as **Admin**.

Default: By default, QCN is not enabled for any priority.

Format: `qcn cnpv-priority priority {interior | edge | disable}`

Command mode: Interface Config

Packet timer	***Description***
cnpv-priority	The range is 0–7.
The possible selections for a Congestion Point (CP) are:	
Interior (ICP)	Used when a flow with the specified dot1p priority needs to be congestion aware.
Edge congestion point (ECP)	Used when the congestion point (CP) is on the edge of the congestion notification domain (CND).

Disabled for QCN	Used when it is desired that the priority be congestion unaware. This setting disables detection of congestion on the priority.

qcn cnpv-priority alternate-priority

Use the *qcn cnpv-priority alternate-priority* command in Interface Config to configure the alternate priority on an interface for the specified incoming ICP priority. This alternate-priority overrides the alternate-priority set in the global mode for this incoming ICP priority on this port. This configuration is applied if the defense mode choice is configured as **Admin**.

Default: By default, the alternate-priority configured in global is used.

Format: `qcn alternate-priority incoming priority alternate-priority`

Command mode: Interface Config

Parameter	*Description*
cnpv-priority	The range is 1–7.
alternate-priority	The range is 0–7.

no qcn cnpv-priority alternate-priority

Use the *no qcn cnpv-priority alternate-priority* command in Interface Config to reset the alternate priority of the given port-priority to the default value. If a global alternate priority value is configured, it is used.

Default: By default, the alternate-priority configured in global is used.

Format: `no qcn alternate-priority incoming-priority alternate-priority`

Command mode: Interface Config

qcn transmit-tlv enable

Use the *qcn transmit-tlv enable* command in Interface Config to enable transmission of QCN TLVs via LLDP.

Default: By default, transmission of QCN TLVs is disabled.

Format: `qcn transmit-tlv enable`

Command mode: Interface Config

no qcn transmit-tlv enable

Use the *no qcn transmit-tlv enable* command in Interface Config to configure the mode of the QCN TLV transmission to disable. QCN TLVs transmission is propagated using LLDP.

Format: `no qcn transmit-tlv enable`

Command mode: Interface Config

clear qcn statistics

Use the *clear qcn statistics* command in Privileged mode to clear the CNM transmitted counters on the CP. If interface and the CP are not mentioned, then this command clears all the CNM counters for all CPs in the system. If only the interface number is specified, then all the CNM transmit counters on that interface are cleared.

Format: `clear qcn statistics [interface unit/slot/port] [cp cp-index]`

Command mode: Privileged

Parameter	*Description*
unit/slot/port	If only the interface number is specified, then all the CNM transmit counters on that interface are cleared.
cp-index	If only the cp index is specified, then CNM transmit counters for that cp index on all interfaces are cleared.

show qcn priority

Use the *show qcn priority* command in Privileged mode to display the QCN configuration.

Format: `show qcn priority [priority ] [interface unit/slot/port| all]`

Command mode: Privileged

Parameter	*Description*
priority	If only priority is specified, then per-priority configuration is displayed.
all	If all is specified, then per priority information for all dot1p priorities is displayed.
unit/slot/port	If the interface number is also specified, then the command displays the configuration per- port-priority for the given priority.

The following data is displayed as part of this command.

show qcn active priority

Use the *show qcn active priority* command in Privileged mode to display the operational QCN configuration for the specified dot1p priority.

Format: `show qcn active priority 0-7`

Command mode: Privileged

show qcn interface

Use the *show qcn interface* command in Privileged mode to display Congestion Point information for the specified port.

Format `show qcn interface unit/slot/port [cp cpindex]`

Command mode: Privileged

show qcn statistics

Use the *show qcn statistics* command in Privileged mode to display the statistics of the CNM and data frames for all the ports or for the specified CP for the given port.

Format `show qcn statistics {interface unit/slot/port cp cp index}`

Command mode: Privileged

11 ROUTING CONFIGURATION COMMANDS

This chapter describes the routing commands available in the CLI. The Routing Commands chapter contains the following sections:

All commands listed in this section are divided into three functional groups:

- **Show commands display switch configuration information, statistics, and other information.**
- **Configuration commands configure switch features. 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.**

11.1 ARP (Address Resolution Protocol) configuration commands

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

arp

This command creates an ARP entry in the specified virtual router instance (vrf vrf-name). If a virtual router is not specified, the static ARP entry is created in the default router. The value for ipaddress is the IP address of a device on a subnet attached to an existing routing interface. The parameter macaddr is a unicast MAC address for that device. The interface parameter specifies the next hop interface.

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

Format: `arp [vrf vrf-name] ipaddress macaddr interface {unit/slot/port | vlan id}`

Command mode: Global Config

no arp

This command deletes an ARP entry in the specified virtual router. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device. The *interface* parameter specifies the next hop interface.

Format: `no arp [vrf vrf-name] ipaddress macaddr interface unit/slot/port`

Command mode: Global Config

ip proxy-arp

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

Default: enabled

Format: `ip proxy-arp`

Command mode: Interface Config

no ip proxy-arp

This command disables proxy ARP on a router interface.

Format: `no ip proxy-arp`

Command mode: Interface Config

ip local-proxy-arp

Use this command to allow an interface to respond to ARP requests for IP addresses within the subnet and to forward traffic between hosts in the subnet.

Default: disabled

Format: `ip local-proxy-arp`

Command mode: Interface Config

no ip local-proxy-arp

This command resets the local proxy ARP mode on the interface to the default value.

Format: `no ip local-proxy-arp`

Command mode: Interface Config

arp cachesize

This command configures the ARP cache size.

Default: 6144

Format: `arp cachesize` *`platform specific integer value`*

Command mode: Global Config

no arp cachesize

This command configures the default ARP cache size.

Format: `no arp cachesize`

Command mode: Global Config

arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out. When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. Traffic to the host may be lost until the router receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option applies only to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of

potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Default: disabled

Format: `arp dynamicrenew`

Command mode: Privileged

no arp dynamicrenew

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

Format: `no arp dynamicrenew`

Command mode: Privileged

arp purge

This command causes the specified IP address to be removed from the ARP cache in the specified virtual router. If no router is specified, the ARP entry is deleted in the default router. Only entries of type dynamic or gateway are affected by this command.

Format: `arp purge [vrf vrf-name] ipaddress interface {unit/slot/port | vlan id}`

Command mode: Privileged

Parameter	*Description*
ipaddress	The IP address to remove from the ARP cache.
vrf-name	The virtual router from which IP addresses will be removed.
interface	The interface from which IP addresses will be removed.

arp resptime

This command configures the ARP request response timeout.

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

Default: 1

Format: `arp resptime 1-10`

Command mode: Global Config

no arp resptime

This command configures the default ARP request response timeout.

Format: `no arp resptime`

Command mode: Global Config

arp retries

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

Default: 4

Format: `arp retries 0-10`

Command mode: Global Config

no arp retries

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

Format: `no arp retries`

Command mode: Global Config

arp timeout

This command configures the ARP entry ageout time.

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

Default: 1200

Format: `arp timeout` *`15-21600`*

Command mode: Global Config

no arp timeout

This command configures the default ARP entry ageout time.

Format: `no arp timeout`

Command mode: Global Config

clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache for the virtual router. If no router is specified, the cache for the default router is cleared. If the gateway keyword is specified, the dynamic entries of type gateway are purged as well.

Format: `clear arp-cache [vrf` *`vrf-name`*`] [gateway]`

Command mode: Privileged

clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, *ping* from the remote system to the DUT. Issue the *show arp switch* command to see the ARP entries. Then issue the *clear arp-switch* command and check the *show arp switch* entries. There will be no more arp entries.

Format: `clear arp-switch`

Command mode: Privileged

show arp

This command displays the Address Resolution Protocol (ARP) cache for a specified virtual router instance. If a virtual router is not specified, the ARP cache for the default router is displayed. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the *show arp* results in conjunction with the *show arp switch* results.

Format: `show arp [vrf` *`vrf-name`*`]`

Command mode: Privileged

Term	*Value*
Age Time (seconds)	ARP record lifetime. The value can be configured. Measured in seconds.
Response Time (seconds)	ARP request lifetime. The value can be configured. Measured in seconds.
Retries	Maximum number of repeated ARP requests.
Cache Size	Maximum number of records in the ARP table.
Dynamic Renew Mode	Indicates whether the system attempts to automatically update dynamic ARP records as they become obsolete.
Total Entry Count Current / Peak	The total number of records in the ARP table and the maximum number of records in the ARP table.
Static Entry Count Current / Max	Number of static records in the ARP table and the maximum number of static records in the ARP table.

The following are displayed for each ARP entry:

Term	*Value*
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing *unit/slot/port* associated with the device ARP entry.
Type	The type that is configurable. Possible values are: Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format).

show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information for a specified virtual router instance. If a virtual router is not specified, the ARP cache for the default router is displayed.

Format: `show arp brief [vrf vrf-name]`

Command mode: Privileged

Term	*Value*
Age Time (seconds)	ARP record lifetime. The value can be configured. Measured in seconds.
Response Time (seconds)	ARP request lifetime. The value can be configured. Measured in seconds.
Retries	Maximum number of repeated ARP requests.
Cache Size	Maximum number of records in the ARP table.
Dynamic Renew Mode	Indicates whether the system attempts to automatically update dynamic ARP records as they become obsolete.
Total Entry Count Current / Peak	The total number of records in the ARP table and the maximum number of records in the ARP table.
Static Entry Count Current / Max	Number of static records in the ARP table and the maximum number of static records in the ARP table.

show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format: `show arp switch`

Command mode: Privileged

Term	*Value*
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing *unit/slot/port* associated with the device ARP entry.

11.2 IP Routing configuration commands

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

routing

This command enables IPv4 and IPv6 routing for an interface or range of interfaces. You can view the current value for this function with the show ip brief command. The value is labeled as "Routing Mode."

Default: disabled

Format: `routing`

Command mode: Interface Config

no routing

This command disables routing for an interface.

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

Format: `no routing`

Command mode: Interface Config

ip routing

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

Format: `ip routing`

Command mode: Global Config
Virtual Router Config

no ip routing

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

Format: `no ip routing`

Command mode: Global Config

ip address

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface. The command supports RFC 3021 and accepts using 31-bit prefixes on IPv4 point-to-point links.

The 31-bit subnet mask is only supported on routing interfaces. The feature is not supported on network port and service port interfaces because switch acts as a host, not a router, on these management interfaces. The 32-bit subnet mask is only supported on loopback interfaces.

Format: `ip address` *ipaddr* {*subnetmask* | */masklen*} `[secondary]`

Command mode: Interface Config

Term	*Value*
ipaddr	IP address of the interface.
subnetmask	A 4-digit dotted-decimal number which represents the subnet mask of the interface.
masklen	Implements RFC 3021. Using the "/" notation of the subnet mask, this is an integer that indicates the length of the subnet mask. Range is 5 to 32 bits.

no ip address

This command deletes an IP address from an interface. The value for ipaddr is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for subnetmask is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command no ip address.

Format: `no ip address [{`*ipaddr subnetmask* `[secondary]}]`

Command mode: Interface Config

ip address dhcp

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

To enable the DHCPv4 client on an in-band interface and send DHCP client messages with the client identifier option, use the ip address dhcp client-id configuration command in Interface Config.

Default: disabled

Format: `ip address dhcp [client-id]`

Command mode: Interface Config

no ip address dhcp

The *no ip address dhcp* command releases a leased address and disables DHCPv4 on an interface. The no form of the *ip address dhcp client-id* command removes the *client-id* option and also disables the DHCP client on the in-band interface.

Format: `no ip address dhcp [client-id]`

Command mode: Interface Config

ip default-gateway

This command manually configures a default gateway for the switch. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway. The system installs a default IPv4 route with the gateway address as the next hop address. The route preference is 253. A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server.

Format: `ip default-gateway` *ipaddr*

Command mode: Global Config
Virtual Router Config

Parameter	*Description*
Ipaddr	The IPv4 address of an attached router.

no ip default-gateway

This command removes the default gateway address from the configuration.

Format: `no ip default-gateway` *ipaddr*

Command mode: Interface Config

ip load-sharing

This command configures IP ECMP load balancing mode.

Default: 6

Format: `ip load-sharing` *mode* `{inner | outer}`

Command mode: Global Config

Parameter	*Description*
mode	Configures the load balancing or sharing mode for all EMCP groups. • src-ip: Based on a hash using the Source IP address of the packet. • dst-ip: Based on a hash using the Destination IP address of the packet. • src-dst-ip: Based on a hash using the Source and Destination IP addresses of the packet. • src-ip-port: Based on a hash using the Source IP address and the Source TCP/UDP Port field of the packet. • dst-ip-port: Based on a hash using the Destination IP address and the Destination TCP/UDP Port field of the packet. • src-dst-ip-port: Based on a hash using the Source and Destination IP address, and the Source and Destination TCP/UDP Port fields of the packet.
inner	Use the inner IP header for tunneled packets.
outer	Use the outer IP header for tunneled packets.

no ip load-sharing

Format: `no ip load-sharing`

Command mode: Global Config

ip route

This command configures a static route in a specified virtual router instance (vrf vrf-name). The *ipaddr* parameter is a valid IP address, and *subnetmask* is a valid subnet mask. The *nexthopip* parameter is a valid IP address of the next hop router. Specifying Null0 as nexthop parameter adds a static reject route. The optional preference parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The *preference* also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

The *description* parameter allows a description of the route to be entered.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Default: preference — 1

Format: `ip route [vrf vrf-name] ipaddr subnetmask { nexthopip | Null0 | interface {unit/slot/ port| vlan-id}} [preference] [description description]`

Command mode: Global Config

no ip route

This command deletes a single next hop to a destination static route. If you use the *nexthopip* parameter, the next hop is deleted. If you use the *preference* value, the preference value of the static route is reset to its default.

Format: `no ip route ipaddr subnetmask [{nexthopip [preference] | Null0}]`

Command mode: Global Config

ip route default

This command configures the default route. The value for nexthopip is a valid IP address of the next hop router. The preference is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default: preference — 1

Format: `ip route default nexthopip [preference]`

Command mode: Global Config

no ip route default

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

Format: `no ip route default [{nexthopip | preference}]`

Command mode: Global Config

ip route distance

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

Default: 1

Format: `ip route distance 1-255`

Command mode: Global Config

no ip route distance

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

Format: `no ip route distance`

Command mode: Global Config

ip route net-prototype

This command adds net prototype IPv4 routes to the hardware.

Format: `ip route net-prototype prefix/prefix-length nexthopip num-routes`

Command mode: Global Config

Parameter	***Description***
prefix/prefix-length	The destination network and mask for the route.
nexthopip	The next-hop ip address, It must belong to an active routing interface, but it does not need to be resolved.
num-routes	The number of routes need to added into hardware starting from the given prefix argument and within the given prefix-length.

no ip route net-prototype

This command deletes all the net prototype IPv4 routes added to the hardware.

Format: `ip route net-prototype prefix/prefix-length nexthopip num-routes`

Command mode: Global Config

ip netdirbcast

This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces.

Default: disabled

Format: *ip netdirbcast*

Command mode: Interface Config

no ip netdirbcast

This command disables the forwarding of network-directed broadcasts.

Format: *no ip netdirbcast*

Command mode: Interface Config

ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation.

Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface. Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.

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

The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets,the Ethernet MTU (see mtu) must take into account the size of the Ethernet header.

Default: 1500 bytes

Format: ip mtu *68-12270* (for MES5448)/ip mtu *68-9394* (for MES7048)

Command mode: Interface Config

no ip mtu

This command resets the ip mtu to the default value.

Format: no ip mtu

Command mode: Interface Config

release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface. The DHCP client sends a DHCP Release message telling the DHCP server that it no longer needs the IP address, and that the IP address can be reassigned to another.

Format: release dhcp {*unit/slot/port* | vlan *id*}

Command mode: Privileged

renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

This command can be used on in-band ports as well as the service or network (out-of-band) port.

Format: `renew dhcp {unit/slot/port | vlan id}`

Command mode: Privileged

renew dhcp network-port

Use this command to renew an IP address on a network port.

Format: `renew dhcp network-port`

Command mode: Privileged

renew dhcp service-port

Use this command to renew an IP address on a service port.

Format: `renew dhcp service-port`

Command mode: Privileged

encapsulation

This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be ethernet or snap.

Default: ethernet

Format: `encapsulation {ethernet | snap}`

Command mode: Interface Config

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

show dhcp lease

This command displays a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. This command does not apply to service or network ports.

Format: `show dhcp lease [interface {unit/slot/port | vlan id}]`

Command mode: Privileged

Parameter	*Description*
IP address, Subnet mask	The IP address and network mask leased from the DHCP serverю
DHCP Lease server	The IPv4 address of the DHCP server that leased the address.
State	State of the DHCPv4 Client on this interface.
DHCP transaction ID	The transaction ID of the DHCPv4 Client.
Lease	The time (in seconds) that the IP address was leased by the server.
Renewal	The time (in seconds) when the next DHCP renew Re-

	quest is sent by DHCPv4 Client to renew the leased IP address.
Rebind	The time (in seconds) when the DHCP Rebind process starts.
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds.

show ip brief

This command displays the summary information of the IP global configurations for the specified virtual router, including the ICMP rate limit configuration and the global ICMP Redirect configuration. If no router is specified, information related to the default router is displayed.

Format: `show ip brief [vrf vrf-name]`

Command mode: Privileged
User

Term	*Value*
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. Burst-intervalis 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.

show ip interface

This command displays all pertinent information about the IP interface. The argument *unit/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 in a *unit/slot/port* format.

Format: `show ip interface {unit/slot/port|vlan 1-4094|loopback 0-7}`

Command mode: Privileged
User

Term	*Value*
Routing Interface Status	Determine the operational status of IPv4 routing Interface. Possible values are: Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.

Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the ip helper-address command.
Routing Mode	The administrative mode of router interface participation. Possible values are: enable or disable.
Administrative Mode	The administrative mode of the specified interface. Possible values are: enable or disable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. Format: 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The format is 6 two-digit hexadecimal numbers that are separated by colons. Possible types: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the *client-id* option on the in-band interface.

show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router, and indicates how each IP address was assigned for a specified virtual router instance. If a virtual router is not specified, the IP configuration settings cache for the default router is displayed.

Format: `show ip interface [vrf vrf-name] brief`

Command mode: Privileged
User

Term	***Value***
Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.

IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Method	Indicates how each IP address was assigned. The field contains one of the following values: • DHCP — the address is leased form a DHCP server; • Manual — the address is manually configured.

show ip load-sharing

This command displays the currently configured IP ECMP load balancing mode.

Format: `show ip load-sharing`

Command mode: Privileged

show ip protocols

This command lists a summary of the configuration and status for each unicast routing protocol running in the specified virtual router. The command lists routing protocols which are configured and enabled. If a protocol is selected on the command line, the display will be limited to that protocol. If no virtual router is specified, the configuration and status for the default router are displayed.

Format: `show ip protocols [vrf` *`vrf-name`*`] [bgp|ospf|rip]`

Command mode: Privileged

Term	*Value*
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 an 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.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked “active”.
Neighbors	A list of configured neighbors and the inbound and out-bound policies configured for each.
OSPFv2 section	
Routing Protocol	OSPFv2.
Router ID	The router ID configured for OSPFv2.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.
Routing for Networks	The address ranges configured with an OSPF network command.
Distance	The administrative distance (or “route preference”) for intra-area, inter-area, and external routes.
Default Route Advertise	Whether OSPF is configured to originate a default route.
Always	Whether default advertisement depends on having a default route in the common routing table.
Metric	The metric configured to be advertised with the default route.
Metric Type	The metric type for the default route.
Redist Source	A type of routes that OSPF is redistributing.
Metric	The metric to advertise for redistributed routes of this type.
Metric Type	The metric type to advertise for redistributed routes of this type.
Subnets	Whether OSPF redistributes subnets of classful addresses, or only classful prefixes.
Dist List	A distribute list used to filter routes of this type. Only routes that pass the distribute list are redistributed.
Number of Active Areas	The number of OSPF areas with at least one interface running on this router. Also broken down by area type.
ABR Status	Whether the router is currently an area border router. A router is an area border router if it has interfaces that are up in more than one area.
ASBR Status	Whether the router is an autonomous system boundary

	router. The router is an ASBR if it is redistributing any routes or originating a default route.
RIP section	
RIP Admin Mode	Whether RIP is globally enabled.
Split Horizon Mode	Whether RIP advertises routes on the interface where they were received.
Default Metric	The metric assigned to redistributed routes.
Default Route Advertise	Whether this router is originating a default route.
Distance	The administrative distance for RIP routes.
Redistribution	A table showing information for each source protocol (connected, static, bgp, and ospf). For each of these source the **distribution list** and **metric** are shown. Fields which are not configured are left blank. For ospf, configured **ospf match** parameters are also shown.
Interface	The interfaces where RIP is enabled and the version sent and accepted on each interface.

show ip route

This command displays the routing table for the specified virtual router (*vrf vrf-name*). If no router is specified, the routing table for the default router is displayed. The *ip-address* specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The *mask* specifies the subnet mask for the given ip-address. When you use the *longer-prefixes* keyword, the *ip-address* and *mask* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the *protocol* parameter to specify the protocol that installed the routes. The value for *protocol* can be *connected, ospf, rip, static*, or *bgp*. Use the *all* parameter to display all routes including best and nonbest routes. If you do not use the *all* parameter, the command displays only the best route.

If you use the *connected* keyword for protocol, the all option is not available because there are no best or nonbest connected routes.

If you use the *static* keyword for protocol, the description option is also available, for example: show ip route *ip-address* static description. This command shows the description of the specified static route.

Format: `show ip route [vrf vrf-name] [{ip-address [protocol] | {ip-address mask [longer- prefixes] [protocol] | protocol} [all] | all}]`

Command mode: Privileged

User

Term	*Value*
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The show ip route command displays the routing tables in the following format:

```
Code IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface, Truncated
```

The columns for the routing table display the following information:

Term	*Value*
Code	The code for the routing protocol that created this routing entry.
Default Gateway	The IP address of the default gateway. When the system

	does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route- Timestamp	The last updated time for dynamic routes. The format for the route-timestamp will be: • Days:Hours:Minutes if days > = 1 • dd:hh:mm, if days have passed < = 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 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/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

show ip route ecmp-groups

This command reports all current ECMP groups in the IPv4 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv4 address and outgoing interface of each next hop in each group.

Format: `show ip route ecmp-groups`

Command mode: Privileged

show ip route hw-failure

Use this command to display the routes that failed to be added to the hardware due to hash errors or a table full condition.

Format: `show ip route hw-failure`

Command mode: Privileged

show ip route net-prototype

This command displays the net-prototype routes. The net-prototype routes are displayed with a P.

Format: `show ip route net-prototype`

Command mode: Privileged

show ip route summary

This command displays a summary of the state of the routing table. When the optional all keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

Format: `show ip route summary [all]`

Command mode: Privileged
User

Term	*Value*
Connected Routes	Total number of routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by the BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.
OSPF Routes	Total number of routes installed by OSPF protocol.
Intra Area Routes	Total number of Intra Area routes installed by OSPF protocol.
External Type-1 Routes	Total number of External Type-1 routes installed by OSPF protocol.
External Type-2 Routes	Total number of External Type-2 routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Net Prototype Routes	The number of net-prototype routes.
Total Routes	Total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination. The value in parentheses indicates the highest count of unique best routes since counters were last cleared.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the

	routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Hardware Failed Route Adds	The number of routes failed be inserted into the hardware due to hash error or a table full condition.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes. The value in parentheses indicates the highest count of unique next hops since counters were last cleared.
Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups (High)	The number of next hop groups with multiple next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	The current number of routes with each number of next hops.

clear ip route counters

The command resets to zero the IPv4 routing table counters reported in the command “show ip route summary” for the specified virtual router. If no router is specified, the command is executed for the default router. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format: `clear ip route counters [vrf vrf-name]`

Command mode: Privileged

show ip route preferences

This command displays detailed information about the route preferences for each type of route. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format: `show ip route preferences`

Command mode: Privileged
User

Term	*Value*
Local	The local route preference value.
Static	The static route preference value.
BGP External	The BGP external route preference value.
OSPF Intra	The OSPF Intra route preference value.
OSPF Inter	The OSPF Inter route preference value.
OSPF External	The OSPF External route preference value.
RIP	The RIP route preference value.
BGP Internal	The BGP internal route preference value.
BGP Local	The BGP local route preference value.
Configured Default Gateway	The route preference value of the statically-configured default gateway.
DHCP Default Gateway	The route preference value of the default gateway learned from the DHCP server.

show ip stats

This command displays IP statistical information for a specified virtual router instance. If a virtual router is not specified, the IP statistical information for the default router is displayed.

Format: `show ip stats [vrf vrf-name]`

Command mode: Privileged
User

show routing heap summary

This command displays a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing applications.

Format: `show routing heap summary`

Command mode: Privileged

Parameter	*Description*
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

11.3 Routing Policy configuration commands

ip policy route-map

Use this command to 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 a route-map applied on the interface is changed, that is, if new statements are added to route-map or match/set terms are added/removed from route-map statement, and also if *route-map* that is applied on an interface is removed, route-map needs to be removed from interface and added back again in order to have changed route-map configuration to be effective.

Route-map and DiffServ cannot work on the same interface.

Format: `ip policy` *`route-map-name`*

Command mode: Interface Config

Parameter	*Description*
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

ip prefix-list

To create a prefix list or add a prefix list entry, use the ip prefix-list command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes of 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.

An empty or nonexistent prefix list permits all prefixes. An implicit deny is assume 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.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

Default: No prefix lists are configured by default.

Format: `ip prefix-list` *`list-name`* {[`seq` *`number`*] {`permit` | `deny`} *`network/length`* [`ge` *`length`*] [`le` *`length`*] | `renumber` *`renumber-interval first-statement-number`*}

Command mode: Global Config

Parameter	***Description***
list-name	The text name of the prefix list. The length is 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.
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	(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.

no ip prefix-list

To delete a prefix list or a statement in a prefix list, use the **no** form of this command. 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.

Format: `no ip prefix-list` *`list-name`* `[seq` *`number`*`] { permit | deny } net-work/length [ge` *`length`*`] [le` *`length`*`]`

Command mode: Global Config

ip prefix-list description

To apply a text description to a prefix list, use the **ip prefix-list** description command in Global Configuration mode.

Default: No description is configured by default.

Format: `ip prefix-list` *`list-name`* `description` *`text`*

Command mode: Global Config

Parameter	*Description*
list-name	The text name of the prefix list.
description text	Text description of the prefix list. Up to 80 characters.

no ip prefix-list description

To remove the text description, use the **no** form of this command.

Format: `no ip prefix-list list-name description`

Command mode: Global Config

ipv6 prefix-list

Use this command to 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 of 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 assume 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. 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.

Default: No prefix lists are configured by default.

Format: `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`*`}`

Command mode: Global Config

Parameter	*Description*
list-name	The text name of the prefix list. The length is 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 IPv6 prefix where the address is specified in hexadecimal using 16-bit values between colons. The prefix-length value 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 length	(Optional) If this option is configured, specifies a prefix length greater than or equal to the ipv6-prefix/prefix-length. It is the lowest value of a range of the length.
le length	(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	A description of the prefix list. It can be up to 80 characters in length.
renumber	(Optional) Provides the option to renumber the sequence numbers of the IPv6 prefix list statements with a given interval starting from a particular sequence number.

no ipv6 prefix-list

Use this command to deletes either the entire prefix list or an individual statement from a prefix list.

Format: `ipv6 prefix-list` *`list-name`*

Command mode: Global Config

The description must be removed using no ip prefix-list description before using this command to delete an IPv6 Prefix List.

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. The software accepts up to 64 route maps.

Default: No route maps are configured by default. If no permit or deny tag is given, permit is the default.

Format: `route-map map-tag [permit|deny] [sequence-number]`

Command mode: Global Config

Parameter	*Description*
map-tag	Text name of the *route-map*. *Route-map*s 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) An integer used to order the set of *route-map*s with the same name. *Route-map*s 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.

no route-map

To delete a *route-map* or one of its statements, use the no form of this command.

Format: `no route-map` *`map-tag`* `[permit|deny] [`*`sequence-number`*`]`

Command mode: Global Config

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.

Format: `match as-path` *`as-path-list-number`*

Command mode: Route Map Configuration

Parameter	*Description*
as-path-list-number	An integer from 1 to 500 identifying the AS path access list to use as match criteria.

no match as-path

This command deletes the match as-path term that matches BGP autonomous system paths against an AS path access list.

Format: `no match as-path as-path-list-number`

Command mode: Route Map Configuration

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.

Format: match community *community-list* [*community-list...*] [exact-match]
Command mode: Route Map Configuration

Parameter	*Description*
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.

no match community

To delete a match term from a route map, use the **no** form of this command. The *no match community list exact-match* command removes the match statement from the *route-map*. (It does not simply remove the exact-match option.) The *no match community* command removes the match term and all its community lists.

Format: no match community *community-list* [*community-list...*] [exact-match]

Command mode: Route Map Configuration

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.

Default: No match criteria are defined by default.

Format: match ip address prefix-list *prefix-list-name* [*prefix-list-name...*]

Command mode: Route Map Configuration

Parameter	*Description*
prefix-list-name	The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

no match ip address

To delete a match statement from a route-map, use the **no** form of this command.

Format: no match ip address [prefix-list *prefix-list-name* [*prefix-list-name...*]]

Command mode: Route Map Configuration

match ip address <access-list-number | access-list-name>

Use this command to configure a route map in order to match based on the match criteria configured in an IP access-list. Note that an IP ACL 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 IP

ACL 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.

Default: No match criteria are defined by default.

Format: `match ip address` *`access-list-number`* | *`access-list-name`* `[...access-list-number| name ]`

Command mode: Route Map Configuration

Parameter	***Description***
Access-list-number	The access-list number that 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	The access-list name that 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.

no match ip address

To delete a match statement from a route-map, use the **no** form of this command.

Format: `no match ip address [`*`access-list-number`* | *`access-list-name`*`]`

Command mode: Route Map Configuration

match ipv6 address

Use this command to configure a route map to match based on a destination prefix. **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 may 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.

Default: No match criteria are defined by default.

Format: `match ipv6 address prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]`

Command mode: Route Map Configuration

no match ipv6 address

To delete a match statement from a route map, use the no form of this command.

Format: `no match ipv6 address prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]]`

Command mode: Route Map Configuration

match length

Use this command to 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 packet's maximum Layer 3 length, inclusive, allowed for a match. Each *route-map* statement can contain one 'match' statement on packet length range.

Default: No match criteria are defined by default.

Format: `match length min max`

Command mode: Route Map Configuration

no match length

Use this command to delete a match statement from a route-map.

Format: `no match length`

Command mode: Route Map Configuration

match mac-list

Use this command to configure a route map in order to match based on the match criteria configured in an 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 or rules are added or deleted from that ACL, the configuration is rejected.

Default: No match criteria are defined by default.

Format: `match mac-list mac-list-name [mac-list-name]`

Command mode: Route Map Configuration

Parameter	*Description*
mac-list-name	The mac-list name that identifies MAC ACLs. MAC Access-list name can be up to 31 characters in length.

no match mac-list

To delete a match statement from a route-map, use the **no** form of this command.

Format: `no match mac-list [...mac-list-name]`

Command mode: Route Map Configuration

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.

Format: `set as-path prepend` *`as-path-string`*

Command mode: Route Map Configuration

Parameter	*Description*
as-path-string	A 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.

no set as-path

To remove a *set* command from a *route-map*, use the **no** form of this command.

Format: `no set as-path prepend` *`as-path-string`*

Command mode: Route Map Configuration

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).

Format: `set comm-list` *`community-list-name`* `delete`

Command mode: Route Map Configuration

Parameter	*Description*
community-list-name	A standard community list name.

no set comm-list

To delete the *set* command from a *route-map*, use the **no** form of this command.

Format: `no set comm-list`

Command mode: Route Map Configuration

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.

Format: `set community {`*`community-number`* `[additive] | none}`
Command mode: Route Map Configuration

Parameter	*Description*
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	(Optional) Removes all communities from matching routes.

no set community

To remove a *set* term from a *route-map*, use the **no** form of this command.

Format: `no set community`
Command mode: Route Map Configuration

set interface

If network administrator does not want to revert to normal forwarding but instead want 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.

Format: `set interface null0`
Command mode: Route Map Configuration

set ip next-hop

Use this command to 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.

Format: `set ip next-hop ip-address [...`*`ip-address`*`]`

Command mode: Route Map Configuration

Parameter	*Description*
ip-address	The 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.

no set ip next-hop

Use this command to remove a *set* command from a *route-map*.

Format: `no set ip next-hop ip-address [...ip-address]`

Command mode: Route Map Configuration

set ip default next-hop

Use this command to set a list of default next-hop IP addresses. If more than one IP address is specified, the first next hop specified that appears to be adjacent to the router 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.

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.

Format: `set ip default next-hop ip-address [...ip-address]`

Command mode: Route Map Configuration

Parameter	*Description*
ip-address	The 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.

no set ip default next-hop

Use this command to remove a *set* command from a *route-map*.

Format: `no set ip default next-hop ip-address [...ip-address]`

Command mode: Route Map Configuration

set ip precedence

Use this command to set the three IP precedence bits in the IP packet header. With three bits, you have eight possible values for the IP precedence: from 0 to 7. 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).

Format: `set ip precedence 0-7`

Command mode: Route Map Configuration

Parameter	*Description*
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 Flash override precedence
6	Sets the internetwork control precedence
7	Sets the network control precedence

no set ip precedence

Use this command to reset the three IP precedence bits in the IP packet header to the default.

Format: `no set ip precedence`

Command mode: Route Map Configuration

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.

Format: `set ipv6 next-hop` *`ipv6-address`*

Command mode: Route Map Configuration

Parameter	*Description*
ipv6-address	The IPv6 address set as the Network Address of Next Hop field in the MP_NLRI attribute of an UPDATE message.

no set ipv6 next-hop (BGP)

To remove a **set** command from a route-map, use the **no** form of this command.

Format: `no set ipv6 next-hop`

Command mode: Route Map Configuration

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. When used in conjunction with a "*matchas-path*" or "*match ip address*" command, this command can be used to prefer routes that transit certain ASs or to make the local router a more preferred exit point to certain destinations.

Format: `set local-preference value`
Command mode: Route Map Configuration

Parameter	*Description*
value	A local preference value, from 0 to 4,294,967,295 (any 32-bit integer).

no set local-preference

To remove a *set* command from a route map, use the **no** form of this command.

Format: `no set local-preference value`

Command mode: Route Map Configuration

set metric (BGP)

To set the metric of a route, use the *set metric* command in *Route Map Configuration* mode. This command sets the Multi Exit Discriminator (MED) when used in a BGP context. 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.

Format: `set metric value`
Command mode: Route Map Configuration

Parameter	*Description*
value	A metric value, from 0 to 4,294,967,295 (any 32-bit integer).

no set metric (BGP)

To remove a *set* command from a *route-map*, use the **no** form of this command.

Format: `no set metric value`

Command mode: Route Map Configuration

show ip policy

This command lists the *route-map* associated with each interface.

Format: `show ip policy`

Command mode: Privileged

Parameter	*Description*
Interface	The interface
Route-map	The route-map

show ip prefix-list

This command displays configuration and status for a prefix list.

Format: `show ip prefix-list [detail | summary] prefix-list-name [network/length] [seq sequence-number] [longer] [first-match]`

Command mode: Privileged

Parameter	*Description*
detail | summary	The interface
prefix-list-name	(Optional) The name of a specific prefix list.
network/length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.
sequence-number	(Optional) 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`

show ipv6 prefix-list

This command displays configuration and status for a selected prefix list.

Format: `show ipv6 prefix-list [detail | summary] listname [ipv6-prefix/prefix-length] [seq sequence- number] [longer] [first-match]`

Command mode: Privileged

Parameter	*Description*
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
list-name	(Optional) The name of a specific prefix list.
ipv6-prefix/prefix- length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.
sequence-number	(Optional) 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`

The command outputs the following information.

Parameter	*Description*
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	The action to take.
sequences	Range of sequence numbers for the entries in the list.
hit count	Number of matches for the prefix entry.

show route-map

To display a route-map, use the *show route-map* command in Privileged mode.

Format: `show route-map [map-name]`

Command mode: Privileged

Parameter	*Description*
map-name	(Optional) Name of a specific route map.

clear ip prefix-list

To reset IP prefix-list counters, use the *clear ip prefix-list* command in Privileged 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.

Format: `clear ip prefix-list [[prefix-list-name] [network/length]]`

Command mode: Privileged

Parameter	*Description*
prefix-list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
network/length	(Optional) The network number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

clear ipv6 prefix-list

Use this command to 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.

Format: `clear ipv6 prefix-list [`*`prefix-list-name`*`] [ipv6-prefix/`*`prefix-length`*`]`

Command mode: Privileged

Parameter	*Description*
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.

11.4 Router Discovery Protocol commands

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

ip irdp

This command enables IRPD on an interface or range of interfaces.

Default: disabled

Format: `ip irdp`

Command mode: Interface Config

no ip irdp

This command disables IRDP on an interface.

Format: `no ip irdp`

Command mode: Interface Config

ip irdp address

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

Default: 224.0.0.1

Format: `ip irdp address` *`ipaddr`*

Command mode: Interface Config

no ip irdp address

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

Format: `no ip irdp address`

Command mode: Interface Config

ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of 4 to 9000 seconds.

Default: 3 * maxinterval

Format: `ip irdp holdtime` *`4-9000`*

Command mode: Interface Config

no ip irdp holdtime

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

Format: `no ip irdp holdtime`

Command mode: Interface Config

ip irdp maxadvertinterval

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

Default: 600

Format: `ip irdp maxadvertinterval` *`4-1800`*

Command mode: Interface Config

no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format: `no ip irdp maxadvertinterval`

Command mode: Interface Config

ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is 3–1800.

Default: 0.75 * maxadvertinterval

Format: `ip irdp minadvertinterval` *`3-1800`*

Command mode: Interface Config

no ip irdp minadvertinterval

This command sets the default minimum time to the default.

Format: `no ip irdp minadvertinterval`

Command mode: Interface Config

ip irdp multicast

This command configures the destination IP address for router advertisements as 224.0.0.1, which is the default address. The no form of the command configures the IP address as 255.255.255.255 to instead send router advertisements to the limited broadcast address.

Format: `ip irdp multicast` *`ip address`*

Command mode: Interface Config

no ip irdp multicast

By default, router advertisements are sent to 224.0.0.1. To instead send router advertisements to the limited broadcast address, 255.255.255.255, use the no form of this command.

Format: `no ip irdp multicast`

Command mode: Interface Config

ip irdp preference

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

Default: 0

Format: `ip irdp preference` *`-2147483648 to 2147483647`*

Command mode: Interface Config

no ip irdp preference

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

Format: `no ip irdp preference`

Command mode: Interface Config

show ip irdp

This command displays the router discovery information for all interfaces, a specified interface, or specified VLAN. The argument *unit/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 *unit/slot/port* format.

Format: `show ip irdp {`*`unit/slot/port`*`|vlan` *`1-4093`*`|all}`

Command mode: Privileged
User

Parameter	*Description*
Interface	The unit/slot/port that corresponds to a physical routing interface or vlan routing interface.
vlan	Use this keyword to specify the VLAN ID of the routing VLAN directly instead of in a *unit/ slot/port* format.
Ad Mode	The advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Dest Address	The destination IP address for router advertisements.

Max Int	The maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	The minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	The amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	The preference of the address as a default router address, relative to other router addresses on the same subnet.

11.5 Virtual Router configuration commands

ip vrf

This command creates a virtual router with a specified name and enters VRF configuration mode.

Default: No VRs are defined

Format: `ip vrf` *vrf-name*

Command mode: Global Config

Parameter	*Description*
vrf-name	The name of the virtual router. The name is a string of up to 64 characters from an ASCII set.

no ip vrf

Deletes the virtual router with the specified name.

Format: `no ip vrf` *vrf-name*

Command mode: Global Config

maximum routes

This command reserves the number of routes allowed and sets 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.

Default: Limited by the number of free routes available.

Format: `maximum routes {`*limit* | `warn` *threshold*`}`

Command mode: Virtual Router Config

Parameter	*Description*
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.

no maximum routes

This command removes any reservation for the number of routes allowed in the virtual router instance and clears the warning threshold value.

Format: `no maximum routes`

Command mode: Virtual Router Config

description

This command allows the user to configure a descriptive text for a virtual router.

Default: none

Format: `description` *`text`*

Command mode: Virtual Router Config

Parameter	*Description*
Text	The descriptive text for the virtual router. A set of ASCII characters up to 512 characters in length.

no description

This command removes the descriptive text configuration for a virtual router.

Format: `no description`

Command mode: Virtual Router Config

ip vrf forwarding

This command associates an IP interface with a virtual router.

Default: Default router

Format: `ip vrf forwarding` *`vrf-name`*

Command mode: Interface Config

Parameter	*Description*
vrf-name	The name of the virtual router.

no ip vrf forwarding

This command disassociates an IP interface from the configured virtual router and associates it back to the default router.

Format: `no ip vrf forwarding`

Command mode: Interface Config

show ip vrf

This command displays information about the virtual router instances.

Default: none

Format: `show ip vrf [{`*`vrf-name`* `| detail` *`vrf-name`* `| interfaces | memory [`*`vrf-name`*`]}]`

Command mode: Privileged

Parameter	*Description*
vrf-name	Name of the virtual router instance.

detail	Displays the configuration and status of the virtual router.
interfaces	Displays the list of interfaces and the virtual routers to which they belong.
memory	Displays the runtime memory utilization of the processes running in a virtual router.

11.6 VLAN Routing configuration commands

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

vlan routing

This command enables routing on a VLAN. The *vlanid* value has a range from 1 to 4093. The [interface ID] value has a range from 1 to 256. Typically, you will not supply the interface ID argument, and the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the *unit/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 *unit/slot/port* for the VLAN interface stays the same across a restart. Keeping the *unit/slot/port* the same ensures that the correct interface configuration is applied to each interface when the system restarts.

Format: `vlan routing` *`vlanid`* [*`interface ID`*]

Command mode: VLAN Config

no vlan routing

This command deletes routing on a VLAN.

Format: `no vlan routing` *`vlanid`*

Command mode: VLAN Config

Typically, you press **<Enter>** without supplying the Interface ID value; the system automatically selects the interface ID.

interface vlan

Use this command to enter Interface Config for the specified VLAN. The vlan-id range is 1 to 4094.

Format: `interface vlan` *`vlan-id`*

Command mode: Global Config

show ip vlan

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

Format: `show ip vlan`

Command mode: Privileged
User

Parameter	***Description***

MAC Address used by Routing VLANs	The 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	The identifier of the VLAN.
Logical Interface	The logical unit/slot/port associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.
Subnet Mask	The subnet mask that is associated with this VLAN.

11.7 VRRP configuration commands[1]

This section describes the 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.

ip vrrp (Global Config)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router.

Default: none

Format: `ip vrrp`

Command mode: Global Config

no ip vrrp

Use this command in Global Config mode to disable the default administrative mode of VRRP on the router.

Format: `no ip vrrp`

Command mode: Global Config

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 vrid parameter is the virtual router ID, which has an integer value range from 1 to 255.

Format: `ip vrrp` *vrid*

Command mode: Interface Config

no ip vrrp

Use this 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.

Format: `no ip vrrp` *vrid*

Command mode: Interface Config

[1] This functionality is available with an VRRP license. To activate the license, please contact the technical support.

ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The vrid parameter is the virtual router ID, which has an integer value range from 1 to 255.

Default: disabled

Format: `ip vrrp vrid mode`

Command mode: Interface Config

no ip vrrp mode

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

Format: `no ip vrrp vrid mode`

Command mode: Interface Config

ip vrrp ip

This command sets 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.

Default: none

Format: `ip vrrp vrid ip ipaddr [secondary]`

Command mode: Interface Config

no ip vrrp ip

Use this command in Interface Config mode to delete a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

Format: `no ip vrrp vrid ipaddress secondary`

Command mode: Interface Config

ip vrrp accept-mode

Use this command to allow the VRRP Master to accept ping packets sent to one of the virtual router's IP addresses.

Default: disabled

Format: `ip vrrp vrid accept-mode`

Command mode: Interface Config

no ip vrrp accept-mode

Use this command to prevent the VRRP Master from accepting ping packets sent to one of the virtual router's IP addresses.

Format: `no ip vrrp vrid accept-mode`

Command mode: Interface Config

ip vrrp authentication

This command sets 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.

Default: no authorization

Format: `ip vrrp vrid authentication {none | simple key}`

Command mode: Interface Config

no ip vrrp authentication

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

Format: `no ip vrrp vrid authentication`

Command mode: Interface Config

ip vrrp preempt

This command sets the preemption mode value for the virtual router 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.

Default: enabled

Format: `ip vrrp vrid preempt`

Command mode: Interface Config

no ip vrrp preempt

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

Format: `no ip vrrp vrid preempt`

Command mode: Interface Config

ip vrrp priority

This command sets 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.

Default: 100 unless the router is the address owner, in which case its priority is automatically set to 255.

Format: `ip vrrp vrid priority 1-254`

Command mode: Interface Config

no ip vrrp priority

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

Format: `no ip vrrp vrid priority`

Command mode: Interface Config

ip vrrp timers advertise

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

Default: 1

Format: `ip vrrp vrid timers advertise 1-255`

Command mode: Interface Config

no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface or range of interfaces.

Format: `no ip vrrp vrid timers advertise`

Command mode: Interface Config

ip vrrp track interface

Use this command to 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 if the IP on that interface is up. Otherwise, the tracked interface is down. You can use this command to configure a single interface or range of interfaces. The argument *unit/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 *unit/slot/port* format.

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. If you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10.

Default value: priority: 10

Format: `ip vrrp vrid track interface {unit/slot/port|vlan 1-4093} [decrement priority]`

Command mode: Interface Config

no ip vrrp track interface

Use this command to remove the interface or range of interfaces from the tracked list or to restore the priority decrement to its default.

Format: `no ip vrrp vrid track interface {unit/slot/port|vlan 1-4093} [decrement]`

Command mode: Interface Config

ip vrrp track ip route

Use this command to 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.

Default value: priority: 10

Format: `ip vrrp vrid track ip route ip-address/prefix-length [decrement priority]`

Command mode: Interface Config

no ip vrrp track ip route

Use this command to remove 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.

Format: `no ip vrrp vrid track interface unit/slot/port [decrement]`

Command mode: Interface Config

show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch. The *unit/slot/port* argument 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 *unit/slot/port* format.

Format: `show ip vrrp interface stats {unit/slot/port|vlan 1-4093} vrid`

Command mode: Privileged
User

Parameter	*Description*
Uptime	The time that the virtual router has been up, in days, hours, minutes and seconds.
Protocol	The protocol configured on the interface.
State Transitioned to Master	The total number of times virtual router state has changed to MASTER.

Advertisment Received	The total number of VRRP advertisements received by this virtual router.
Advertisment Interval Errors	The total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
Authentication Failure	The total number of VRRP packets received that don't pass the authentication check.
IP TTL errors	The total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.
Zero Priority Packets Received	The total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	The total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	The total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	The total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
Packet Length Errors	The total number of VRRP packets received with packet length less than length of VRRP header.

show ip vrrp

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

Format: `show ip vrrp`

Command mode: Privileged
User

Parameter	***Description***
VRRP Admin Mode	The administrative mode for VRRP functionality on the switch.
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with invalid VRID for this virtual router.

show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface. The *unit/slot/port* argument corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is the VLAN ID of the routing VLAN instead of in a *unit/slot/port* format. Use the output of the command to verify the track interface and track IP route configurations.

Format: `show ip vrrp interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`} `*`vrid`*

Command mode: Privileged
User

Term	*Value*
IP Address	The configured IP address for the Virtual router.
VMAC address	The VMAC address of the specified router.
Authentication type	The authentication type for the specific virtual router.
Priority	The priority value for the specific virtual router, taking into account any priority decrements for tracked interfaces or routes.
Configured Priority	The priority configured through the ip vrrp vrid priority 1-254 command.
Advertisement interval	The advertisement interval in seconds for the specific virtual router.
Pre-Empt Mode	The preemption mode configured on the specified virtual router.
Administrative Mode	The status (Enable or Disable) of the specific router.
Accept Mode	When enabled, the VRRP Master can accept ping packets sent to one of the virtual router's IP addresses.
State	The state (Master/backup) of the virtual router.

show ip vrrp interface brief

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format: `show ip vrrp interface brief`

Command mode: Privileged
User

Term	*Value*
Interface	The interface in unit/slot/port format
VRID	The router ID of the virtual router.
IP Address	The virtual router IP address.
Mode	Indicates whether the virtual router is enabled or disabled.
State	The state (Master/backup) of the virtual router.

11.8 VRRPv3 configuration commands

The VRRPv3 provides router address redundancy (for both IPv4 and IPv6). VRRPv3 support is similar to VRRP support. The main differences between the protocol versions are shown in the following table.

VRRPv2	*VRRPv3*
IPv4 Address Reservation Support	Support for both IPv4 and IPv6 Address Reservation
Authentication support	No authentication support
Do not operates with link-local addresses	Support for operation with link-local IPv6 addresses
The interval for sending VRRP announcements is set in seconds.	The interval for sending VRRP announcements is set in centiseconds (0.01 seconds).
The format of MAC address for VRRP is 00-00-5E-00-01-{VRID}	The format of MAC address for IPv6 VR IP addresses is 00-00-5E-00-02-{VRID}
The SNMP MIB implementation is based on RFC 2787. 32-bit counters are used.	The SNMP MIB implementation is based on RFC 6527. 64-bit counters are used.

fhrp version vrrp v3

Use the fhrp version vrrp v3 command in Global Config mode to enable VRRP version 3 configuration support (VRRPv3) on the device,

When you enable VRRPv3, VRRP version 2 (VRRPv2) becomes unavailable. After execution of the no fhrp version vrrp v3 command, VRRPv3 support is disables, the VRRPv2 version is enables. In addition, this command resets live data and applies the VRRPv2 configuration. Similar processes occur when the no ip vrrp command is executed while using VRRPv2.

Default: disabled

Format: `fhrp version vrrp v3`

Command mode: Global Config

no fhrp version vrrp v3

Use this command to disable the VRRPv3 on the device and enable VRRPv2.

Format: `no fhrp version vrrp v3`

Command mode: Global Config

snmp-server enable traps vrrp

Use this command to enable sending SNMP traps defined in the standards for VRRPv2 and VRRPv3.

Default: enabled

Format: `snmp-server enable traps vrrp`

Command mode: Global Config

no snmp-server enable traps vrrp

Use this command to disable sending SNMP traps defined in the standards for VRRPv2 and VRRPv3.

Default: enabled

Format: `no snmp-server enable traps vrrp`

Command mode: Global Config

vrrp

Use the vrrp command allows you to create a VRRPv3 virtual router group and enter the VRRPv3 Group Configuration mode.

Format: `vrrp group-id address-family {ipv4 | ipv6}`

Command mode: Interface Config

Parameter	*Description*
group-id	Virtual router group number. The range is 1 to 255.
address-family	The address family for this VRRP group.
ipv4	(Optional) The IPv4 address family.
ipv6	(Optional) The IPv6 address family.

no vrrp

Use the no vrrp command to remove the specified VRRPv3 virtual router group. Before using this command, you must disable the virtual router by executing the shutdown command in the appropriate VRRP Config mode.

Format: `no vrrp group-id address-family {ipv4 | ipv6}`

Command mode: Interface Config

preempt

Use this command to configure the device as the master virtual router for the VRRP group if its priority is higher than the priority of the current master virtual router.

Default: enabled, default delay value is 0

Format: `preempt [delay minimum centiseconds]`

Command mode: VRRPv3 Config

Parameter	*Description*
delay minimum	The length of the delay (in centiseconds) before the device sends an announcement about receiving the status of the master device. The default delay time is 0 centiseconds. The range of this value is 0–3600 centiseconds.

no preempt

Use this command to prevent the device, whose priority is higher than the priority of the current master virtual router, from becoming the master virtual router.

Format: `no preempt [delay minimum` *`centiseconds`*`]`

Command mode: VRRPv3 Config

accept-mode

Use this command to set the mode in which the master router will receive packets sent to the virtual IP addresses of other owners (not belonging to it) as their packets.

Default: disabled

Format: `accept-mode`

Command mode: VRRPv3 Config

no accept-mode

Use thid command to return the mode of receiving packets to virtual IP addresses to the default value.

Format: `no accept-mode`

Command mode: VRRPv3 Config

priority

Use this command to set the device priority in the VRRPv3 group. The priority value determines which device becomes the master virtual router.

Default: 100

Format: `priority level`

Command mode: VRRPv3 Config

Parameter	*Description*
level	The priority of the device in VRRPv3 group. The range is 1 to 254. Default: 100.

no priority

Use this command to set the device priority to the default value.

Format: `priority`

Command mode: VRRPv3 Config

timers advertise

Use this command to set the interval between consecutive announcements sent by the master virtual router in the VRRP group. Use the no form of this command to restore the default value.

Announcements sent by the master virtual router contain the announcement interval, status, and priority of the current master virtual router. The interval between consecutive announcements is the time after which other routers will consider the master router inaccessible. Redundant VRRP routers learn the corresponding values from the announcements of the master router. The interval values configured on the master router always override any other health assessment intervals defined on the redundant VRRP routers.

Default: 100

Format: `timers advertise centiseconds`

Command mode: VRRPv3 Config

Parameter	*Description*
centiseconds	The interval between consecutive announcements of the master virtual router. The value is set in centiseconds. Valid value range: 0–4095 centiseconds.

no timers advertise

Use this command to set the interval between announcements to the default value.

Format: `no timers advertise`

Command mode: VRRPv3 Config

shutdown

Use the shutdown command to disable the configuration of the VRRP group on this router.

Format: `shutdown`

Command mode: VRRPv3 Config

no shutdown

Use the no shutdown command to update the status of the virtual router after configuration is complete.

Format: `no shutdown`

Command mode: VRRPv3 Config

address

Use this command to set the primary or secondary IP address of the device within the VRRPv3 group. Use the no form of this command to remove the secondary address.

If the primary or secondary parameter is not defined, the specified IP address will be set as primary. The primary virtual IPv6 address should only be the link-local address. If the global IPv6 address is specified as the VRRP primary IP address, an error will be returned with the following text: «Error! Primary virtual IPv6 address should be a link-local address only». Removing the primary virtual IP address (both IPv4 and IPv6) is not allowed. The primary virtual IP address of the virtual router can not be deleted. The secondary virtual IP address can be removed using the no form of this command. Due to the VRRPv3 requirements for IPv6, for the functioning of the group, you should configure the primary virtual link-local IPv6 address. After adding a primary link-local IPv6 address to the group, you can add global addresses as secondary ones.

Format: `address ip-address [primary | secondary]`

Command mode: VRRPv3 Config

Parameter	***Description***
ip-address	An IPv4 or IPv6 address can be specified in one of the following formats: *ipv4-address*, *ipv6-link-local-address*, *ipv6-address*>/<*prefix-len*>.
primary	(Optional) Sets the primary IP address of the VRRPv3 group.
secondary	(Optional) Sets the secondary IP address of the VRRPv3 group.

no address

Use this command to delete the configured secondary IPv4 or IPv6 address. The primary address cannot be deleted, it can only be changed.

Format: `no address ip-address secondary`

Command mode: VRRPv3 Config

track interface

Use this command to configure the the device interface tracking in the VRRPv3 group. After configuring tracking, the system will display notifications when the state of the interface changes. Using the decrement parameter, you can set the value by which the device priority in the VRRPv3 group will be reduced if the interface disables.

Default: enabled

Format: `track interface {unit/slot/port | vlan vlan-id} [decrement number]`

Command mode: VRRPv3 Config

Parameter	*Description*
unit/slot/port	The interface for tracking
vlan-id	The VLAN for tracking
decrement number	(Optional) VRRP priority reduction step for the monitored object. The number by which the priority will be reduced. Range — 1–254.

no track interface

Use this command to disable the device interface tracking in the VRRPv3 group.

Default: enabled.

Format: `track interface {unit/slot/port | vlan vlan-id} [decrement number]`

Command mode: VRRPv3 Config

track ip route

Use this command to configure IP route tracking for a device in the VRRPv3 group. After configuring tracking, the system will display notifications when the state of the IP route changes. Using the decrement parameter, you can set the value by which the device priority in the VRRPv3 group will be reduced if the route will become unavailable.

Default: disabled

Format: `track ip route ip-address/prefix-len [decrement number]`

Command mode: VRRPv3 Config

Parameter	*Description*
ip-address/prefix-len	The prefix and length of the prefix of the route for tracking.
decrement number	(Optional) VRRP priority reduction step for the monitored object. The number by which the priority will be reduced. Range — 1–254.

no track ip route

Use this command to disable the IP route tracking.

Format: `no track ip route ip-address/prefix-len [decrement number]`

Command mode: VRRPv3 Config

clear vrrp statistics

Use this command to delete the VRRP statistics for the specified device interface in the VRRPv3 group and the corresponding IP address family. After execution of this command without additional parameters, the global statistics will be deleted and all virtual routers (both IPv4 and IPv6) will be rebooted.

If additional parameters are specified, statistics will be deleted only for virtual routers that match the specified values (such as the IP address family, interface, and virtual router group ID).

Format: `clear vrrp statistics [{ipv4| ipv6} {unit/slot/port | vlan vlan-id} vr-id]`

Command mode: Privileged

Parameter	*Description*
ipv4	(Optional) Indicates that the virtual router group belongs to the IPv4 address family.
ipv6	(Optional) Indicates that the virtual router group belongs to the IPv6 address family.
unit/slot/port	(Optional) The number of the interface to which the virtual router belongs.
vlan-id	(Optional) The number of VLAN to which the virtual router belongs.
vr-id	(Optional) Virtual router group number. The range is 1 to 255.

show vrrp

Use this command to display information on all active VRRPv3 groups (without parameters), all active VRRPv3 groups configured in the IPv4 or IPv6 address family, or active VRRPv3 groups configured in the IPv4 or IPv6 address family for the specified interface.

Format: `show vrrp [{ipv4 | ipv6}] [{unit/slot/port | vlan vlan-id} vr-id]`

Command mode: Privileged

Parameter	*Description*
ipv4	(Optional) Indicates that the virtual router group belongs to the IPv4 address family.
ipv6	(Optional) Indicates that the virtual router group belongs to the IPv6 address family.
unit/slot/port	(Optional) The number of the interface to which the virtual router belongs.
vlan-id	(Optional.) The number of VLAN to which the virtual router belongs.
vr-id	(Optional) Virtual router group number. The range is 1 to 255.

show vrrp brief

Use this command to display a summary of all active VRRPv3 groups.

Format: `show vrrp brief`

Command mode: Privileged

Parameter	*Description*
Interface	The interface on which the VRRPv3 is configured.
VR	The router ID of the virtual router.
A-F	The type of IP address family (IPv4 or IPv6) to which this virtual router belongs to.
Pri	The router priority of the virtual router.
AdvIntvl	Announcement sending interval configured for this virtual router.
Pre	The priority interrupt mode of the virtual router.

Acc	The receive mode of this virtual router.
State	The status of the virtual router in the VRRPv3 group. It can take one of the following values: Init, Backup, Master
VR IP address	The virtual IP address of the VRRPv3 group.

show vrrp statistics

Use this command to display statistics for the specified VRRPv3 group or global statistics. If you execute this command without parameters, global statistics will be displayed.

If parameters are set, only statistics for virtual routers matching the parameter values (such as the IP address family, interface, and virtual router group ID) will be displayed.

Format: `show vrrp statistics [{ipv4| ipv6} {unit/slot/port | vlan vlan-id} vrid]`

Command mode: Privileged

Parameter	*Description*
ipv4	(Optional) Indicates that the virtual router group belongs to the IPv4 address family.
ipv6	(Optional) Indicates that the virtual router group belongs to the IPv6 address family.
unit/slot/port	(Optional) The number of the interface to which the virtual router belongs.
vlan-id	(Optional.) The number of VLAN to which the virtual router belongs.
vr-id	(Optional) Virtual router group number. The range is 1 to 255.

11.9 DHCP and BOOTP Relay configuration commands

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

bootpdhcprelay cidoptmode

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

Default: disabled

Format: `bootpdhcprelay cidoptmode`

Command mode: Global Config
Virtual Router Config

no bootpdhcprelay cidoptmode

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

Format: `no bootpdhcprelay cidoptmode`

Command mode: Global Config
Virtual Router Config

bootpdhcprelay maxhopcount

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

Default: 4

Format: `bootpdhcprelay maxhopcount` *`1-16`*

Command mode: Global Config
Virtual Router Config

no bootpdhcprelay maxhopcount

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

Format: `no bootpdhcprelay maxhopcount`

Command mode: Global Config
Virtual Router Config

bootpdhcprelay minwaittime

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

Default: 0

Format: `bootpdhcprelay minwaittime` *`0-100`*

Command mode: Global Config
Virtual Router Config

no bootpdhcprelay minwaittime

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

Format: `no bootpdhcprelay minwaittime`

Command mode: Global Config
Virtual Router Config

bootpdhcprelay serverip

This command configures the server IP address of the BootP/DHCP Relay on the system. The *ipaddr* parameter is the IP address of the server.

Default: 0.0.0.0

Format: `ip helper-address` *`ipaddr`* `dhcp`

Command mode: Global Config

no bootpdhcprelay serverip

This command returns the server IP address of the BootP/DHCP Relay on the system to the default value of 0.0.0.0.

Format: `no ip helper-address` *ipaddr* `dhcp`

Command mode: Global Config

bootpdhcprelay enable

Use this command to enable the relay of DHCP packets.

Default: disabled

Format: `ip helper enable`

Command mode: Global Config

no bootpdhcprelay enable

Use this command to disable the relay of DHCP packets.

Default: disabled

Format: `no ip helper enable`

Command mode: Global Config

show bootpdhcprelay

This command displays the BootP/DHCP Relay information for the virtual router. If no router is specified, information related to the default router is displayed.

Format: `show bootpdhcprelay [vrf` *vrf-name*`]`

Command mode: Privileged
User

Parameter	*Value*
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit ID option which may be enabled or disabled.

show ip bootpdhcprelay

This command displays BootP/DHCP Relay information.

Format: `show ip bootpdhcprelay`

Command mode: Privileged
User

Parameter	*Value*
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.

Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit ID option which may be enabled or disabled.

11.10 IP Helper configuration commands

This section describes the commands 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 at 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 nonlocal 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.

The network administrator can configure relay entries both globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). The network administrator may configure multiple relay entries for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. That is, if a packet's destination UDP port matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

The network administrator can configure discard relay entries, which direct the system to discard matching packets. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

In addition to configuring the server addresses, the network administrator also configures which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI as a convenience, but the network administrator can configure a relay entry with any UDP port number. The network administrator may configure relay entries that do not specify a destination UDP port. The relay agent relays assumes these entries match packets with the UDP destination ports listed in table below. This is the list of default ports.

Default Ports: UDP Port Numbers Implied as masks

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 he likes. 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.

clear ip helper statistics

Use this command to reset to zero the statistics displayed in the show ip helper statistics command for the specified virtual router. If no router is specified, the command is executed for the default router.

Format: `clear ip helper statistics [vrf` *`vrf-name`*`]`

Command mode: Privileged

ip helper-address (Global Config)

Use this command to 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.

Default: No helper addresses are configured.

Format: `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]`

Command mode: Global Config

Virtual Router Config

Parameter	*Description*
server-address	The 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	A destination UDP port number from 0 to 65535.
port-name	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) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

no ip helper-address (Global Config)

Use the **no** form of the command to delete an IP helper entry. The *no ip helper-address* command with no arguments clears all global IP helper addresses.

Format: `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]`

Command mode: Global Config

ip helper-address (Interface Config)

Use this command to 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.

Default: No helper addresses are configured.

Format: `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]`

Command mode: Interface Config

Parameter	*Description*
server-address	The 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	A destination UDP port number from 0 to 65535.
port-name	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) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

no ip helper-address (Interface Config mode)

Use this command to delete a relay entry on an interface. The no command with no arguments clears all helper addresses on the interface.

Format: `no 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]`

Command mode: Interface Config

ip helper enable

Use this command to 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, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

Default: disabled

Format: `ip helper enable`

Command mode: Global Config
Virtual Router Config

no ip helper enable

Use the **no** form of this command to disable relay of all UDP packets.

Format: `no ip helper enable`

Command mode: Global Config

show ip helper-address

Use this command to 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 *unit/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 unit/slot/port format.

Format: `show ip helper-address [vrf vrf-name] [{unit/slot/port|vlan 1-4093}]`

Command mode: Privileged

Parameter	*Description*
interface	The relay configuration is applied to packets that arrive on this interface. This field is set to any for global IP helper entries.
UDP Port	The 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	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

show ip helper statistics

Use this command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent on the specified virtual router. If no virtual router is specified, the configuration of the default router is displayed.

Format: `show ip helper statistics [vrf vrf-name]`

Command mode: Privileged

Parameter	*Description*
DHCP client messages received	The 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	The 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	The 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	The number of DHCP server messages relayed to a client.
UDP clients messages received	The 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	The 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	The 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	The 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	The 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	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.

11.11 OSPF (Open Shortest Path First Protocol) configuration commands[1]

This section describes the commands you use to view and configure Open Shortest Path First (OSPF). OSPF is a link-state routing protocol that you use to route traffic within a network. The protocol using Dijkstra's Algorithm to find the shortest route. OSPF is an internal gateway protocol (IGP). OSPF protocol distributes information on available routes between routers in a single autonomous system.

11.11.1 General OSPF configuration commands

router ospf

Use this command to 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.

Format: `router ospf [vrf vrf-name]`

Command mode: Global Config

Parameter	*Description*
vrf vrf-name	The virtual router on which to enable OSPF routing.

[1] This functionality is available with an OSPF license. To activate the license, please contact the technical support.

enable

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

Default: enabled

Format: `enable`

Command mode: Router OSPF Config

no enable

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

Format: `no enable`

Command mode: Router OSPF Config

network area

Use this command to enable OSPFv2 on an interface and set its area ID if the IP address of an interface is covered by this network command.

Default: disabled

Format: `network` *`ip-address wildcard-mask`* `area` *`area-id`*

Command mode: Router OSPF Config

no network area

Use this command to disable the OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command.

Format: `no network` *`ip-address wildcard-mask`* `area` *`area-id`*

Command mode: Router OSPF Config

1583compatibility

This command enables OSPF 1583 compatibility.

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

Default: enabled

Format: `1583compatibility`

Command mode: Router OSPF Config

no 1583compatibility

This command disables OSPF 1583 compatibility.

Format: `no 1583compatibility`

Command mode: Router OSPF Config

area default-cost

This command configures the default cost for the stub area. You must specify the area ID and an integer value between 1-16777215.

Format: `area areaid default-cost 1-16777215`

Command mode: Router OSPF Config

area nssa

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

Format: `area areaid nssa`

Command mode: Router OSPF Config

no area nssa

This command disables nssa from the specified area identifier.

Format: `no area areaid nssa`

Command mode: Router OSPF Config

area nssa default-info-originate

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is ****. The metric type can be comparable (nssa-external 1) or noncomparable (nssa-external 2).

Format: `area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`

Command mode: Router OSPF Config

no area nssa default-info-originate

This command disables the default route advertised into the NSSA.

Format: `no area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`

Command mode: Router OSPF Config

area nssa no-redistribute

This command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

Format: `area areaid nssa no-redistribute`

Command mode: Router OSPF Config

no area nssa no-redistribute

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format: `no area areaid nssa no-redistribute`

Command mode: Router OSPF Config

area nssa no-summary

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

Format: *area areaid nssa no-summary*

Command mode: Router OSPF Config

no area nssa no-summary

This command disables nssa from the summary LSAs.

Format: no area *areaid* nssa no-summary

Command mode: Router OSPF Config

area nssa translator-role

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

Format: area *areaid* nssa translator-role {always | candidate}

Command mode: Router OSPF Config

no area nssa translator-role

This command disables the NSSA translator role from the specified area id.

Format: no area *areaid* nssa translator-role {always | candidate}

Command mode: Router OSPF Config

area nssa translator-stab-intv

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

Default: 40

Format: area *areaid* nssa translator-stab-intv *stabilityinterval*

Command mode: Router OSPF Config

no area nssa translator-stab-intv

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format: no area *areaid* nssa translator-stab-intv *stabilityinterval*

Command mode: Router OSPF Config

area range

Use the area range command in Router OSPF Config mode to configure a summary prefix that an area border router advertises for a specific area.

Default: No area ranges are configured by default. No cost is configured by default.

Format: area *areaid* range *ip-address netmask* {summarylink | nssaexternallink} [advertise | not-advertise] [cost *cost*]

Command mode: OSPFv2 Router Configuration

Parameter	*Description*
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	(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.

no area range

The **no** form of this command deletes a specified area range or reverts an option to its default.

Format: no area *areaid* range *prefix netmask* {summarylink | nssaexternallink} [advertise | not- advertise] [cost]

Command mode: OSPFv2 Router Configuration

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.

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.

area stub

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

Format: `area areaid stub`

Command mode: Router OSPF Config

no area stub

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

Format: `no area areaid stub`

Command mode: Router OSPF Config

area stub no-summary

This command configures the Summary LSA mode for the stub area identified by areaid. Use this command to prevent Type 3 LSA Summaries from being sent.

Default: disabled

Format: `area areaid stub no-summary`

Command mode: Router OSPF Config

no area stub no-summary

This command configures the default Summary LSA mode for the stub area identified by areaid.

Format: `no area areaid stub no-summary`

Command mode: Router OSPF Config

area virtual-link

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

Format: `area areaid virtual-link neighbor`

Command mode: Router OSPF Config

no area virtual-link

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

Format: `no area areaid virtual-link neighbor`

Command mode: Router OSPF Config

area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The value for *type* is either *none*, *simple*, or *encrypt*. The *key* is composed of standard symbols. 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 encrypt, a key id in the range of 0 and 255 must be specified. The default value for authentication type is none. Neither the default password key nor the default key id are configured.

Default: none

Format: `area areaid virtual-link neighbor authentication {none | {simple key} | {encrypt key keyid}}`

Command mode: Router OSPF Config

no area virtual-link authentication

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

Format: `no area areaid virtual-link neighbor authentication`

Command mode: Router OSPF Config

area virtual-link dead-interval

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

Default: 40

Format: `area areaid virtual-link neighbor dead-interval seconds`

Command mode: Router OSPF Config

no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface.

Format: `no area areaid virtual-link neighbor dead-interval`

Command mode: Router OSPF Config

area virtual-link hello-interval

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

Default: 10

Format: `area areaid virtual-link neighbor hello-interval 1-65535`

Command mode: Router OSPF Config

no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface.

Format: `no area areaid virtual-link neighbor hello-interval`

Command mode: Router OSPF Config

area virtual-link retransmit-interval

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

Default: 5

Format: `area` *areaid* `virtual-link` *neighbor* `retransmit-interval` *seconds*

Command mode: Router OSPF Config

no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface.

Format: `no area` *areaid* `virtual-link` *neighbor* `retransmit-interval`

Command mode: Router OSPF Config

area virtual-link transmit-delay

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

Default: 1

Format: `area` *areaid* `virtual-link` *neighbor* `transmit-delay` *seconds*

Command mode: Router OSPF Config

no area virtual-link transmit-delay

This command resets the default transmit delay for the OSPF virtual interface to the default value.

Format: `no area` *areaid* `virtual-link` *neighbor* `transmit-delay`

Command mode: Router OSPF Config

auto-cost

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 for OSPF 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). The reference bandwidth range is 1-4294967 Mbps.

Default: 100 Mbps

Format: `auto-cost reference-bandwidth` *1-4294967*

Command mode: Router OSPF Config

no auto-cost reference-bandwidth

Use this command to set the reference bandwidth to the default value.

Format: `no auto-cost reference-bandwidth`

Command mode: Router OSPF Config

capability opaque

Use this command to 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. The system 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.

Default: enabled

Format: `capability opaque`

Command mode: Router OSPF Config

no capability opaque

Use this command to disable Opaque Capability on the router.

Format: `no capability opaque`

Command mode: Router OSPF Config

clear ip ospf

Use this command to disable and re-enable OSPF for the specified virtual router. If no virtual router is specified, the default router is disabled and re-enabled.

Format: `clear ip ospf [vrf` *`vrf-name`*`]`

Command mode: Privileged

clear ip ospf configuration

Use this command to reset the OSPF configuration to factory defaults for the specified virtual router. If no virtual router is specified, the default router is cleared.

Format: `clear ip ospf configuration [vrf` *`vrf-name`*`]`

Command mode: Privileged

clear ip ospf counters

Use this command to reset global and interface statistics for the specified virtual router. If no virtual router is specified, the global and interface statistics are reset for the default router.

Format: `clear ip ospf counters`

Command mode: Privileged

clear ip ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors for the specified virtual router. On each neighbor's 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 neighbor's Router ID using the optional parameter [*neighbor-id*].

Format: `clear ip ospf neighbor [ vrf` *`vrf-name`*`] [`*`neighbor-id`*`]`

Command mode: Privileged

clear ip ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter [unit/slot/port]. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [neighbor-id].

Format: `clear ip ospf neighbor interface` *`[unit/slot/port] [`*`neighbor-id`*`]`*

Command mode: Privileged

clear ip ospf redistribution

Use this command to 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.

Format: `clear ip ospf redistribution [vrf` *`vrf-name`*`]`

Command mode: Privileged

default-information originate

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

Default: metric — unspecified;

type — 2

Format: `default-information originate [always] [metric` *`0-16777214`*`] [metric-type {1 | 2}]`

Command mode: Router OSPF Config

no default-information originate

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

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

Command mode: Router OSPF Config

default-metric

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

Format: `default-metric 1-16777214`

Command mode: Router OSPF Config

no default-metric

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

Format: `no default-metric`

Command mode: Router OSPF Config

distance ospf

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF 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.

Default: 110

Format: `distance ospf {intra-area` *1-255* `| inter-area` *1-255* `| external` *1-255*`}`

Command mode: Router OSPF Config

no distance ospf

This command sets the default route preference value of OSPF routes in the router. The type of OSPF can be *intra*, *inter*, or *external*. All external routes are assigned the same priority value.

Format: `no distance ospf {`*intra-area | inter-area | external*`}`

Command mode: Router OSPF Config

distribute-list out

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

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

Command mode: Router OSPF Config

no distribute-list out

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

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

Command mode: Router OSPF Config

exit-overflow-interval

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

Default: 0

Format: `exit-overflow-interval` *seconds*

Command mode: Router OSPF Config

no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format: `no exit-overflow-interval`

Command mode: Router OSPF Config

external-lsdb-limit

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

Default: -1

Format: `external-lsdb-limit` *`limit`*

Command mode: Router OSPF Config

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format: `no external-lsdb-limit`

Command mode: Router OSPF Config

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.

Default: Adjacency state changes are logged, but without the detail option.

Format: `log-adjacency-changes [detail]`

Command mode: OSPFv2 Router Configuration

Parameter	*Description*
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.

no log-adjacency-changes

Use the no form of the command to disable state change logging.

Format: `no log-adjacency-changes [detail]`

Command mode: OSPFv2 Router Configuration

prefix-suppression

This command 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 Config. Prefixes associated with secondary IPv4 addresses can never be suppressed.

Default: prefix suppression is disabled.

Format: `prefix-suppression`

Command mode: Router OSPF Config

no prefix-suppression

This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format: `no prefix-suppression`

Command mode: Router OSPF Config

prefix-suppression

This command 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 ipv ospf prefix-suppression command in Interface Config. Prefixes associated with secondary IPv6 addresses can never be suppressed.

Default: prefix suppression is disabled.

Format: `prefix-suppression`

Command mode: Router OSPFv3 Config

no prefix-suppression

This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format: `no prefix-suppression`

Command mode: Router OSPFv3 Config

router-id

This command sets the unique identifier of the OSPF router.

Format: `router-id` *`ipaddress`*

Command mode: Router OSPF Config

redistribute

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

Default: metric — unspecified;
type — 2;
tag — 0.

Format: `redistribute {rip | bgp | static | connected} [metric` *`0-16777214`*`] [metric-type {1 | 2}] [tag` *`0-4294967295`*`] [subnets]`

Command mode: Router OSPF Config

no redistribute

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

Format: `no redistribute {rip | bgp | static | connected} [metric] [metric-type] [tag] [subnets]`

Command mode: Router OSPF Config

maximum-paths

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

Default: 4

Format: `maximum-paths` *maxpaths*

Command mode: Router OSPF Config

no maximum-paths

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

Format: `no maximum-paths`

Command mode: Router OSPF Config

passive-interface default

Use this command to 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.

Default: disabled

Format: `passive-interface default`

Command mode: Router OSPF Config

no passive-interface default

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to nonpassive mode.

Format: `no passive-interface default`

Command mode: Router OSPF Config

passive-interface

Use this command to set the interface as passive. It overrides the global passive mode that is currently effective on the interface. The argument *unit/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 *unit/slot/port* format.

Default: disabled

Format: `passive-interface {`*unit/slot/port*`|vlan` *1-4094*`}`

Command mode: Router OSPF Config

no passive-interface

Use this command to set the interface as nonpassive. It overrides the global passive mode that is currently effective on the interface.

Format: `no passive-interface {`*unit/slot/port*`|vlan` *1-4093*`}`

Command mode: Router OSPF Config

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 (1/the pacing interval). Use this command to adjust this packet rate.

Default: 33 milliseconds

Format: `timers pacing flood` *`milliseconds`*

Command mode: OSPFv2 Router Configuration

Parameter	*Description*
Milliseconds	The average time between transmission of LS Update packets. The range is from 5 ms to 100 ms. The default is 33 ms.

no timers pacing flood

To revert LSA transmit pacing to the default rate, use the *no timers pacing flood* command.

Format: `no timers pacing flood`

Command mode: OSPFv2 Router Configuration

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.

Default: 60 seconds

Format: `timers pacing lsa-group` *`seconds`*

Command mode: OSPFv2 Router Configuration

Parameter	*Description*
seconds	Width of the window in which LSAs are refreshed. The range is 10 to 1800 seconds.

timers spf

Use this command to configure the SPF delay time and hold time. The valid range for both parameters is 0- 65535 seconds.

Default: delay-time — 5
hold-time — 10

Format: `timers spf` *`delay-time hold-time`*

Command mode: Router OSPF Config

trapflags

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group's specific trapflags to enable or disable, are listed in the following table.

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 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*.

Default: disabled

Format: `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} | re-transmit {all | packets | virt-packets} |state-change {all | if-state-change | neighbor-state-change | virtif-state-change | virtneighbor-state-change}`

Command mode: Router OSPF Config

no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the group name followed by that particular flag.
- To disable all the flags in that group, give the group name followed by all.
- To disable all the flags, give the command as trapflags all.

Format: `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 | if-state-change | neighbor-state-change | virtif-
state- change | virtneighbor-state-change}
```

Command mode: Router OSPF Config

11.11.2 OSPF Interface configuration commands

ip ospf area

Use this command to 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.

Default: disabled

Format: `ip ospf area` *`area-id`* `[secondaries none]`

Command mode: Interface Config

no ip ospf area

Use this command to disable OSPF on an interface.

Format: `no ip ospf area [secondaries none]`

Command mode: Interface Config

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.

Default: actual interface bandwidth

Format: `bandwidth` *`1-10000000`*

Command mode: Interface Config

no bandwidth

Use this command to set the interface bandwidth to its default value.

Format: `no bandwidth`

Command mode: Interface Config

ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface or range of interfaces. The value for *type* is either *none*, *simple*, or *encrypt*. The *key* is composed of standard symbols. 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. There is no default value for this command.

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

Command mode: Interface Config

no ip ospf authentication

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

Format: `no ip ospf authentication`

Command mode: Interface Config

ip ospf cost

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

Default: 10

Format: `ip ospf cost 1-65535`

Command mode: Interface Config

no ip ospf cost

This command configures the default cost on an OSPF interface.

Format: `no ip ospf cost`

Command mode: Interface Config

ip ospf database-filter all out

Use the *ip ospf database-filter all out* command in Interface Config to disable OSPFv2 LSA flooding on an interface.

Default: disabled

Format: `ip ospf database-filter all out`

Command mode: Interface Config

no ip ospf database-filter all out

Use the no ip ospf database-filter all out command in Interface Config to enable OSPFv2 LSA flooding on an interface.

Default: disabled

Format: `ip ospf database-filter all out`

Command mode: Interface Config

ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface or range of interfaces. The value for seconds (range: 1–65535) 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.

Default: 40

Format: `ip ospf dead-interval` *`seconds`*

Command mode: Interface Config

no ip ospf dead-interval

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

Format: `no ip ospf dead-interval`

Command mode: Interface Config

ip ospf hello-interval

This command sets 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.

Default: 10

Format: `ip ospf hello-interval` *`seconds`*

Command mode: Interface Config

no ip ospf hello-interval

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

Format: `no ip ospf hello-interval`

Command mode: Interface Config

ip ospf network

Use this command to 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.

Default: broadcast

Format: `ip ospf network {broadcast | point-to-point}`

Command mode: Interface Config

no ip ospf network

Use this command to return the OSPF network type to the default.

Format: `no ip ospf network`

Command mode: Interface Config

ip ospf prefix-suppression

This command 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.

Default: prefix suppression is not configured.

Format: `ip ospf prefix-suppression [disable]`

Command mode: Interface Config

no ip ospf prefix-suppression

This 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.

Format: `no ip ospf prefix-suppression`

Command mode: Interface Config

ip ospf priority

This command sets the OSPF priority for the specified router interface or range of interfaces. 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.

Default: 1, which is the highest router priority

Format: `ip ospf priority` *`0-255`*

Command mode: Interface Config

no ip ospf priority

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

Format: `no ip ospf priority`

Command mode: Interface Config

ip ospf retransmit-interval

This command sets 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. Range — from 0 to 3600 seconds (1 hour).

Default: 5

Format: `ip ospf retransmit-interval 0-3600`

Command mode: Interface Config

no ip ospf retransmit-interval

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

Format: `no ip ospf retransmit-interval`

Command mode: Interface Config

ip ospf transmit-delay

This command sets 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).

Default: 1

Format: `ip ospf transmit-delay 1-3600`

Command mode: Interface Config

no ip ospf transmit-delay

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

Format: `no ip ospf transmit-delay`

Command mode: Interface Config

ip ospf mtu-ignore

This command 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.

Default: enabled

Format: `ip ospf mtu-ignore`

Command mode: Interface Config

no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format: `no ip ospf mtu-ignore`

Command mode: Interface Config

11.11.3 IP Event Dampening configuration commands

dampening

Use this command to enable IP event dampening on a routing interface.

Format: `dampening [half-life period] [reuse-threshold suppress-threshold max-suppress-time[restart restart-penalty]]`

Command mode: Interface Config

Parameter	*Description*
Half-life period	The number of seconds it takes for the penalty to reduce by half. The configurable range is 1-30 seconds. Default value is 5 seconds.
Reuse Threshold	The value of the penalty at which the dampened interface is restored. The configurable range is 1-20,000. Default value is 1000.
Suppress Threshold	The value of the penalty at which the interface is dampened. The configurable range is 1-20,000. Default value is 2000.
Max Suppress Time	The maximum amount of time (in seconds) an interface can be in suppressed state after it stops flapping. The configurable range is 1-255 seconds. The default value is four times of half-life period. If half-period value is allowed to default, the maximum suppress time defaults to 20 seconds.
Restart Penalty	Penalty applied to the interface after the device reloads. The configurable range is 1-20,000. Default value is 2000.

no dampening

This command disables IP event dampening on a routing interface.

Format: `no dampening`

Command mode: Interface Config

show dampening interface

This command summarizes the number of interfaces configured with dampening and the number of interfaces being suppressed.

Format: `show dampening interface`

Command mode: Privileged

show interface dampening

This command displays the status and configured parameters of the interfaces configured with dampening.

Format: `show interface dampening`

Command mode: Privileged

Parameter	*Description*
Flaps	The number times the link state of an interface changed

	from UP to DOWN.
Penalty	Accumulated Penalty.
Supp	Indicates if the interface is suppressed or not.
ReuseTm	Number of seconds until the interface is allowed to come up again.
HalfL	Configured half-life period.
ReuseV	Configured reuse-threshold.
SuppV	Configured suppress threshold.
MaxSTm	Configured maximum suppress time in seconds.
MaxP	Maximum possible penalty.
Restart	Configured restart penalty.

1. **The clear counters command resets the flap count to zero**
2. **The 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.**

11.11.4 OSPF Graceful Restart configuration 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.

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.

nsf

Use this command to enable the OSPF graceful restart functionality on an interface.

Default: disabled

Format: `nsf [ietf] [planned-only]`

Command mode: Router OSPF Config

Parameter	*Description*
ietf	This keyword is accepted but not required.
planned-only	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).

no nsf

Use this command to disable graceful restart for all restarts.

Format: `no nsf`

Command mode: Router OSPF Config

nsf restart-interval

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the initiate failover command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Default: 120 seconds

Format: `nsf [ietf] restart-interval` *1-1800*

Command mode: Router OSPF Config

Parameter	*Description*
ietf	This keyword is accepted but not required.
seconds	The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.

no nsfrestart-interval

Use this command to revert the grace period to its default value.

Format: `no [ietf] nsf restart-interval`

Command mode: Router OSPF Config

nsf helper

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default: OSPF may act as a helpful neighbor for both planned and unplanned restarts

Format: `nsf helper [planned-only]`

Command mode: Router OSPF Config

Parameter	*Description*
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

no nsf helper

Use this command to disable helpful neighbor functionality for OSPF.

Format: `no nsf helper`

Command mode: Router OSPF Config

nsf ietf helper disable

Use this command to disable helpful neighbor functionality for OSPF.

The commands no nsf helper and nsf ietf helper disable are functionally equivalent. The command nsf ietf helper disable is supported solely for compatibility with other network software CLI.

Format: `nsf ietf helper disable`

Command mode: Router OSPF Config

nsf helper strict-lsa-checking

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

Default: enabled

Format: `nsf [ietf] helper strict-lsa-checking`

Command mode: Router OSPF Config

Parameter	*Description*
ietf	This keyword is accepted but not required.

no nsf [ietf] helper strict-lsa-checking

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default: enabled

Format: `nsf [ietf] helper strict-lsa-checking`

Command mode: Router OSPF Config

11.11.5 OSPFv2 Stub Router configuration commands

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 nonstub links in its router LSA to LsInfinity. 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. OSPF remains in stub router mode until you take OSPF 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 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.

Default: OSPF is not in stub router mode by default

Format: `max-metric router-lsa [on-startup seconds] [summary-lsa {metric}]`

Command mode: OSPFv2 Router Configuration

Parameter	*Description*
on-startup	(Optional) OSPF starts in stub router mode after a reboot.
seconds	(Required if on-startup) 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	(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. Default: 16,711,680 (0xFF0000).

no max-metric router-lsa

Use this 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.

Format: `no max-metric router-lsa [on-startup] [summary-lsa]`

Command mode: OSPFv2 Router Configuration

clear ip ospf stub-router

Use the clear ip ospf stub-router command in Privileged 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.

Format: `clear ip ospf stub-router [vrf vrf-name]`

Command mode: Privileged

11.11.6 OSPF Show commands

show ip ospf

This command displays OSPF global configuration information for the specified virtual router. If no router is specified, it displays information for the default router.

Format: `show ip ospf [vrf vrf-name]`

Command mode: Privileged

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

Term	*Value*
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.
RFC 1583 Compatibility	Indicates whether 1583 compatibility is enabled or disabled.
External LSDB Limit	The maximum number of nondefault AS-external-LSA (link state advertisement) 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 Delay Time	The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.
Spf Hold Time	The number of seconds between two consecutive spf calculations.
Flood Pacing Interval	The average time, in milliseconds, between LS Update packet transmissions on an interface.
LSA Refresh Group Pacing Time	The size in seconds of the LSA refresh group window.
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.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
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.
Stub Router Startup Time	Shows the time during which the router will be in Stub Router mode after booting. This row is only listed if OSPF is configured to be a stub router at startup.
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	The 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	The 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. The router automatically becomes an ASBR when it is configured to redistribute routes learned from other protocols. The possible values for the ASBR status are enabled (if the router is configured to redistribute routes

	learned by other protocols) or disabled (if the router is not configured for the same). Enable implies that the router is an autonomous system border router.
Stub Router Status	One of **Active**, **Inactive**.
Stub Router Reason	One of **Configured**, **Startup**, **Resource Limitation**. The row is only listed if stub router is active.
Stub Router Startup Time Remaining	The 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	The 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	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The 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	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
AS Scope LSA Flood List Length	The number of LSAs currently in the global flood queue waiting to be flooded through the OSPF domain.
Retransmit List Entries	The 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	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
Retransmit Entries High Water Mark	The maximum number of LSAs on all neighbors' retransmit lists at any given time.
NSF Support	Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both ("Always").
NSF Restart Interval	The user-configurable grace period during which a

	neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.
NSF Restart Status	The current graceful restart status of the router. • Not Restarting • Planned Restart Unplanned Restart
NSF Restart Age	Number of seconds until the graceful restart grace period expires.
NSF Restart Exit Reason	Indicates why the router last exited the last 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 re-start terminated prematurely because of a to-pology change
NSF Help 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.
Prefix- suppression	Displays whether prefix-suppression is enabled or disa-bled.

show ip ospf abr

This command displays 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.

Format: `show ip ospf abr [vrf vrf-name]`

Command mode: Privileged
User

Term	***Value***
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.

show ip ospf area

This command displays 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.

Format: `show ip ospf area` *areaid* [`vrf` *vrf-name*]

Command mode: Privileged
User

Term	*Value*
AreaId	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	The 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.
Flood List Length	The number of LSAs waiting to be flooded within the area.
Import Summary LSAs	Shows whether to import summary LSAs.
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:

Term	*Value*
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.

show ip ospf asbr

This command displays 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.

Format: `show ip ospf asbr [vrf` *`vrf-name`*`]`

Command mode: Privileged
User

Term	*Value*
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.

show ip ospf database

This command displays 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.

Term	*Value*
vrf-name	Specifies the virtual router for which to display information.
asbr-summary	Use *asbr-summary* to show the autonomous system boundary router (ASBR) summary LSAs.
external	Use *external* to display the external LSAs.
network	Use *network* to display the network LSAs.
nssa-external	Use *nssa-external* to display NSSA external LSAs.

opaque-area	Use *opaque-area* to display area opaque LSAs.
opaque-as	Use *opaque-as* to display AS opaque LSAs.
opaque-link	Use *opaque-link* to display link opaque LSAs.
router	Use *router* to display router LSAs.
summary	Use *summary* to show the LSA database summary information.
lsid	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	Use *adv-router* to show the LSAs that are restricted by the advertising router.
self-originate	Use *self-originate* to display the LSAs in that are self originated.

The information below is only displayed if OSPF is enabled.

Format: `show ip ospf [areaid] database [vrf vrf-name] [{database-summary | [{asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router| summary}] [lsid] [{adv-router [ipaddr] | self-originate}]}]`

Command mode: Privileged

User

For each link-type and area, the following information is displayed:

Term	*Value*
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.
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.

show ip ospf database database-summary

Use this command to 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.

Format: `show ip ospf database database-summary`

Command mode: Privileged

User

Term	*Value*
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.

show ip ospf interface

This command displays the information for the IFO object or virtual interface tables. The argument *unit/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 *unit/slot/port* format.

Format: `show ip ospf interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`| loopback `*`loopback-id`*`}`

Command mode: Privileged

User

Term	*Value*
IP Address	The IP address for the specified interface.
Subnet Mask	A subnet mask.
Secondary IP Address(es)	The 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	The area id of this OSPF interface.
OSPF Network Type	The type of network on this interface that the OSPF is running on.
Router Priority	A number representing the OSPF Priority for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the

	specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.
Transmit Delay	A number representing the OSPF Transmit Delay for the specified interface.
Authentication type	The OSPF Authentication Type for the specified interface are: none, simple or encrypt.
Metric Cost	The 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.
OSPF Interface Type	The OSPF Interface Type will be 'broadcast' or 'ptp'.
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.
Local Link LSAs	The number of Link Local Opaque LSAs in the link-state database.
Local Link LSA Checksum	The 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.

show ip ospf interface brief

This command displays 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.

Format: `show ip ospf interface brief [vrf` *`vrf-name`*`]`

Command mode: Privileged
User

Term	***Value***
Interface	*unit/slot/port*
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The area id of this OSPF interface.
Router Priority	A number representing the OSPF Priority for the

	specified interface.
Cost	The metric cost of the OSPF interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Interface Transmit Delay	A number representing the OSPF Transmit Delay for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.

show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled. The argument *unit/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 *unit/slot/port* format.

Format: `show ip ospf interface stats {`*`unit/slot/port`*`|vlan `*`1-4093`*`}`

Command mode: Privileged
User

Term	*Value*
OSPF Area ID	The area id of this OSPF interface.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
AS Border Router Count	The total number of Autonomous System border routers reachable within this area.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IP Address	The IP address associated with this OSPF interface.
OSPF Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
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.
Source Not On Local Subnet	The 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	The number of received OSPF packets discarded where the ingress interface is in a nonbackbone 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	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 packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
Wrong Authentication Type	The 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. **Note** This field applies only to OSPFv2.
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.

show ip ospf lsa-group

This command displays 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.

Format: `show ip ospf lsa-group [vrf` *`vrf-name`*`]`

Command mode: Privileged
User

Term	*Value*
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.

show ip ospf neighbor

This command displays information about OSPF neighbors for the specified virtual router. If no router is specified, it displays information for the default 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. If you specify an interface or tunnel, only the information for that interface or tunnel displays, if the interface is a physical routing interface and vlan format if the interface is a routing vlan. The ip-address is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Format: `show ip ospf neighbor [vrf` *`vrf-name`*`][interface {`*`unit/slot/port`*`|vlan` *`1-4093`*`}] [ip- address]`

Command mode: Privileged

User

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

Term	*Value*
Router ID	The input neighbor Router ID.
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.
IP Address	The IP address of the neighbor.
Interface	The interface of the local router in unit/slot/port format.
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. • 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	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

If you specify an IP address for the neighbor router, the following fields display:

Term	*Value*
Interface	unit/slot/port
Neighbor IP Address	The IP address of the neighbor router.
Interface index	The interface ID of the neighbor router.
Area ID	The area ID of the OSPF area associated with the interface.
Options	An 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 (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
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.
Dead Timer Due	The 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	The state of the neighboring routers.
Events	The number of times this neighbor relationship has

	changed state, or an error has occurred.
Retransmitted LSAs	The number of LSAs retransmitted to this neighbor.
Retransmission Queue Length	An 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 OSPF 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	The 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 — 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

show ip ospf range

This command displays 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.

Format: `show ip ospf range` *areaid* [`vrf` *vrf-name*]

Command mode: Privileged

Term	*Value*
Prefix	The summary prefix.
Subnet Mask	The 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	Whether the range is currently active. Value: **Y** or **N**.

show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations for the specified virtual router. If no router is specified, it 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.

Format: `show ip ospf statistics` [`vrf` *vrf-name*]

Command mode: Privileged

Term	*Value*
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 to compute routes, in milliseconds. The total may exceed the sum of the 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. Reason codes are as follows: • R - new router LSA • N - new network LSA • SN - new network summary LSA • SA - new ASBR summary LSA • X - new external LSA

show ip ospf stub table

This command displays 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.

Format: `show ip ospf stub table [vrf vrf-name]`

Command mode: Privileged
User

Term	*Value*
Area ID	A 32-bit identifier for the created stub area.
Type of Service	The type of service associated with the stub metric. The switch only supports Normal TOS.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

show ip ospf traffic

This command displays 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).

The clear ip ospf counters command does not clear the message queue high water marks.

Format: `show ip ospf traffic [vrf vrf-name]`

Command mode: Privileged

Parameter	*Description*
OSPFv2 Packet Statistics	The number of packets of each type sent and received since OSPF counters were last cleared.
LSAs Retransmitted	The number of LSAs retransmitted by this router since OSPF counters were last cleared.
LS Update Max Receive Rate	The 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	The 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	The 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.

show ip ospf virtual-link

This command displays 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.

Format: `show ip ospf virtual-link [vrf` *`vrf-name`*`] areaid neighbor`

Command mode: Privileged
User

Parameter	*Description*
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 transmission delay type of the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication type	The configured authentication type of the OSPF virtual interface.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

show ip ospf virtual-link brief

The configured transmission delay type of the OSPF virtual interface.

This command displays the OSPF Virtual Interface information for all areas in the system.

Format: `show ip ospf virtual-link brief`

Command mode: Privileged
User

Parameter	*Description*
Area ID	The area id of the requested OSPF area.
Neighbor	The neighbor interface of the OSPF virtual interface.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Transmit Delay	The configured transmission delay type of the OSPF virtual interface.

11.12 RIP configuration commands[1]

This section describes the commands you use to view and configure Routing Information Protocol (RIP), which is a distance-vector routing protocol that you use to route traffic within a small network.

router rip

Use this command to enter Router RIP mode.

Format: `router rip`

Command mode: Global Config

enable (RIP)

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

Default: enabled

Format: `enable`

Command mode: Router RIP Config

no enable (RIP)

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

Format: `no enable`

Command mode: Router RIP Config

ip rip

This command enables RIP on a router interface or range of interfaces.

Default: disabled

Format: `ip rip`

Command mode: Interface Config

[1] This functionality is available with an RIP license. To activate the license, please contact the technical support.

no ip rip

This command disables RIP on a router interface.

Format: `no ip rip`

Command mode: Interface Config

auto-summary

This command enables the RIP auto-summarization mode.

Default: disabled

Format: `auto-summary`

Command mode: Router RIP Config

no auto-summary

This command disables the RIP auto-summarization mode.

Format: `no auto-summary`

Command mode: Router RIP Config

default-information originate (RIP)

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

Format: `default-information originate`

Command mode: Router RIP Config

no default-information originate (RIP)

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

Format: `no default-information originate`

Command mode: Router RIP Config

default-metric (RIP)

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

Format: `default-metric` *`0-15`*

Command mode: Router RIP Config

no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format: `no default-metric`

Command mode: Router RIP Config

distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. A route with a preference of 255 cannot be used to forward traffic.

Default: 15

Format: `distance rip 1-255`

Command mode: Router RIP Config

no distance rip

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

Format: `no distance rip`

Command mode: Router RIP Config

distribute-list out (RIP)

This command is used to specify the access list to filter routes received from the source protocol.

Default: 0

Format: `distribute-list 1-199 out {ospf | bgp | static | connected}`

Command mode: Router RIP Config

no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format: `no distribute-list 1-199 out {ospf | bgp | static | connected}`

Command mode: Router RIP Config

ip rip authentication

This command sets the RIP Version 2 Authentication Type and Key for the specified interface or range of interfaces. The value for *type* is either *none*, *simple*, or *encrypt*. The value for authentication key *[key]* must be 16 bytes or less. The *[key]* is composed of standard symbols. If the value of type is *encrypt*, a keyid in the range of 0 and 255 must be specified.

Unauthenticated interfaces do not need an authentication key or authentication key ID.

Default: none

Format: `ip rip authentication {none | {simple key} | {encrypt key keyid}}`

Command mode: Interface Config

no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

Format: `no ip rip authentication`

Command mode: Interface Config

ip rip receive version

This command configures an interface or range of interfaces to allow RIP control packets of the specified version(s) to be received.

The value for mode is one of: *rip1* to receive only RIP version 1 formatted packets, *rip2* for RIP version 2, *both* to receive packets from either format, or none to not allow any RIP control packets to be received.

Default: both

Format: `ip rip receive version {rip1 | rip2 | both | none}`

Command mode: Interface Config

no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format: `no ip rip receive version`

Command mode: Interface Config

ip rip send version

This command configures an interface or range of interfaces to allow RIP control packets of the specified version to be sent. The value for mode is one of: *rip1* to broadcast RIP version 1 formatted packets, *rip1c* (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, *rip2* for sending RIP version 2 using multicast, or none to not allow any RIP control packets to be sent.

Default: rip2

Format: `ip rip send version {rip1 | rip1c | rip2 | none}`

Command mode: Interface Config

no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

Format: `no ip rip send version`

Command mode: Interface Config

hostroutesaccept

This command enables the RIP hostroutesaccept mode.

Default: enabled

Format: `hostroutesaccept`

Command mode: Router RIP Config

no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format: `no hostroutesaccept`

Command mode: Router RIP Config

split-horizon

This command sets the RIP *split horizon* mode. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None — no special processing for this case. *Simple* — a route will not be included in updates sent to the router from which it was learned. *Poisoned reverse* — a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

Default: simple

Format: `split-horizon {none | simple | poison}`

Command mode: Router RIP Config

no split-horizon

This command sets the default RIP split horizon mode.

Format: `no split-horizon`

Command mode: Router RIP Config

redistribute (RIP)

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. Internal routes are redistributed by default.

Default: metric — not-configured;
match — internal.

Command mode: Router RIP Config

Format for OSPF as source protocol: `redistribute ospf [metric 0-15] [match[internal] [external 1] [external 2] [nssa- external 1] [nssa-external-2]]`

Format for other source protocol: `redistribute {bgp | static | connected} [metric 0-15]`

no redistribute

This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Format: `no redistribute {ospf | bgp | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`

Command mode: Router RIP Config

show ip rip

This command displays information relevant to the RIP router.

Format: `show ip rip`

Command mode: Privileged
User

Term	*Value*
RIP Admin Mode	Enable or disable.

Split Horizon Mode	None, simple or poison reverse.
Auto Summary Mode	Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries. Default: enable.
Host Routes Accept Mode	Enable or disable. If enabled the router accepts host routes. Default: enable.
Global Route Changes	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global queries	The number of responses sent to RIP queries from other systems.
Default Metric	The default metric of redistributed routes if one has already been set, or blank if not configured earlier. Valid values: 1 to 15.
Default Route Advertise	The default route.

show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e., ip rip).

Format: `show ip rip interface brief`

Command mode: Privileged
User

Term	*Value*
Interface	*unit/slot/port*
IP Address	The IP source address used by the specified RIP interface.
Send Version	The RIP version(s) used when sending updates on the specified interface. Used types: none, RIP-1, RIP-1c and RIP-2.
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. Used types: none, RIP-1, RIP-2 and Both.
RIP Mode	The administrative mode of router RIP operation (enabled or disabled).
Link State	The mode of the interface (up or down).

show ip rip interface

This command displays information related to a particular RIP interface. The argument *unit/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 *unit/slot/port* format.

Format: `show ip rip interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`}`

Command mode: Privileged
User

Term	*Value*
Interface	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
IP Address	The IP source address used by the specified RIP interface.
Send Version	The RIP version(s) used when sending updates on the specified interface. Used types: none, RIP-1, RIP-1c and RIP-2. This is a configured value.
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. Used types: none, RIP-1, RIP-2 and Both. This is a configured value.
RIP Admin Mode	RIP administrative mode of router RIP operation
Link State	Indicates whether the RIP interface is up or down.
Authentication type	The RIP Authentication Type for the specified interface. Possible values are: none, simple and encrypt.

The following information will be invalid if the link state is down.

Term	*Value*
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes contained in valid RIP packets that were ignored for any reason.
Updates Sent	The number of triggered RIP updates actually sent on this interface.

11.13 ICMP Throttling commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

ip unreachables

Use this command to enable the generation of ICMP Destination Unreachable messages on an interface or range of interfaces. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default: enabled

Format: `ip unreachables`

Command mode: Interface Config

no ip unreachables

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format: `no ip unreachables`

Command mode: Interface Config

ip redirects

Use this command to enable the generation of ICMP Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all interfaces.

Default: enabled

Format: `ip redirects`

Command mode: Global Config
Interface Config
Virtual Router Config

no ip redirects

Use this command to prevent the generation of ICMP Redirect messages by the router.

Format: `no ip redirects`

Command mode: Global Config
Interface Config

ipv6 redirects

Use this command to enable the generation of ICMPv6 Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all interfaces.

Default: enabled

Format: `ipv6 redirects`

Command mode: Interface Config

no ipv6 redirects

Use this command to prevent the generation of ICMPv6 Redirect messages by the router.

Format: `no ipv6 redirects`

Command mode: Interface Config

ip icmp echo-reply

Use this command to enable the generation of ICMP Echo Reply messages by the router. By default, the generation of ICMP Echo Reply messages is enabled.

Default: enabled

Format: `ip icmp echo-reply`

Command mode: Global Config
Virtual Router Config

no ip icmp echo-reply

Use this command to prevent the generation of ICMP Echo Reply messages by the router.

Format: `no ip icmp echo-reply`

Command mode: Global Config

ip icmp error-interval

Use this command to 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).

Default: *burst-interval* — 1000 ms.
burst-size — 100 messages

Format: `ip icmp error-interval` *`burst-interval [burst-size]`*

Command mode: Global Config
Virtual Router Config

no ip icmp error-interval

Use the no form of the command to return burst-interval and burst-size to their default values.

Format: `no ip icmp error-interval`

Command mode: Global Config

11.14 BFD (Bidirectional Forwarding Detection) configuration 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).

feature bfd

This command enables BFD on the device. Note that BFD must be enabled in order to configure other protocol and interface parameters.

Default: disabled

Format: `feature bfd`

Command mode: Global Config

no feature bfd

Disables BFD globally and removes runtime session data. Static configurations are retained.

Format: `no feature bfd`

Command mode: Global Config

bfd

This command enables BFD on all interfaces associated with the OSPF process. BFD must be enabled on the individual interface to trigger BFD on that interface.

Default: disabled

Format: `bfd`

Command mode: Router OSPF Config

no bfd

This command disables BFD globally on all interfaces associated with the OSPF process.

Format: `no bfd`

Command mode: Router OSPF Config

bfd echo

This command enables BFD echo mode on an IP interface.

Default: disabled

Format: `bfd echo`

Command mode: Interface Config

no bfd echo

This command disables BFD echo mode on an IP interface.

Format: `no bfd echo`

Command mode: Interface Config

bfd interval

This command configures 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).

Default: none

Format: `bfd interval` *`transmit-interval`* `min_rx` *`minimum-receive-interval`* `multiplier` *`detection- time-multiplier`*

Command mode: Global Config
Interface Config

Term	*Value*
transmit-interval	The desired minimum transmit interval, which is the minimum interval that theuser wants to use while transmitting BFD control packets. It is represented in milliseconds. The range is 100 ms to 1000 ms (with a change granularity of 100) a with default value of 100 ms.
minimum-receive-interval	The required minimum receive interval, which is the minimum interval at which the system can receive BFD control packets. It is represented in milliseconds. The range is 100 ms to 1000 ms (with a change granularity of 100) with a default value of 100 ms.
detection-time-multiplier	The number of BFD control packets that must be missed in a row to declare a session down. Its range is 1 to 50 with default value of 3.

no bfd interval

In Global Config mode, this command 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.

Format: `no bfd interval`

Command mode: Global Config
Interface Config

bfd slow-timer

This command sets up the required echo receive interval preference value. This value determines the interval the asynchronous sessions use for BFD control packets the 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.

Default: 2000

Format: `bfd slow-timer` *`echo-receive-interval`*

Command mode: Global Config

Term	*Value*
echo-receive-interval	The 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.

no bfd slow-timer

This command resets the BFD slow-timer preference value to its default.

Format: `no bfd slow-timer`

Command mode: Global Config

ip ospf bfd

This command enables BFD on interfaces associated with the OSPF process.

Default: disabled

Format: `ip ospf bfd`

Command mode: Interface Config

ip ospf bfd

This command disables BFD on interfaces associated with the OSPF process.

Default: disabled

Format: `no ip ospf bfd`

Command mode: Interface Config

neighbor fall-over bfd

This command enables BFD support for fast failover for a BGP neighbor.

Default: disabled

Format: `neighbor ipaddress fall-over bfd`

Command mode: BGP Router Config

no neighbor fall-over bfd

This command disables BFD support for fast failover for a BGP neighbor.

Format: `no neighbor ipaddress fall-over bfd`

Command mode: BGP Router Config

show bfd neighbors

This command displays the BFD adjacency list showing the active BFD neighbors.

Format: `show bfd neighbors [details]`

Command mode: Privileged

Parameter	*Description*
details	Provides additional details with the routing protocol BFD has registered and displays the Admin Mode status as Enabled or Disabled.

The information presented below is displayed.

Parameter	*Description*
Our IP address	The current IP address.
Neighbor IP Address	The IP address of the active BFD neighbor.
State	The current state: Up or Down.
Interface	The current interface.

Uptime	The amount of time the interface has been up.
Registered Protocol	The protocol from which the BFD session was initiated and that is registered to receive events from BFD. (for example, BGP).
Local Diag	The 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. Note. Demand mode is not supported in the current release.
Minimum transmit interval	The minimum interval to use when transmitting BFD control packets.
Actual TX Interval	The transmitting interval being used for control packets.
Actual TX Echo interval	The transmitting interval being used for echo packets.
Minimum receive interval	The minimum interval at which the system can receive BFD control packets.
Detection interval multiplier	The 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	The number of transmitted BFD packets.
Rx Count	The number of received BFD packets.
Drop Count	The number of dropped packets.

debug bfd event

This command displays BFD state transition information.

Format: `debug bfd event`

Command mode: Privileged

debug bfd packet

This command displays BFD control packet debugging information.

Format: `debug bfd packet`

Command mode: Privileged

12 BGP (BORDER GATEWAY PROTOCOL) COMMANDS[1]

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 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 reset part of the protocol state.**

Parameter	*Description*
as-number	The router's autonomous system number (ASN). The as-number ranges from 1–429496729.

no router bgp

If you invoke no router bgp, BGP is 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.

Default: BGP is inactive by default.
Format: `no router bgp as-number`
Command mode: Global Config

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.

Default: VRF configuration is disabled by default.
Format: `address-family ipv4 vrf vrf-name`
Command mode: BGP Router Config

no address-family ipv4

Use the no form of this command to delete the IPv4 VRF configuration.

Format: `no address-family ipv4 vrf vrf-name`

Command mode: BGP Router Config

[1] This functionality is available with an BGP license. To activate the license, please contact the technical support.

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.

Default: IPv6 route sharing is disabled.

Format: `address-family ipv6`

Command mode: BGP Router Config

no address-family ipv6

Use the no form of this command to clear all IPv6 address family configuration.

Format: `no address-family ipv6`

Command mode: BGP Router Config

address-family vpnv4 unicast

This command enters into VPN4 Address 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.

Default: The VPNv4 address family is disabled.

Format: `address-family vpnv4 unicast`

Command mode: BGP Router Config

no address-family vpnv4 unicast

Use the no form of this command to delete the configuration done in this mode.

Format: `no address-family vpnv4 unicast`

Command mode: BGP Router Config

aggregate-address

To configure a summary address for BGP, use the aggregate-address command in Router Configuration mode. No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the ATOMIC_AGGREGATE attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.

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.

Default: No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the ATOMIC_AGGREGATE attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.

Format: `aggregate-address {address mask|`*`ipv6-prefix/pfx-len`*`} [as-set] [summary-only]`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Parameter	***Description***
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	Summary IPv6 prefix and prefix length. The range for prefix length is 1 to 127.
as-set	(Optional) Normally, the aggregate is advertised with an empty AS path and the ATOMIC_AGGREGATE attribute. If the as-set option is configured, then the aggregate is advertised with a nonempty AS_PATH. If the AS_PATH of all contained routes is the same, then the AS_PATH of the aggregate is the AS_PATH of the contained routes. 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 aggregated routes. If the as-set option is not configured, the aggregate is advertised with an empty AS_PATH.
summary-only	(Optional) When the summary-only option is given, the more-specific routes within the aggregate address are not advertised to neighbors.

no aggregate-address

Use this command to delete a summary address for BGP. The address mask is a summary prefix and mask.

Format: `no aggregate-address address mask`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

bgp aggregate-different-meds

Use the bgp aggregate-different meds command 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.

Default: All the routes aggregated by a given aggregate address must have the same MED value.

Format: bgp aggregate-different-meds

Command mode: BGP Router Config
IPv6 VRF Address Family Config
IPv4 VRF Address Family Config

no bgp aggregate-different-meds

Use the no bgp aggregate-different meds command in BGP Router Configuration mode to return the command to the default.

Format: `no bgp aggregate-different-meds`

Command mode: BGP Router Config
IPv6 VRF Address Family Config
IPv4 VRF Address Family Config

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.

Default: By default, MED values are only compared for paths received from peers in the same AS.

Format: `bgp always-compare-med`

Command mode: BGP Router Config
IPv6 VRF Address Family Config
IPv4 VRF Address Family Config

no bgp always-compare-med

Use the no form of this command to revert to the default behavior, only comparing MED values from paths received from neighbors in the same AS.

Format: `no bgp always-compare-med`

Command mode: BGP Router Config
IPv6 VRF Address Family Config
IPv4 VRF Address Family Config

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.

Default: By default, AS PATH length is not ignored in the BGP best path calculations.

Format: `bgp bestpath as-path ignore`

Command mode: BGP Router Config
IPv6 VRF Address Family Config
IPv4 VRF Address Family Config

no bgp bestpath as-path ignore

Use the no form of this command to revert to the default behavior, where AS PATH length is not ignored in the BGP best path calculation.

Format: `no bgp bestpath as-path ignore`

Command mode: BGP Router Config
IPv6 VRF Address Family Config
IPv4 VRF Address Family Config

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 reflection command enables client-to-client reflection for IPv4, IPv6, or IPv4 VRF routes, depending on the mode.

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 influenced by the IGP metric of the route to reach the BGP next hop. Since a client's IGP distance to a given next hop may differ from the route reflector's 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 cluster's route reflectors to reflect client routes to other clients within the cluster. When client-to-client reflection is disabled, a route reflector continues to reflect routes from non-clients to clients and from clients to non-clients.

Default: Client-to-client reflection is enabled when a router is configured as a route reflector.

Format: `bgp client-to-client reflection`

Command mode: BGP Router Config
IPv6 VRF Address Family Config
IPv4 VRF Address Family Config

no bgp client-to-client reflection

Format: `no bgp client-to-client reflection`

Command mode: BGP Router Config
IPv6 VRF Address Family Config
IPv4 VRF Address Family Config

bgp cluster-id

Use the bgp cluster-id command in BGP router configuration mode to specify the cluster ID of a route reflector. 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; otherwise, some routes may not be reflected to some clients. The same cluster ID is used for both IPv4 and IPv6 route reflection.

Default: A route reflector with an unconfigured cluster ID uses its BGP router ID (configured with bgprouter-id) as the cluster ID.

Format: **`bgp cluster-id`** *`cluster-id`*

Command mode: BGP Router Config
IPv4 VRF Address Family Config

Parameter	*Description*
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.

no bgp cluster-id

Format: **`no bgp cluster-id`** *`cluster-id`*

Command mode: BGP Router Config
IPv4 VRF Address Family Config

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.

Default: If this command is not given, BGP advertises a local preference of 100 in UPDATE messages to internal peers.

Format: `bgp default local-preference` *number*

Command mode: BGP Router Config
IPv4 VRF Address Family Config

Parameter	*Description*
number	The value to use as the local preference for routes advertised to internal peers. The range is 0 to 4,294,967,295.

no bgp default local-preference

This command sets the default value of local preference of the BGP router.

Format: `no bgp default local-preference`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

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 interfaces using the command ip bgp fast-external-failover.

Default: fast external failover mode enabled.

Format: `bgp fast-external-failover`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

no bgp fast-external-failover

Use this command to disable BGP fast-external-failover.

Format: `no bgp fast-external-failover`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

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 nondefault route to the peer's IP address), then BGP drops the adjacency.

Default: Fast internal failover is enabled by default.

Format: `bgp fast-internal-failover`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

no bgp fast-internal-failover

Use this command to return the bgp fast-internal-failover command to the default.

Format: `no bgp fast-internal-failover`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

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.

Default: No subnets are associated with a BGP listen subnet range, and the BGP dynamic neighbor feature is not activated.

Format: `bgp listen { limit` *`max-number`* `| range` *`network / length`* `[ inherit peer` *`peer-template- name`* `] }`

Command mode: BGP Router Config
IPv6 VRF Address Family Config

Parameter	***Description***
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.

no bgp listen

Use this command to deactivate the IPv4 BGP dynamic neighbors feature and delete an IPv4 listen range and deassociate it with a specified peer template.

Format: `no bgp listen { limit | range` *`network / length`* `[ inherit peer` *`peer-template-name`* `] }`

Command mode: BGP Router Config

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.

Default: Neighbor state changes are not logged by default.

Format: `bgp log-neighbor-changes`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

no bgp log-neighbor-changes

Use this command to return the bgp log-neighbor-changes command to the default.

Format: `no bgp log-neighbor-changes`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

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.

Default: BGP accepts AS paths with up to 75 AS numbers.

Format: `bgp maxas-limit` *`number`*

Command mode: BGP Router Config
IPv4 VRF Address Family Config

Parameter	*Description*
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.

no bgp maxas-limit

To revert to the default the limit on the length of AS Paths that BGP accepts from its neighbors, use the no form of this command.

Format: `no bgp maxas-limit`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

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 re-enables BGP, causing all adjacencies to be re-established.

Default: 0.0.0.0

Format: `bgp router-id router-id`

Command mode: BGP Router Config

Parameter	*Description*
router-id	An IPv4 address for BGP to use as its router ID.

no bgp router-id

Use this command to reset the BGP router ID, disabling BGP.

Format: `no bgp router-id router-id`

Command mode: BGP Router Config

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.

Default: BGP does not originate a default route. The **always** option is disabled by default.

Format: `default-information originate [always]`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
always	(Optional) This optional keyword allows BGP to originate a default route, even if the common routing table has no default route.

no default-information originate

Use this command to disable BGP from originating a default route.

Format: `no default-information originate`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

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).

Default: No default metric is set and no MED is included in redistributed routes.

Format: `default-metric` *value*

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
value	The value to set as the MED. The range is 1 to 4,294,967,295.

no default metric

Use this command to delete the default for the metric of redistributed routes.

Format: `no default-metric`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

distance (BGP router configuration)

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 of this command. Two instances of this 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's 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.

Default: BGP assigns preference values according to the distance bgp command, unless overridden for specific neighbors or prefixes by this command.

Format: `distance` *distance* [*prefix wildcard-mask* [*prefix-list*]]

Command mode: BGP Router Config

Parameter	*Description*
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.

no distance (BGP router configuration)

Use this command to set the preference of BGP routes to the default.

Format: `no distance` *`distance`* [*`prefix wildcard-mask`* [*`prefix-list`*]]

Command mode: BGP Router Config

distance BGP

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.

Default: external — 20
internal — 200
local — 200

Format: `distance bgp` *`external-distance internal-distance local-distance`*

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
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.

no distance bgp

Use this command to set the default route preference value of BGP routes in the router.

Format: `no distance bgp`

Command mode: BGP Router Config

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.

Default: announcement lists are not specified.

Format: `distribute-list prefix` *`list-name`* `in`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

Parameter	*Description*
list-name	A prefix list used to filter routes received from all peers based on destination prefix.

no distribute-list prefix in

Use this command to disable a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix.

Format: `no distribute-list prefix` *`list-name`* `in`
Command mode: BGP Router Config
IPv4 VRF Address Family Config

distribute-list prefix out

Use this command to configure a filter that restricts the 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.

Default: announcement lists are not specified.

Format: `distribute-list prefix` *`list-name`* `out [` *`protocol`* `| connected | static ]`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

Parameter	*Description*
prefix 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.

no distribute-list prefix out

Use this command to reset the distribute-list out (BGP) command to the default.

Format: `no distribute-list prefix list-name out [ protocol | connected | static]`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

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.

Format: `enable`

Command mode: BGP Router Config

no enable

This command globally disables the administrative mode of BGP on the system, while retaining the configuration. 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.

Format: `no enable`

Command mode: BGP Router Config

ip bgp fast-external-failover

This command provides the ability of graceful restart.

Default: Disabled.

Format: `bgp graceful-restart [restart-time` *`restart-time`* `|stalepath-time` *`stalepath-time`*`]`

Command mode: BGP Router Config

Parameter	***Description***
Restart-time	The maximum time in seconds before which the graceful restart must be completed. The range is 1 to 3600 seconds. The default value is 120 seconds.
Stalepath-time	The maximum time that the secondary router keeps obsolete routes from restarting the BGP host. The range is 1 to 3600 seconds. The default value is 300 seconds.

no ip bgp fast-external-failover

This command restores the graceful restart configuration to the default value.

Format: `no bgp graceful-restart [restart-time` *`restart-time`* `|stalepath-time` *`stalepath-time`*`]`

Command mode: BGP Router Config

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.

Default: Fast external failover is enabled globally by default. There is no interface configuration by default.

Format: `ip bgp fast-external-failover {permit | deny}`

Command mode: Interface Config

Parameter	*Description*
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.

no ip bgp fast-external-failover

This command unconfigures the feature on the interface, and the interface uses the global setting.

Format: `no ip bgp fast-external-failover`

Command mode: Interface Config

maximum-paths

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.

Default: BGP uses one closest node.

Format: `maximum-paths` *`number-of-paths`*

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
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.

no maximum-paths

This command resets back to the default the number of next hops BGP may include in an ECMP route.

Format: `no maximum-paths`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

maximum-paths igbp

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.

Default: BGP uses one closest node.

Format: `maximum-paths igbp` *`number-of-paths`*

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
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.

no maximum-paths igbp

Use this 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.

Format: `no maximum-paths igbp`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

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.

Default: VPNv4 prefixes are not sent to the neighbor.

Format: `neighbor *prefix* activate`

Command mode: IPv4 VRF Address Family Config

Parameter	*Description*
prefix	An Ipv4 address in dotted notation.

no neighbor activate (IPv4 VRF Address Family Config)

Use the no form of this command to disable exchange of IPv4 VRF prefixes with the neighbor and to disassociate the export map for the specified VRF instance.

Format: `no neighbor *prefix* activate`

Command mode: IPv4 VRF Address Family Config

neighbor activate (IPv6 Address Family Config)

To enable exchange of IPv6 routes with a neighbor, use the neighbor activate command. 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.

Default: IPv6 route sharing is disabled.

Format: `neighbor {*ipv4-address* | *ipv6-address* [interface *interface-name*] | autodetect interface *interface-name*} activate`

Command mode: IPv6 VRF Address Family Config

Parameter	*Description*
ipv4-address	The neighbor's IPv4 address.
ipv6-address	The neighbor's IPv6 address.
interface	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 neighbor's link local iPv6 address is auto-detected.

no neighbor activate

Use the no version of the command to disable exchange of IPv6 routes.

Format: `no neighbor {*ipv4-address* | *ipv6-address* [interface *interface-name*] | autodetect interface *interface-name*} activate`

Command mode: IPv6 VRF Address Family Config

Parameter	*Description*
ipv4-address	The neighbor's IPv4 address.
ipv6-address	The neighbor's IPv6 address.
interface	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 neighbor's link local iPv6 address is auto-detected.

neighbor advertisement-interval

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.

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.

Default: 30 seconds for external peers;
5 seconds for external peers.

Format: `neighbor` *`ip-address`* `advertisement-interval` *`seconds`*

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
ip-address	The neighbor's IPv4 address.
seconds	The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

no neighbor advertisement-interval

Use this command to return to the default the minimum time that must elapse between advertisements of the same route to a given neighbor.

Format: `no neighbor` *`ip-address`* `advertisement-interval`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

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, switch 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.

Default: 2 seconds

Format: `neighbor {ip-address | ipv6-address [interface interface-name] | autodetect interface interface-name} connect-retry-interval retry-time`

Command mode: BGP Router Config

Parameter	*Description*
ip-address	The neighbor's IP address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. 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.
retry-time	The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

no neighbor connect-retry-interval

This command resets to the default the initial connection retry time for a specific neighbor.

Format: `no neighbor ip-address connect-retry-interval`

Command mode: BGP Router Config
IPv4 VRF Address Family Config

neighbor default-originate

To configure BGP to originate a default route to a specific neighbor, use the neighbor default-originate command. 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).

Origination of the default route is not subject to a prefix filter configured with the command distribute-list prefixout.

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.

Default: No default is originated by default.

Format: `neighbor` *`ip-address`* `default-originate [if-default-present][route-map` *`map-name`*`]`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	***Description***
ip-address	The neighbor's IPv4 address.
map-name	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

no neighbor default-originate

Use this command to prevent BGP from originating a default route to a specific neighbor.

Format: `no neighbor` *`ip-address`* `default-originate [if-default-present][route-map` *`map-name`*`]`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

neighbor description

Use this command to record a text description of a neighbor. The description is informational and has no functional impact.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default: No description is originated by default.

Format: `neighbor ip-address autodetect interface interface-name description text`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
Peer Template Config

Parameter	***Description***
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.

no neighbor description

Use this command to delete the text description of a neighbor.

Format: `no neighbor` *`ip-address`* `autodetect interface` *`interface-name`* `description`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
Peer Template Config

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.

Default: 1

Format: `neighbor { ip-address | ipv6-address [ interface interface-name ] | autodetect interface interface-name } ebgp-multihop hop-count`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
Peer Template Config

Parameter	*Description*
ip-address	The neighbor's IPv4 address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. 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.
ebgp-multihop hop-count	The maximum hop-count allowed to reach the neighbor. The allowed range is 1-255.

no neighbor ebgp-multihop

Use this command to remove neighborships.

Format: `no neighbor { ip-address | ipv6-address [ interface interface-name ] | autodetect interface interface-name } ebgp-multihop`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
Peer Template Config

neighbor filter-list

This command filters advertisements to or from a specific neighbor according to the advertisement's 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.

Default: No neighbor filter lists are configured by default.

Format: `neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Parameter	*Description*
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.

no neighbor filter-list

Use this command to unconfigure neighbor filter lists.

Format: `no neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

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 nonexistent AS path access list, all routes are filtered.

Default: No neighbor filter lists are configured by default.

Format: `neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`

Command mode: IPv6 VRF Address Family Config

Parameter	*Description*
ip-address	The neighbor's IPv6 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.

no neighbor filter-list (IPv6 Address Family Config)

Use this command to unconfigure neighbor IPv6 filter lists.

Format: `no neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`

Command mode: IPv6 VRF Address Family Config

neighbor inherit peer

To configure a BGP peer to inherit peer configuration parameters from a peer template, use the neighbor inherit peer command. 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.

Default: No peer configuration parameters are inherited by default.

Format: `neighbor {`*`ip-address`*`| `*`ipv6-address`* `[interface `*`interface-name`*`] autodetect interface `*`interface-name`*`} inherit peer `*`template-name`*

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Parameter	***Description***
ip-address	The IP address of a neighbor whose configuration parameters are inherited from the peer template.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. 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.
template-name	The name of the peer template whose peer configuration parameters are to be inherited by this neighbor.

no neighbor inherit peer

Use this command to remove the inheritance.

Format: `no neighbor` *`ip-address`* `inherit peer` *`template-name`*

Command mode: BGP Router Config

IPv4 VRF Address Family Config

neighbor local-as

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. This command is only allowed on the external BGP neighbors. A neighbor can inherit this configuration from a peer template.

Default: No local AS is configured by default on a peer.

Format: `neighbor { ip-address | ipv6-address [ interface interface-name ] | autodetect interface interface-name } local-as as-number no-prepend replace-as`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Parameter	*Description*
ip-address	The neighbor's IPv4 address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. 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.
local-as *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.

neighbor maximum-prefix (BGP router configuration)

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.

Default: By default the prefix limit is set to the maximum number of routes that can be installed in the forwarding table. The default warning threshold is 75%. A neighbor that exceeds the limit is shutdown unless the warning-only option is configured.

Format: `neighbor ip-address maximum-prefix { maximum | unlimited } [threshold] [warning-only]`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

IPv6 VRF Address Family Config

Parameter	*Description*
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 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 accepts the excess prefixes and writes a log message rather than shutting down the adjacency.

no neighbor maximum-prefix

This command reverts to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

Format: `no neighbor` *`ip-address`* `maximum-prefix`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

neighbor next-hop-self

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.

Default: not enabled

Format: `neighbor` *`ip-address`* `next-hop-self`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	***Description***
ip-address	The neighbor's IP address.

no neighbor next-hop-self

This command disables the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

Format: `no neighbor` *`ip-address`* `next-hop-self`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

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.

Default: MD5 authentication is disabled.

Format: `neighbor {`*`ip-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] |autodetect interface` *`interface-name`*`} password` *`string`*

Command mode: BGP Router Config

IPv4 VRF Address Family Config

IPv6 VRF Address Family Config

Peer Template Config

Parameter	*Description*
ip-address	The neighbor's IP address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface i*nterface-name*	The routing interface on which the neighbor's link local iPv6 address is auto-detected.
string	Case-sensitive password from 1 to 25 characters in length.

no neighbor password

This command disables MD5 authentication of TCP segments sent to and received from a neighbor.

Format: `neighbor {`*`ip-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] |autodetect interface` *`interface-name`*`} password`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

IPv6 VRF Address Family Config

Peer Template Config

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.

Default: No prefix list is configured.

Format: `neighbor` *`ip-address`* `prefix-list` *`prefix-list-name`* `{ in | out }`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config
Peer Template Config

Parameter	*Description*
ip-address	The neighbor's IP 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.

no neighbor prefix-list

This command disables filtering advertisements sent to a specific neighbor based on the destination prefix of each route.

Format: `no neighbor` *`ip-address`* `prefix-list` *`prefix-list-name`* `{ in | out }`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config
Peer Template Config

neighbor remote-as

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.

Default: No neighbors are configured by default.

Format: `neighbor {ip-address | ipv6-address [interface interface-name] |autodetect interface interface-name remote-as as-number`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
Peer Template Config

Parameter	*Description*
ip-address	The neighbor's IP address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. 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.
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.

no neighbor remote-as

This command unconfigures neighbors.

Format: `no neighbor {ip-address | ipv6-address [interface interface-name] | autodetect interface interface-name remote-as`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
Peer Template Config

neighbor remove-private-as

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.

Default: Private AS numbers are not removed by default.

Format: `neighbor ip-address remove-private-as [all replace-as]`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
ip-address	The neighbor's IP address.
all replace-as	To retain the original AS path length, replace each private AS number with the local AS number. This is optional.

no neighbor remove-private-as

Format: `no neighbor ip-address remove-private-as`

Command mode: BGP Router Config

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.

Default: RFC 5549 support is enabled by default for all neighbors if IPv6 package is available in the build.

Format: `neighbor { ipv6-address | autodetect interface interface-name } rfc5549-support`

Command mode: BGP Router Config

Parameter	*Description*
ipv6-address	The neighbor's IPv6 address.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local iPv6 address is auto-detected.

no neighbor rfc5549-support

This command disables advertisement of IPv4 routes over IPv6 next hops.

Format: `no neighbor { ipv6-address | autodetect interface interface-name } rfc5549-support`

Command mode: BGP Router Config

neighbor route-map

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.

Default: No route maps are applied by default.

Format: `neighbor ip-address route-map map-name {in|out}`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

IPv6 VRF Address Family Config

Parameter	*Description*
ipv6-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.

no neighbor route-map

Use the no neighbor route-map command to remove the route map.

Format: `no neighbor ip-address route-map map-name {in|out}`

Command mode: BGP Router Config

neighbor route-reflector-client (BGP router configuration)

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.

Default: Peers are not route reflector clients.

Format: `neighbor {ip-address} route-reflector-client`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
ip-address	The neighbor's IP address.

no neighbor route-reflector-client

Format: `no neighbor {ip-address} route-reflector-client`

Command mode: BGP Router Config

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.

Default: The communities attribute is not sent to neighbors by default.

Format: `neighbor ip-address send-community`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
ip-address	The neighbor's IP address.

no neighbor send-community

Use the *no neighbor send-community* command to return to the default configuration.

Format: `no neighbor ip-address send-community`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

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.

Default: The extended communities attribute is not sent.

Format: `neighbor ip-address send-community [extended | both]`

Command mode: VPNv4 Address Family Config

Parameter	*Description*
ip-address	The neighbor's IPv4 address.
[extended | both]	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.

no neighbor send-community extended

Use the *no neighbor send-community extended* command to disable the exchange of VPNv4 prefixes with the neighbor.

Format: `no neighbor ip-address send-community`

Command mode: VPNv4 Address Family Config

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 re-enabled (using the no neighbor shutdown command below).

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default: Neighbors are not shutdown by default.

Format: `neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface interface-name } shutdown`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Peer Template Config

Parameter	*Description*
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address on the link that connects the two peers.
autodetect interface interface-name	The routing interface on which the neighbor's link local iPv6 address is auto-detected.

no neighbor shutdown

This command administratively enables a BGP peer.

Format: `no neighbor {`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`]| autodetect interface` *`interface-name`* `} shutdown`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Peer Template Config

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.

Default: KeepAlive – 30 sec. Hold – 90 sec.

Format: `neighbor {`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`]| autodetect interface` *`interface-name`* `}timers` *`keepalive holdtime`*

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Peer Template Config

Parameter	*Description*
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.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local iPv6 address is auto-detected.
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 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.

no neighbor timers

This command reverts 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.

Format: `no neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface interface-name }timers`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Peer Template Config

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.

Default: When no update source is configured, TCP connections use the primary IPv4 address on the outgoing interface to the neighbor.

Format: `neighbor {ipv4-address | autodetect interface interface-name } update-source interface`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Peer Template Config

Parameter	*Description*
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.
autodetect interface *interface-name*	The neighbor's IPv6 link local address that will be auto detected on the specified 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.

no neighbor update-source

This command configures BGP to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

Format: `no neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface interface-name } update-source`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Peer Template Config

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 nonBGP 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 (network0.0.0.0 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.

Default: No networks are advertised by default.

Format: `network prefix mask network-mask [route-map rm-name]`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

IPv6 VRF Address Family Config

Parameter	*Description*
prefix	An IPv4 address prefix in dotted notation.
network-mask	The network mask for the prefix in dotted quad notation (e.g., 255.255.0.0).
rm-name	(Optional) A route map can be used to set path attributes on the route.

no network (BGP Router Config)

This command disables BGP from advertising an address prefix.

Format: `no network prefix mask network-mask [route-map rm-name]`

Command mode: BGP Router Config

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 forwarding 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:

- 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.

Default: A VRF does not associate with any RD

Format: `rd route-distinguisher`

Command mode: Virtual Router Config

Parameter	*Description*
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)

This command is effective only if BGP is running on the router. The RD for a VRF once configured cannot be removed or changed. For this 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.

redistribute (BGP Router Configuration)

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.

Default: BGP redistributes no routes by default. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.

Format: `redistribute {ospf | rip | connected | static} [metric metric-value]`
`[match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map map-tag]`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

Parameter	*Description*
ospf, rip, 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 route map can be used to set attributes on redistributed routes.

no redistribute (BGP Router Config)

This command removes the configuration for the redistribution for BGP protocol from the specified source protocol/routers. The command no redistribute opsf match external 1 will withdraw only OSPF external type 1 routes, ospf inter routes will still be redistributing.

Format: `no redistribute {ospf | rip | connected | static} [metric` *`metric-value`*`]`
`[match {internal | external 1 | external 2 | nssa-external 1 | nssa external 2}] [route-map` *`map-tag`*`]`

Command mode: BGP Router Config
IPv4 VRF Address Family Config
IPv6 VRF Address Family Config

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:

- 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.

Default: A VRF does not associate with any RT.

Format: `route-target {export | import | both} rt-ext-comm`

Command mode: Virtual Router Config

Parameter	*Description*
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 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)

This command is effective only if BGP is running on the router. The RD for a VRF once configured cannot be removed or changed. For this 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.

This command is effective only if BGP is running on the router.

no route-target

This command removes the *route-target* specified for a VRF instance.

Format: `no route-target {export | import | both} rt-ext-comm`

Command mode: Virtual Router Config

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 only 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).

The *remote-as as-number* command is doesn't supported in Peer Template Configuration mode. The neighbor's AS number must be specified when the neighbor is created.

Default: No peer templates are configured by default.

Format: `template peer` *name*

Command mode: BGP Router Config

Parameter	*Description*
name	The name of the template. The name may be no more than 32 characters.

no template peer

Use the **no** form of the command to delete a peer template.

Format: `no template peer` *name*

Command mode: BGP Router Config

Parameter	*Description*
name	The name of the template. The name may be no more than 32 characters.

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 The following commands can be added to a peer template in Address Family Configuration mode:

- activate
- advertisement-interval seconds
- default-originate
- filter-list as-path-list-number {in | out}
- maximum-prefix {maximum | unlimited} [threshold]
- next-hop-self
- prefix-list prefix-list-name {in | out}
- remove-private-as [all replace-as]
- route-map map-name {in | out}
- route-reflector-client
- send-community

Format: `address-family {ipv4 vrf|ipv6} vrf`

Command mode: Privileged

Parameter	*Description*
ipv4	Configure policy parameters to be applied to IPv4 routes.
Ipv6	Configure policy parameters to be applied to IPv6 routes.

no address-family

To delete all policy commands for an address family in a peer template, use the no form of this command.

Format: `no address-family {ipv4|ipv6}`

Command mode: Privileged

Parameter	*Description*
ipv4	Configure policy parameters to be applied to IPv4 routes.
Ipv6	Configure policy parameters to be applied to IPv6 routes.

activate

Use this command in the Peer Template Configuration mode to activate the exchange of IPv6 routes.

Format: `activate`

Command mode: IPv6 VRF Address Family Config

connect-retry-interval

Use this command in Peer Template Configuration mode to add it to a peer template to configure a connection retry interval. If a neighbor does not respond to an initial TCP connection attempt, it retries three times. The first retry is after the retry interval configured with the command neighbor connect-retry-interval(BGP Router Config). 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.

Default: 2 seconds

Format: `connect-retry-interval` *`retry-time`*

Command mode: Peer Template Config

Parameter	*Description*
retry-time	The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

no connect-retry-interval

This command resets to the default the connection retry time in a peer template.

Format: `no connect-retry-interval`

Command mode: Peer Template Config

description

Use this command in Peer Template Configuration mode to add to a peer template a text description of a neighbor. The description is informational and has no functional impact.

Default: No description is originated by default.

Format: `description text`

Command mode: Peer Template Config

Parameter	*Description*
Text	Text description of neighbor. Up to 80 characters are allowed.

no description

Use this command to delete the text description of a neighbor from a peer template.

Format: `no description`

Command mode: BGP Router Config
Peer Template Config

password

Use this command in Peer Template Configuration mode to configure a TCP password in a peer template.

Default: MD5 authentication is disabled.

Format: `password string`

Command mode: Peer Template Config

Parameter	*Description*
String	Case-sensitive password from 1 to 25 characters in length.

no password

This command disables a TCP password in a peer template.

Format: `no password`

Command mode: Peer Template Config

shutdown

Use this command in Peer Template Configuration mode to configure the administration status in a peer template.

Default: Neighbors are not shutdown by default.

Format: `shutdown`

Command mode: Peer Template Config

no shutdown

This command administratively enables a BGP peer template.

Format: `no shutdown`

Command mode: BGP Router Config
Peer Template Config

timers

Use this command in Peer Template Configuration mode to configure the keepalive and hold timers in a peer template.

Default: The keepalive and hold timers default to the globally configured values set with the address-family command.

Format: `timers` *`keepalive holdtime`*

Command mode: Peer Template Config

Parameter	*Description*
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 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.

no timers

This command reverts the keep alive and hold time for a peer template to their defaults. After executing this command, the BGP peer must be reset before the changes will take effect.

Format: `no timers`

Command mode: Peer Template Config

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.

Default: When no update source is configured, TCP connections use the primary IPv4 address on the outgoing interface to the neighbor.

Format: `update-source {`*`unit/slot/port`* `|` `vlan` *`id`*`}`

Command mode: Peer Template Config

Parameter	*Description*
update-source interface	The primary IPv4 address on this interface is used as the source IP address for the TCP connection with the neighbor.

no update-source

This command configures the peer template to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

Format: `no update-source`

Command mode: Peer Template Config

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.

Default: The default keepalive time is 30 seconds. The default hold time is 90 seconds.

Format: `timers bgp` *`keepalive holdtime`*

Command mode: BGP Router Config
IPv4 VRF Address Family Config

Parameter	*Description*
update-source interface	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 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.

no timers bgp

This command sets to the default the keepalive and hold times that BGP uses for all of its neighbors.

Format: `no timers bgp`

Command mode: BGP Router Config

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 policy changes

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.

Default: The default delay time is 180 seconds.

Format: `timers policy-apply delay` *`delay`*

Command mode: BGP Router Config

IPv4 VRF Address Family Config

Parameter	***Description***
delay	The time, in seconds, after which the global or per neighbor policies are applied. The range is 0 to 180 seconds.

no timers policy-apply delay

This command sets to the default the delay after which any change to the global or per BGP neighbor inbound/ outbound policies are applied.

Format: `no timers policy-apply delay`

Command mode: BGP Router Config

IPv4 VRF Address Family Config

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.

Format: `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]`

Command mode: Privileged

Parameter	***Description***
vrf-name	The name of the VRF instance.
*	Reset adjacency with every BGP peer.
as-number	Only reset adjacencies with BGP 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	Only reset the adjacency on a specified interface. The adjacency must be formed with IPv6 link-local or with the auto detect feature.
listen range	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.

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.

Format: `clear ip bgp [vrf` *`vrf-name`*`] counters`

Command mode: Privileged

debug ip bgp

To enable debug tracing of BGP events, use the debug ip bgp command in Privileged mode. Debug messages are sent to the system log at the DEBUG severity level. To print them on the console, enable console logging at the DEBUG level (logging console debug command).

The debug options enabled for a specific peer are the union of the options enabled globally and the options enabled specifically for the peer.

Enabling one of the packet type options enables packet tracing in both the inbound and outbound directions.

Default: No debug tracing is enabled by default

Format: `debug ip bgp [ peer-address | events | keepalives | notification | open | refresh | updates ]`

Command mode: Privileged

Parameter	*Description*
peer-address	(Optional) The IPv4 or IPv6 address of a BGP peer. Debug traces are enabled for a specific peer when this option is specified. The command can be issued multiple times to enable simultaneous tracing for multiple peers.

events	(Optional) Trace adjacency state events.
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.
refresh	(Optional) Traces transmit and receive of ROUTE REFRESH packets.
updates	(Optional) Traces transmit and receive of UPDATE packets.

show ip bgp

To view routes in the BGP routing table, use the show ip bgp command in Privileged mode. The output lists both best and nonbest paths to each destination. If a VRF instance is specified, the IPv4 routes in the BGP routing table of the VRF instance are displayed.

Format: show ip bgp [vrf *vrf-name*] [*network/pfx-len* [longer-prefixes | shorter-prefixes [*length*]] | filter-list *as-path-list*| prefix-list *pfx-list-name*]

Command mode: Privileged

Parameter	*Description*
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, longer than a specified length. This option may not be given if the longer-prefixes option is given.
filter-list as-path	(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.
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 prefix list is given.

The command output displays the following information.

Parameter	*Description*
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 • * – 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 attribute
LocPrf	The local preference
Path	AS Path

If the command is given with network/pfx-len 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 nonbest paths. The output only shows attributes that are included with each path.

Parameter	***Description***
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 forwarding.
Advertised To Update Groups	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	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 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.

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.

Format: `show ip bgp [vrf vrf-name] aggregate-address`

Command mode: Privileged

Parameter	*Description*
Prefix/Len	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 of AS 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.

show ip bgp community

This command shows BGP IPv4 routes that belong to a specified set of communities.

Format: `show ip bgp [vrf vrf-name] community communities [exact-match]`

Parameter	*Description*
vrf-name	(Optional) Display routes belonging to communities within the 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.

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.

Format: `show ip bgp [vrf vrf-name] community communities [exact-match]`

Command mode: Privileged

Parameter	*Description*
vrf-name	(Optional) Display routes belonging to communities within the VRF instance.
name	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.

show ip bgp extcommunity-list

This command displays all the permit and deny attributes of the given extended community list. If the list-nameis specified, the output is displayed that matches the given list-name; else all the lists are displayed.

Format: `show ip bgp extcommunity-list [list-name]`

Command mode: Privileged

Parameter	*Description*
list-name	A standard extended community list name.

The command output displays the following information.

Parameter	*Description*
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.

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.

Format: `show ip bgp [network/length]`

Command mode: Privileged

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.

Format: `show ip bgp [vrf vrf-name] neighbors [neighbor-address]`

Command mode: Privileged

Parameter	*Description*
vrf-name	(Optional) Displays the neighbors belonging to the communities within the VRF instance.
neighbor-address	(Optional) The IP address of a neighbor. Used to limit the output to show a single neighbor.

The command output displays the following information.

Parameter	*Description*
Description	Text string assigned using the command neighbor filter-list (BGP Router Config). 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 Fallover	Specifies if BFD has been enabled for BGP neighbors.
Peer ID	The neighbor's BGP router ID.
Peer Admin Status	START or STOP
Peer State	The adjacency state of this neighbor.
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.
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
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. Indicates whether IPv6 unicast routes can be exchanged with this peer.
IPv6 Unicast Support	**Both** and **Sent** have the same meaning as for IPv4. **None** indicates that neither the local router nor the 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.
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.
MD5 Password	The TCP MD5 password, if one is configured, in plain text.
Last Error (Sent)	The last error that occurred on the connection to this neighbor.
Last SubError	The suberror reported with the last error.
Established Transitions	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 neighbor's 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 neighbor that 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 lists each non-zero counter, just after the LastSubError. The counters that may be listed are as follows:

Parameter	***Description***
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 was 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.

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.

Format: `show ip bgp [vrf vrf-name] neighbors ip-address advertised-routes`

Command mode: Privileged

Parameter	***Description***
vrf-name	(Optional) Display the communities within the VRF instance.
ip-address	The neighbor's IP address.

The command output displays the following information.

Parameter	*Description*
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	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.

The output indicates whether BGP is configured to originate a default route to this peer (neighbor default- originate).

This output differs slightly from the output in show ip bgp. Suppressed routes and nonbest routes are not advertised, so these status codes are not relevant here. Advertised routes always havea single next hop, the BGP NEXT HOP advertised to the peer. Local preference is never sent to external peers.

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.

Format: `show ip bgp [vrf vrf-name] neighbors [{ip-address]} policy`

Command mode: Privileged

Parameter	*Description*
vrf-name	(Optional) Display the communities within the VRF instance.
ip-address	(Optional) Specifies an IPv4 address of a neighbor to which to limit the output.

The command output displays the following information.

Parameter	*Description*
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.

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.

Format: `show ip bgp [vrf vrf-name] neighbors [ip-address {received-routes | routes | rejected- routes}]`

Command mode: Privileged

Parameter	*Description*
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.

The command output displays the following information.

Parameter	*Description*
Network	Destination prefix
Next Hop	The BGP NEXT HOP as advertised to 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

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 configuration of the communities within the 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.

Format: `show ip bgp [vrf vrf-name] route-reflection`

Command mode: Privileged

Parameter	*Description*
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.

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 with-drawn 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 communities within the VRF instance are displayed.

Format: `show ip bgp [vrf` *`vrf-name`*`] statistics`

Command mode: Privileged

The command outputs the following information.

Parameter	*Description*
Delta T	How long since the decision process was run. Hours:minutes:seconds 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 decision process 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 reset. 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.

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 communities within a VRF instance is displayed.

Format: `show ip bgp [vrf vrf-name] summary`

Command mode: Privileged

The command outputs the following information.

Parameter	*Description*
IPv4 Routing	Whether IPv4 routing is globally enabled. BGP does not include the IPv4 unicast AFI/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 neighbor's IP address. 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, OPEN 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 days:hours:minutes:seconds format.
Pfx Rcvd	The number of prefixes received from the neighbor.

show ip bgp template

Use this command to view information about all configured BGP peer templates or for the specified BGP template.

Format: `show ip bgp template` *name*

Command mode: Privileged

Parameter	***Description***
Name	The name of a BGP peer template
AF	The address family to which the configuration command applies. This field is blank for session parameters, which apply to all address families.
Configuration	Configuration commands that are included in the template.

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 for the communities within the VRF instance are displayed.

Format: `show ip bgp [vrf` *vrf-name*`] traffic`

Command mode: Privileged

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:

Parameter	*Description*
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.

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 the communities within the VRF instance are displayed.

Format: `show ip bgp [vrf` *`vrf-name`*`] update-group [group-index | peer-address ]`

Command mode: Privileged

Parameter	*Description*
group-index	(Optional) If specified, this option restricts the output to a single update group.
peer-address	(Optional) If specified, this option restricts the output to the update group containing the peer with the given address.

The command outputs the following information.

Parameter	*Description*
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 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 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:

Parameter	***Description***
Version	The UPDATE version.
Delta T	The amount of time elapsed since the update send process executed. hours::minutes::seconds.
Duration	How long the update send process took, in milliseconds.
UPD Built	The number of UPDATE messages built.
UPD Sent	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	The number of paths advertised.
Pfxs Adv	The number of prefixes advertised.
Pfxs Wd	The number of prefixes withdrawn.

show ip bgp vpnv4

This command displays the VPNv4 address information in the BGP table. If an optional VRF is specified, the address information for communities within that VRF instance are displayed.

Format: `show ip bgp vpnv4 {all | rd` *`route-distinguisher`* `| vrf` *`vrf-name`*`} [`*`ip-prefix/length`*`]`

Command mode: Privileged

Parameter	*Description*
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 communities within the named VRF instance.
ip-prefix/length	IP address (in dotted decimal format) and the length of the mask (0 to 32). The slash (/) mark must be included.

The command outputs the following information, depending on the selected parameters.

Parameter	*Description*
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. • *: BGP never displays invalid routes; so this code is always displayed (to maintain consistency with the industry 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	BGP metric.
LocPrf	The local preference.
Path	The AS Path for the 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	AS Path. This form of the 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	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 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.

show bgp ipv6

Use the show bgp ipv6 command in Privileged mode to display IPv6 routes in the BGP routing table.

Format: `show bgp ipv6 [`*`ipv6-prefix`*`|`*`prefix-length`* `[longer-prefixes | shorter-prefixes [`*`Length`*`]] | filter-list `*`as-path-list`*`]`

Command mode: Privileged

Parameter	*Description*
ipv6-prefix 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	(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.
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.

The command output displays the following information.

Parameter	*Description*
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. • *: 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: 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 attribute
LocPrf	The local preference
Path	AS Path
Origin	Value of the Origin attribute.

show bgp ipv6 aggregate-address

This command lists IPv6 aggregate addresses that have been configured and indicates whether each is currently active.

Format: `show bgp ipv6 aggregate-address`

Command mode: Privileged

Parameter	*Description*
Prefix/Len	The 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 of AS 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.

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*.

Format: `show bgp ipv6 community` *communities* `[exact-match]`

Command mode: Privileged

Parameter	*Description*
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.

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.

Format: `show bgp ipv6 community-list` *name* `[exact-match]`

Command mode: Privileged

Parameter	*Description*
name	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.

show bgp ipv6 listen range

This command displays information about BGP listen ranges.

Format: `show bgp ipv6 listen range [`*network/length*`]`

Command mode: Privileged

Parameter	*Description*
listen range	Displays all listen subnet ranges that have been created.
network / length	Displays information about specified listen range.

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.

Format: `show bgp ipv6 neighbors {`*ipv4-address* | *ipv6-address* `[interface` *interface-name*`]|autodetect interface` *interface-name*`} advertised-routes`

Command mode: Privileged

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.

Format: `show bgp ipv6 neighbors [`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`* `{received-routes | routes | rejected-routes}`

Command mode: Privileged

show bgp ipv6 neighbors policy

Use 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. Specifying an IPv4 or IPv6 address limits the output to a single neighbor. If the neighbor’s address is a link local address, the interface must be specified.

Format: `show bgp ipv6 neighbors [`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`* `policy`

Command mode: Privileged

show bgp ipv6 route-reflection

This command shows the configuration of the local router as a route reflector.

Format: `show bgp ipv6 route-reflection`

Command mode: Privileged

Parameter	*Description*
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.

show bgp ipv6 statistics

This command shows statistics for the IPv6 decision process. The description of the output and fields are similar to those shown in the show ip bgp statistics command.

Format: `show bgp ipv6 statistics`

Command mode: Privileged

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.

Format: `show bgp ipv6 summary`

Command mode: Privileged

show bgp ipv6 update-group

This command reports the status of IPv6 outbound update groups and their numbers. The description of the output and fields are similar to those shown in the show ip bgp template command.

Format: `show bgp ipv6 update-group [`*`group-index`*` | `*`ipv4-address`*` | `*`ipv6-address`*` [interface `*`interface-name`*`] autodetect interface `*`interface-name`*

Command mode: Privileged

Parameter	*Description*
group-index	(Optional) If specified, this option restricts the output to a single update group.
ipv4-address	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	The neighbor's IPv6 address. 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.
autodetect interface	The routing interface on which the neighbor's link local iPv6 address is auto-detected.

12.1 Routing Policy configuration 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.

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 ACL 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.

The router 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.

Table 12.1 lists AS path list regular expression syntax.

Default: No AS path lists are configured by default. There are no default values for any of the parameters of this command.

Format: `ip as-path access-list` *`as-path-list-number`* `{permit|deny}` *`regexp`*

Command mode: Global Config

Parameter	*Description*
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 12.1. ACL AS Path Regular Expression Syntax

Special Character	*Symbol*	*Action*
asterisk	*	Matches zero or more sequences of the pattern.
sq. 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.
question mark	?	Matches 0 or 1 occurrences of the pattern.
underscore	_	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.

no ip as-path access-list

To delete an AS path access list, use the no form of this command.

Format: `no ip as-path access-list` *`as-path-list-number`*

Command mode: Global Config

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.

Default: Standard communities are displayed in AA:NN format.

Format: `ip bgp-community new-format`

Command mode: Global Config

no ip bgp-community new-format

To display BGP standard communities as 32-bit integers, use the **no** form of this command.

Format: `no ip bgp-community new-format`

Command mode: Global Config

ip community-list

To create or configure a BGP community list, use the ip community-list command in Global Configuration mode. A community 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.

Default: No community lists are configured by default.

Format: `ip community-list standard` *`list-name`* `{permit | deny} [`*`community-number`*`] [no- advertise] [no-export]`

Command mode: Global Config

Parameter	***Description***
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-number	From zero to 16 community numbers formatted as a 32-bit integers or in AA:NN format, where AA 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	The well-known standard community, NO_ADVERTISE (0xFFFFFF02).
no-export	The well-known standard community, NO_EXPORT, (0xFFFFFF01).

no ip community-list

To delete a community list, use the **no** form of the command.

Format: `no ip community-list standard` *`list-name`*

Command mode: Global Config

show ip as-path-access-list

This command displays the contents of AS path access lists.

Format: `show ip as-path-access-list [as-path-list-number]`

Command mode: Privileged

Parameter	*Description*
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.

show ip community-list

This command displays community lists. The format of community values is dictated by the command *ip bgp-community new-format*.

Format: `show ip community-list [community-list-name]`

Command mode: Privileged

Parameter	*Description*
community-list-name	(Optional) A standard community list name. This option limits the output to a single list.

clear ip community-list

This command clears community lists.

Format: `clear ip community-list [community-list-name]`

Command mode: Privileged

Parameter	*Description*
community-list-name	(Optional) A community list name.

13 IPV6 MANAGEMENT COMMANDS

This chapter describes the IPv6 commands available in the CLI.

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.**

13.1 IPv6 management commands

The switch provides following IPv6 capabilities:

- Static assignment of IPv6 addresses and gateways for the service/network ports.
- The ability to ping an IPv6 link-local address over the service/network port.
- Using IPv6 Management commands, you can send SNMP traps and queries via the service/network port.
- The user can manage a device via the network port (in addition to a Routing Interface or the Service port).

serviceport ipv6 enable

Use this command to enable IPv6 operation on the service port. By default, IPv6 operation is enabled on the service port.

Default: enabled

Format: `serviceport ipv6 enable`

Command mode: Privileged

no serviceport ipv6 enable

Use this command to disable IPv6 operation on the service port.

Format: `no serviceport ipv6 enable`

Command mode: Privileged

network ipv6 enable

Use this command to enable IPv6 operation on the network port. By default, IPv6 operation is enabled on the network port.

Default: enabled

Format: `network ipv6 enable`

Command mode: Privileged

no network ipv6 enable

Use this command to disable IPv6 operation on the network port.

Format: `no network ipv6 enable`

Command mode: Privileged

serviceport ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information on the service port.

Multiple IPv6 prefixes can be configured on the service port.

Format: `serviceport ipv6 address {address/prefix-length [eui64]|autoconfig|dhcp}`

Command mode: Privileged

Parameter	*Description*
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 address format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

no serviceport ipv6 address

Use the *no serviceport ipv6 address* command to remove all configured IPv6 prefixes on the service port interface.

Use the command with the *address* option to remove the manually configured IPv6 global address on the network port interface.

Use the command with the *autoconfig* option to disable the stateless global address autoconfiguration on the service port.

Use the command with the *dhcp* option to disable the dhcpv6 client protocol on the service port.

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

Command mode: Privileged

serviceport ipv6 gateway

Use this command to configure IPv6 gateway (i.e. Default routers) information for the service port.

Only a single IPv6 gateway address can be configured for the service port. There may be a combination of IPv6 prefixes and gateways that are explicitly configured and those that are set throughauto-address configuration with a connected IPv6 router on their service port interface.

Format: `serviceport ipv6 gateway` *`gateway-address`*

Command mode: Privileged

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

no serviceport ipv6 gateway

Use this command to remove IPv6 gateways on the service port interface.

Format: `no serviceport ipv6 gateway`

Command mode: Privileged

serviceport ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for the service port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format: `serviceport ipv6 neighbor` *`ipv6-address macaddr`*

Command mode: Privileged

Parameter	*Description*
ipv6-address	The IPv6 address of the neighbor or interface.
macaddr	The link-layer address.

no serviceport ipv6 neighbor

Use this command to remove IPv6 neighbors from the IPv6 neighbor table for the service port.

Format: `no serviceport ipv6 neighbor` *`ipv6-address macaddr`*

Command mode: Privileged

network ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information for the network port. Multiple IPv6 addresses can be configured on the network port.

Format: `network ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`

Command mode: Privileged

Parameter	*Description*
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 address format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

no network ipv6 address

The *no network ipv6 address* command removes all configured IPv6 prefixes.

Use the command with the *address* option to remove the manually configured IPv6 global address on the network port interface.

Use the command with the autoconfig option to disable the stateless global address autoconfiguration on the network port.

Use this command with the *dhcp* option to disable the dhcpv6 client protocol on the network port.

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

Command mode: Privileged

network ipv6 gateway

Use this command to configure IPv6 gateway (i.e. default routers) information for the network port.

Format: `network ipv6 gateway` *`gateway-address`*

Command mode: Privileged

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

no network ipv6 gateway

Use this command to remove IPv6 gateways on the network port interface.

Format: `no network ipv6 gateway`

Command mode: Privileged

network ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for this network port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format: `network ipv6 neighbor` *`ipv6-address macaddr`*

Command mode: Privileged

Parameter	*Description*
ipv6-address	The IPv6 address of the neighbor or interface.
macaddr	The link-layer address.

no network ipv6 neighbor

Use this command to remove IPv6 neighbors from the neighbor table.

Format: `no network ipv6 neighbor` *`ipv6-address macaddr`*

Command mode: Privileged

show network ipv6 neighbors

Use this command to display the information about the IPv6 neighbor entries cached on the network port. The information is updated to show the type of the entry.

Default: none

Format: `show network ipv6 neighbors`

Command mode: Privileged

Parameter	*Description*
IPv6 Address	The neighbor’s IPv6 address.
MAC Address	The neighbor's MAC Address.
isRtr	Shows whether the neighbor is a router. If TRUE, the neighbor is a router; FALSE it is not a router.
Neighbor State	The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe and Unknown.
Age	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.

show serviceport ipv6 neighbors

Use this command to displays information about the IPv6 neighbor entries cached on the service port. The information is updated to show the type of the entry.

Default: none

Format: `show serviceport ipv6 neighbors`

Command mode: Privileged

Parameter	*Description*
IPv6 Address	The neighbor's IPv6 address.
MAC Address	The neighbor's MAC Address.
isRtr	Shows whether the neighbor is a router. If TRUE, the neighbor is a router; FALSE it is not a router.
Neighbor State	The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe and Unknown.
Age	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.

ping ipv6

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI interface. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the *ping* utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *ipv6-address*|*hostname* parameter to ping an interface by using the global IPv6 address of the interface. Use the optional *size* keyword to specify the size of the ping packet. Use the outgoing-interface option to specify the outgoing interface for a multicast IP/IPv6 ping.

You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address *ipv6-global-address*|*hostname*. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the *ping* or *traceroute* request is routed out the service/network port properly. When referencing an IPv6 *link-local* address, you must also specify the service or network port interface by using the *serviceport* or *network* parameter.

Default: the default count is 1;
the default interval is 3 seconds;
the default size is 0 bytes.

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

Command mode: Privileged

User

ping ipv6 interface

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three *ping*s to the target station. Use the *interface* keyword to ping an interface by using the *link-local* address or the global IPv6 address of the interface. You can use a loopback, network port, serviceport, tunnel, or physical interface as the source. Use the optional *size* keyword to specify the size of the ping packet. The *ipv6-address* is the link local IPv6 address of the device you want to query. Use the outgoing-interface option to specify the outgoing interface for a multicast IP/IPv6 ping.

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

Command mode: Privileged

User

Keyword	***Description***
interface	Use the interface keyword to ping an interface by using the link-local address or the global IPv6 address of the interface.
size	Use the optional size keyword to specify the size of the ping packet.
ipv6-address	The link local IPv6 address of the device you want to query.

13.2 Tunnel Interface configuration commands

The commands in this section describe how to create, delete, and manage tunnel interfaces. Several different types of tunnels provide functionality to facilitate the transition of IPv4 networks to IPv6 networks. These tunnels are divided into two classes: configured and automatic. The distinction is that configured tunnels are explicitly configured with a destination or endpoint of the tunnel. Automatic tunnels, in contrast, infer the endpoint of the tunnel from the destination address of packets routed into the tunnel. To assign an IP address to the tunnel interface, see the ip address command. To assign an IPv6 address to the tunnel interface, see the ipv6 address command.

interface tunnel

Use this command to enter the Interface Config mode for a tunnel interface. The *tunnel-id* range is 0 to 7.

Format: interface tunnel *tunnel-id*

Command mode: Global Config

no interface tunnel

This command removes the tunnel interface and associated configuration parameters for the specified tunnel interface.

Format: `no interface tunnel` *`tunnel-id`*

Command mode: Global Config

tunnel source

This command specifies the source transport address of the tunnel, either explicitly or by reference to an interface.

Format: `tunnel source {`*`ipv4-address`* | `ethernet` *`unit/slot/port`*`}`

Command mode: Interface Config

tunnel destination

This command specifies the destination transport address of the tunnel.

Format: `tunnel destination {`*`ipv4-address`*`}`

Command mode: Interface Config

tunnel mode ipv6ip

This command specifies the mode of the tunnel. With the optional 6to4 argument, the tunnel mode is set to 6to4 automatic. Without the optional 6to4 argument, the tunnel mode is configured.

Format: `tunnel mode ipv6ip [6to4]`

Command mode: Interface Config

show interface tunnel

This command displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

Format: `show interface tunnel [`*`tunnel-id`*`]`

Command mode: Privileged

If you do not specify a tunnel ID, the command shows the following information for each configured tunnel:

Term	*Value*
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.

If you specify a tunnel ID, the command shows the following information for the tunnel:

Term	*Value*
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	If you enable IPv6 on the interface and assign an address, the IPv6 address and prefix display.

13.3 Loopback Interface configuration commands

The commands in this section describe how to create, delete, and manage *loopback* interfaces. A *loopback* interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols.

To assign an IP address to the *loopback* interface, see the *ip address* command. To assign an IPv6 address to the *loopback* interface, see the *ipv6 address* command.

interface loopback

Use this command to enter the Interface Config mode for a loopback interface. The range of the loopback ID is from 0 to 7.

Format: `interface loopback` *`Loopback-id`*

Command mode: Global Config

no interface loopback

This command removes the *loopback* interface and associated configuration parameters for the specified loopback interface.

Format: `no interface loopback` *`Loopback-id`*

Command mode: Global Config

show interface loopback

This command displays information about configured *loopback* interfaces.

Format: `show interface loopback [`*`Loopback-id`*`]`

Command mode: Privileged

If you do not specify a *loopback* ID, the following information appears for each loopback interface on the system:

Term	*Value*
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 you specify a loopback ID, the following information appears:

Term	*Value*
Interface Link Status	Shows whether the link is up or down.
IP Address	The IPv4 address of the interface.
MTU Size	The maximum transmission unit for packets on the interface in bytes.

13.4 IPv6 Routing commands

This section describes the IPv6 commands you use to configure IPv6 on the system and on the interfaces. This section also describes IPv6 management commands and show commands.

ipv6 hop-limit

This command defines the unicast hop count used in ipv6 packets originated by the node. The value is also included in router advertisements. Valid values for hops are 1-255 inclusive. The default not configured means that a value of zero is sent in router advertisements and a value of 64 is sent in packets originated by the node. Note that this is not the same as configuring a value of 64.

Default: not configured

Format: `ipv6 hop-limit` *hops*

Command mode: Global Config

no ipv6 hop-limit

This command returns the unicast hop count to the default.

Format: `no ipv6 hop-limit`

Command mode: Global Config

ipv6 unicast-routing

Use this command to enable the forwarding of IPv6 unicast datagrams.

Default: disabled

Format: `ipv6 unicast-routing`

Command mode: Global Config

no ipv6 unicast-routing

Use this command to disable the forwarding of IPv6 unicast datagrams.

Format: `no ipv6 unicast-routing`

Command mode: Global Config

ipv6 enable

Use this command to enable IPv6 routing on an interface or range of interfaces, including tunnel and loopback interfaces, that has not been configured with an explicit IPv6 address. When you use this command, the interface is automatically configured with a link-local address. You do not need to use this command if you configured an IPv6 global address on the interface.

Default: disabled

Format: `ipv6 enable`

Command mode: Interface Config

no ipv6 enable

Use this command to disable IPv6 routing on an interface.

Format: `no ipv6 enable`

Command mode: Interface Config

ipv6 address

Use this command to configure an IPv6 address on an interface or range of interfaces, including tunnel and loopback interfaces, and to enable IPv6 processing on this interface. You can assign multiple globally reachable addresses to an interface by using this command. You do not need to assign a link-local address by using this command since one is automatically created. The prefix field consists of the bits of the address to be configured. The prefix_length designates how many of the high-order contiguous bits of the address make up the prefix.

You can express IPv6 addresses in eight blocks. Also of note is that instead of a period, a colon now separates each block. For simplification, leading zeros of each 16 bit block can be omitted. One sequence of 16 bit blocks containing only zeros can be replaced with a double colon "::", but not more than one at a time (otherwise it is no longer a unique representation).

- 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 in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is `3ffe:1::1234/64`.

The optional [eui-64] field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address. If you use this option, the value of prefix_length must be 64 bits.

Format: `ipv6 address` *`prefix/prefix_length`* `[eui64]`

Command mode: Interface Config

no ipv6 address

Use this command to remove all IPv6 addresses on an interface or specified IPv6 address. The prefix parameter consists of the bits of the address to be configured. The prefix_length designates how many

of the high-order contiguous bits of the address make up the prefix. The optional [eui-64] field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address.

If you do not supply any parameters, the command deletes all the IPv6 addresses on an interface.

Format: `no ipv6 address [prefix/prefix_length] [eui64]`

Command mode: Interface Config

ipv6 address autoconfig

Use this command to allow an in-band interface to acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages.

Default: disabled

Format: `ipv6 address autoconfig`

Command mode: Interface Config

no ipv6 address autoconfig

This command the IPv6 autoconfiguration status on an interface to the default value.

Format: `no ipv6 address autoconfig`

Command mode: Interface Config

ipv6 address dhcp

This command enables the DHCPv6 client on an in-band interface so that it can acquire network information, such as the IPv6 address, from a network DHCP server.

Default: disabled

Format: `ipv6 address dhcp`

Command mode: Interface Config

no ipv6 address dhcp

This command releases a leased address and disables DHCPv6 on an interface.

Format: `no ipv6 address dhcp`

Command mode: Interface Config

ipv6 route

Use this command to configure an IPv6 static route. The ipv6-prefix is the IPv6 network that is the destination of the static route. The prefix_length is the length of the IPv6 prefix — a decimal value (usually 0-64) that shows 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 prefix_length. The next-hop-address is the IPv6 address of the next hop that can be used to reach the specified network. Specifying Null0 as nexthop parameter adds a static reject route. The preference parameter is a value the router uses to compare this route with routes from other route sources that have the same destination. The range for preference is 1–255, and the default value is 1. The argument unit/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 unit/slot/port format. You can specify a unit/slot/port or vlan id or tunnel tunnel_id interface to identify direct static routes from point- to-point and broadcast interfaces. The interface must be specified when using a link-local address as the next hop. A route with a preference of 255 cannot be used to forward traffic.

Default: disabled

Format: `ipv6 route` *ipv6-prefix/prefix_length* {*next-hop-address* | `Null0` | `interface` {*unit/ slot/port*|`vlan` *1-4093*|`tunnel` *tunnel_id*} *next-hop-address*} [*preference*]

Command mode: Global Config

no ipv6 route

Use this command to delete an IPv6 static route. Use the command without the optional parameters to delete all static routes to the specified destination. Use the *preference* parameter to revert the preference of a route to the default preference.

Format: `no ipv6 route` *ipv6-prefix/prefix_length* [{*next-hop-address* | `Null0` | `interface` {*unit/ slot/port*|`vlan` *1-4093*|`tunnel` *tunnel_id*} *next-hop-address* | *preference*}]

Command mode: Global Config

ipv6 route distance

This command sets the default distance (preference) for IPv6 static routes. Lower route distance values are preferred when determining the best route. The ipv6 route command allows you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in this command.

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 ipv6 route distance command.

Default: 1

Format: `ipv6 route distance` *1-255*

Command mode: Global Config

no ipv6 route distance

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

Format: `no ipv6 route distance`

Command mode: Global Config

ipv6 route net-prototype

This command adds net prototype IPv6 routes to the hardware.

Format: `ip route net-prototype` *prefix/prefix-length nexthopip num-routes*

Command mode: Global Config

Parameter	*Description*
prefix/prefix-length	The destination network and mask for the route.
nexthopip	The next-hop ip address, It must belong to an active routing interface, but it does not need to be resolved.
num-routes	The number of routes need to added into hardware starting from the given prefix argument and within the given prefix-length.

no ipv6 route net-prototype

This command deletes all the net prototype IPv6 routes added to the hardware.

Format: `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*

Command mode: Global Config

ipv6 mtu

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface or range of interfaces. This command replaces the default or link MTU with a new MTU value.

The default MTU value for a tunnel interface is 1480. You cannot change this value.

Default: 1500

Format: `ipv6 mtu 1280-12270 (for MES5448)/ipv6 mtu 1280-9394 (for MES7048)`

Command mode: Interface Config

no ipv6 mtu

This command resets maximum transmission unit value to default value.

Format: `no ipv6 mtu`

Command mode: Interface Config

ipv6 nd dad attempts

This command sets the number of duplicate address detection attempts transmitted on an interface or range of interfaces. Duplicate address detection verifies that an IPv6 address on an interface is unique.

Default: 1

Format: `ipv6 nd dad attempts` *`0 - 600`*

Command mode: Interface Config

no ipv6 nd dad attempts

This command resets to number of duplicate address detection value to default value.

Format: `no ipv6 nd dad attempts`

Command mode: Interface Config

ipv6 nd managed-config-flag

This command sets the “managed address configuration” flag in router advertisements on the interface or range of interfaces. When the value is true, end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

Default: false

Format: `ipv6 nd managed-config-flag`

Command mode: Interface Config

no ipv6 nd managed-config-flag

This command resets the “managed address configuration” flag in router advertisements to the default value.

Format: `no ipv6 nd managed-config-flag`

Command mode: Interface Config

ipv6 nd ns-interval

This command sets the interval between router advertisements for advertised neighbor solicitations, in milliseconds. An advertised value of 0 means the interval is unspecified. This command can configure a single interface or a range of interfaces.

Default: 0

Format: `ipv6 nd ns-interval {`*`1000-4294967295 | 0`*`}`

Command mode: Interface Config

no ipv6 nd ns-interval

This command resets the neighbor solicit retransmission interval of the specified interface to the default value.

Format: `no ipv6 nd ns-interval`

Command mode: Interface Config

ipv6 nd other-config-flag

This command sets the “other stateful configuration” flag in router advertisements sent from the interface.

Default: false

Format: `ipv6 nd other-config-flag`

Command mode: Interface Config

no ipv6 nd other-config-flag

This command resets the “other stateful configuration” flag back to its default value in router advertisements sent from the interface.

Format: `no ipv6 nd other-config-flag`

Command mode: Interface Config

ipv6 nd ra-interval

This command sets the transmission interval between router advertisements on the interface or range of interfaces.

Default: 600

Format: `ipv6 nd ra-interval-max` *4- 1800*

Command mode: Interface Config

no ipv6 nd ra-interval

This command sets router advertisement interval to the default.

Format: `no ipv6 nd ra-interval-max`

Command mode: Interface Config

ipv6 nd ra-lifetime

This command sets the value, in seconds, that is placed in the *Router Lifetime* field of the router advertisements sent from the interface or range of interfaces. The *lifetime* value must be zero, or it must be an integer between the value of the router advertisement transmission interval and 9000. A value of zero means this router is not to be used as the default router.

Default: 1800

Format: `ipv6 nd ra-lifetime` *lifetime*

Command mode: Interface Config

no ipv6 nd ra-lifetime

This command resets router lifetime to the default value.

Format: `no ipv6 nd ra-lifetime`

Command mode: Interface Config

ipv6 nd ra hop-limit unspecified

This command configures the router to send Router Advertisements on an interface with an unspecified (0) Current Hop Limit value. This tells the hosts on that link to ignore the Hop Limit from this Router.

Default: disabled

Format: `ipv6 nd ra hop-limit unspecified`

Command mode: Interface Config

no ipv6 nd ra hop-limit unspecified

This command configures the router to send Router Advertisements on an interface with the global configured Hop Limit value.

Format: `no ipv6 nd ra hop-limit unspecified`

Command mode: Interface Config

ipv6 nd reachable-time

This command sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation. Reachable time is specified in milliseconds. A value of zero means the time is unspecified by the router. This command can configure a single interface or a range of interfaces.

Default: 0

Format: `ipv6 nd reachable-time` *`0–4294967295`*

Command mode: Interface Config

no ipv6 nd reachable-time

This command means reachable time is unspecified for the router.

Format: `no ipv6 nd reachable-time`

Command mode: Interface Config

ipv6 nd router-preference

Use this command to configure default router preferences that the interface advertises in router advertisement messages.

Default: medium

Format: `ipv6 nd router-preference { low | medium | high}`

Command mode: Interface Config

no ipv6 nd router-preference

This command resets the router preference advertised by the interface to the default value.

Format: `no ipv6 nd router-preference`

Command mode: Interface Config

ipv6 nd suppress-ra

This command suppresses router advertisement transmission on an interface or range of interfaces.

Default: disabled

Format: `ipv6 nd suppress-ra`

Command mode: Interface Config

no ipv6 nd suppress-ra

This command enables router transmission on an interface.

Format: `no ipv6 nd suppress-ra`

Command mode: Interface Config

ipv6 nd prefix

Use the *ipv6 nd prefix* command to configure parameters associated with prefixes the router advertises in its router advertisements. The first optional parameter is the valid lifetime of the router, in seconds. You can specify a value or indicate that the lifetime value is infinite. The second optional parameter is the *preferred* lifetime of the router.

This command can be used to configure a single interface or a range of interfaces.

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the *ipv6 address* interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the ipv6 nd prefix command to configure these values.

The *ipv6 nd prefix* command allows you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the *ipv6 address* command. Prefixes specified using *ipv6 nd prefix* without associated interface address will not be included in RAs and will not be committed to the device configuration.

Default: valid-lifetime — 2 592 000;
preferred-lifetime — 604 800;
autoconfig — enabled;
on-link — enabled.

Format: `ipv6 nd prefix` *`prefix/prefix_length [{0-4294967295 | infinite} {0-4294967295 | infinite}] [no-autoconfig off-link]`*

Command mode: Interface Config

no ipv6 nd prefix

This command sets prefix configuration to default values.

Format: `no ipv6 nd prefix` *`prefix/prefix_length`*

Command mode: Interface Config

ipv6 neighbor

Configures a static IPv6 neighbor with the given IPv6 address and MAC address on a routing or host interface.

Format: `ipv6 neighbor` *`ipv6address`* `{`*`unit/slot/port`*`|vlan` *`1-4093`*`}` *`macaddr`*

Command mode: Global Config

Parameter	*Description*
ipv6address	The neighbor's IPv6 address.
unit/slot/port	The *unit/slot/port* for the interface.
vlan	The VLAN for the interface.
macaddr	The neighbor's MAC Address.

no ipv6 neighbor

Removes a static IPv6 neighbor with the given IPv6 address on a routing or host interface.

Format: `no ipv6 neighbor` *ipv6address* {*unit/slot/port*|`vlan` *1-4093*}

Command mode: Global Config

ipv6 neighbors dynamicrenew

Use this command to automatically renew the IPv6 neighbor entries. Enables/disables the periodic NUD (neighbor unreachability detection) to be run on the existing IPv6 neighbor entries based on the activity of the entries in the hardware. If the setting is disabled, only those entries that are actively used in the hardware are triggered for NUD at the end of STALE timeout of 1200 seconds. If the setting is enabled, periodically every 40 seconds a set of 300 entries are triggered for NUD irrespective of their usage in the hardware.

Default: disabled

Format: `ipv6 neighbors dynamicrenew`

Command mode: Global Config

no ipv6 neighbors dynamicrenew

Disables automatic renewing of IPv6 neighbor entries.

Format: `no ipv6 neighbors dynamicrenew`

Command mode: Global Config

ipv6 nud

Use this command to configure Neighbor Unreachability Detection (NUD). NUD verifies that communication with a neighbor exists.

Format: `ipv6 nud {backoff-multiple | max-multicast-solicits | max-unicast-solicits}`

Command mode: Global Config

Parameter	*Description*
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.

ipv6 prefix-list

To create a prefix list or add a prefix list entry, use the *ipv6 prefix-list* command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes of 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. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assume 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 *match ip address*.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

Default: No prefix lists are 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.

Format: `ipv6 prefix-list` *`list-name`* `{[seq` *`number`*`] {permit | deny}` *`ipv6-prefix/prefix-length`* `[ge` *`length`*`] [le` *`length`*`] | renumber` *`renumber-interval first-statement-number`*`}`

Command mode: Global Config

Term	***Value***
list-name	The text name of the prefix list. The length is 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 more 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	(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.

no ipv6 prefix-list

To delete a prefix list or a statement in a prefix list, use the **no** form of this command. The command **no ipv6 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.

Format: `no ipv6 prefix-list` *`list-name`* `[seq` *`number`*`] {permit | deny}` *`network/length`* `[ge` *`length`*`] [le` *`length`*`]`

Command mode: Global Config

ipv6 unreachables

Use this command to enable the generation of ICMPv6 Destination Unreachable messages on the interface or range of interfaces. By default, the generation of ICMPv6 Destination Unreachable messages is enabled.

Default: enabled

Format: `ipv6 unreachables`

Command mode: Interface Config

no ipv6 unreachables

Use this command to prevent the generation of ICMPv6 Destination Unreachable messages.

Format: `no ipv6 unreachables`

Command mode: Interface Config

ipv6 unresolved-traffic

Use this command to control the rate at which IPv6 data packets come into the CPU. By default, rate limiting is disabled. When enabled, the rate can range from 50 to 1024 packets per second.

Default: 1024

Format: `ipv6 unresolved-traffic rate-limit` *`<50-1024>`*

Command mode: Global Config

no ipv6 unresolved-traffic

Use this command to disable the rate limiting.

Format: `no ipv6 unresolved-traffic rate-limit`

Command mode: Global Config

ipv6 icmp error-interval

Use this command to limit the rate at which ICMPv6 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 ICMPv6 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).

Default: *burst-interval* – 1000 ms.
burst-size – *100 messages*.

Format: ipv6 icmp error-interval *burst-interval* [*burst-size*]

Command mode: Global Config

no ipv6 icmp error-interval

Use the *no* form of the command to return **burst-interval** and *burst-size* to their default values.

Format: `no ipv6 icmp error-interval`

Command mode: Global Config

show ipv6 brief

Use this command to display the IPv6 status of forwarding mode and IPv6 unicast routing mode.

Format: `show ipv6 brief`

Command mode: Privileged

Term	*Value*
IPv6 Forwarding Mode	Shows whether the IPv6 forwarding mode is enabled.
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 the ipv6 hop-limit command.
ICMPv6 Rate Limit Error Interval	Shows how often the token bucket is initialized with burst-size tokens. For more information, see the ipv6 icmp error-interval command.
ICMPv6 Rate Limit Burst Size	Shows the number of ICMPv6 error messages that can be sent during one burst-interval. For more information, see the ipv6 icmp error-interval command.
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.

show ipv6 interface

Use this command to show the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent. The *unit/slot/port* argument 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 *unit/ slot/port* format. The keyword **loopback** specifies the loopback interface directly. The keyword tunnel specifies the IPv6 tunnel interface.

Format: `show ipv6 interface {brief | unit/slot/port|vlan 1-4093|loopback 0-7|tunnel 0-7}`

Command mode: Privileged

If you use the *brief* parameter, the following information displays for all configured IPv6 interfaces:

Term	*Value*
Interface	The interface in unit/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 form a DHCP server; • Manual — the address is manually configured. Global addresses with no annotation are assumed to be manually configured.

If you specify an interface, the following information also appears.

Term	*Value*
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 the bandwidth of the interface.
Interface Maximum Transmission Unit	The MTU size, in bytes.
Router Duplicate Address Detection Transmits	The number of consecutive duplicate address detection attempts to transmit.
Address Autoconfigure Mode	Shows whether the autoconfigure mode is enabled or disabled.
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).
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.

If an IPv6 prefix is configured on the interface, the following information also appears.

Term	*Value*
IPv6 Prefix is	The IPv6 prefix for the 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.

show ipv6 interface vlan

Use the *show ipv6 interface vlan* in Privileged mode to show to show the usability status of IPv6 VLAN interfaces.

Format: `show ipv6 interface vlan` *vlan-id* `[prefix]`

Command mode: Privileged

User

Parameter	***Description***
vlan-id	A valid VLAN identifier.
prefix	Display IPv6 Interface Prefix Information.

show ipv6 dhcp interface

This command displays a list of all IPv6 addresses currently leased from a DHCP server on a specific in-band interface. The *unit/slot/port* argument 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 *unit/ slot/port* format.

Format: `show ipv6 dhcp [interface {`*unit/slot/port*`|vlan` *1-4093*`}]`

Command mode: Privileged

Term	***Value***
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 and 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.

show ipv6 nd raguard policy

This command shows the status of IPv6 RA GUARD feature on the switch. It lists the ports/interfaces on which this feature is enabled and the associated device role.

Format: `show ipv6 nd raguard policy`

Command mode: Privileged

Parameter	*Description*
Interface	The port/interface on which this feature is enabled.
Role	The associated device role for the interface.

show ipv6 neighbors

Use this command to display information about the IPv6 neighbors.

Format: `show ipv6 neighbor [interface {`*`unit/slot/port`* `| vlan` *`1-4093`* `| tunnel` *`0-7`*`} |` *`ipv6- address`*`]`

Command mode: Privileged

Term	*Value*
Interface	The interface in unit/slot/port format. IPV6 address of neighbor or interface.
MAC Address	The neighbor's MAC 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	The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe and Unknown.
Age	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.

clear ipv6 neighbors

Use this command to clear all entries IPv6 neighbor table or an entry on a specific interface. Use the *unit/slot/port* parameter to specify an interface, the *ipv6address* parameter to specify an IPV6 address, or the vlan parameter to specify a VLAN.

Format: `clear ipv6 neighbors [{unit/slot/port | ipv6address | vlan id}]`

Command mode: Privileged

show ipv6 protocols

This command lists a summary of the configuration and status for the active IPv6 routing protocols. The command lists routing protocols that are configured and enabled. If a protocol is selected on the command line, the display will be limited to that protocol.

Format: `show ipv6 protocols [bgp|ospf]`

Command mode: Privileged

Term	*Value*
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. 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 an 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.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked “active”.
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
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.
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.

show ipv6 route

This command displays the IPv6 routing table. The *ipv6-address* specifies a specific IPv6 address for which the best-matching route would be displayed. The *ipv6-prefix/ipv6-prefix-length* specifies a specific IPv6 network for which the matching route would be displayed. The *interface* specifies that the routes with next-hops on the interface be displayed. The *unit/slot/port* argument 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 *unit/ slot/port* format. The *protocol* specifies the protocol that installed the routes. The *protocol* is one of the following keywords: *connected, ospf, static.* The *all* specifies that all routes including best and nonbest routes are displayed. Otherwise, only the best routes are displayed.

If you use the *connected* keyword for *protocol*, the *all* option is not available because there are no best or nonbest connected routes.

Format: `show ipv6 route [{`*`ipv6-address`* `[`*`protocol`*`] | {{`*`ipv6-prefix/ipv6-prefix-length`* `|` *`unit/ slot/port`*`|vlan` *`1-4093`*`} [`*`protocol`*`] |` *`protocol`* `| summary} [all] | all}]`

Command mode: Privileged

User

The columns for the routing table display the following information:

Term	*Value*
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 toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format for the 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 routing 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/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

show ipv6 route ecmp-groups

This command reports all current ECMP groups in the IPv6 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 IPv6 address and outgoing interface of each next hop in each group.

Format: `show ipv6 route ecmp-groups`

Command mode: Privileged

show ipv6 route hw-failure

Use this command to display the routes that failed to be added to the hardware due to hash errors or a table full condition.

Format: `show ipv6 route hw-failure`

Command mode: Privileged

show ipv6 route net-prototype

This command displays the net-prototype routes. The net-prototype routes are displayed with a P.

Format: `show ipv6 route net-prototype`

Command mode: Privileged

show ipv6 route preferences

Use this command to show the preference value associated with the type of route. Lower numbers have a greater preference. A route with a preference of 255 cannot be used to forward traffic.

Format: `show ipv6 route preferences`

Command mode: Privileged

Term	*Value*
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	Preference 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.

show ipv6 route summary

This command displays a summary of the state of the routing table. When the optional *all* keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the routing table. To include only the number of best routes, do not use the optional keyword.

Format: `show ipv6 route summary [all]`

Command mode: Privileged
User

Term	*Value*
Connected Routes	Total number of connected routes in the routing table.
Static Routes	Total number of static 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.
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	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 Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Hardware Failed Route Adds	The number of routes failed be inserted into the hardware due to hash error or a table full condition.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be

	installed when a routing interface bounces.
Unique Next Hops	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 Water	The highest count of unique next hops since counters were last cleared.
Next Hop Groups	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops.
Next Hop Groups High Water	The highest count of next hop groups since counters were last cleared.
ECMP Groups	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the routing 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.

show ipv6 snooping counters

This command displays the counters associated with IPv6 RA GUARD feature. The number of router advertisement and router redirect packets dropped by the switch globally due to RA GUARD feature are displayed in the command output.

Format: `show ipv6 snooping counters`

Command mode: Privileged

Global Config

show ipv6 vlan

This command displays IPv6 VLAN routing interface addresses.

Format: `show ipv6 vlan`

Command mode: Privileged

User

Term	*Value*
MAC Address used by Routing VLANs	Shows the MAC address.

The rest of the output for this command is displayed in a table with the following column headings:

Column Headings	*Value*
VLAN ID	The VLAN ID of a configured VLAN.
Logical Interface	The interface in unit/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.

show ipv6 traffic

Use this command to show traffic and statistics for IPv6 and ICMPv6. Specify a logical, loopback, or tunnel interface to view information about traffic on a specific interface. The *unit/slot/port* argument 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 *unit/ slot/port* format. If you do not specify an interface, the command displays information about traffic on all interfaces.

Format: `show ipv6 traffic [{`*`unit/slot/port`*`|vlan `*`1-4093`*`| loopback `*`loopback-id`*` | tunnel `*`tunnel- id`*`}]`

Command mode: Privileged

Term	*Value*
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 To 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 necessarily be 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). Forentities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
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 re-assembly.
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 theirfinal 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 ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) 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.
Fragments Created	The number of fragments that were created.
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 ipv6IfIcmpInErrors. 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 ashaving ICMP-specific errors (bad ICMP checksums, bad length, etc.).
ICMPv6 Destination Unreachable Messages Received	Number of ICMP Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively Received	Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages Received	Number of ICMP Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages Received	Number of ICMP Parameter Problem messages received by the interface.
ICMPv6 Packet Too Big Messages Received	Number of ICMP Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	Number of ICMP Echo (request) messages received by the interface.
ICMPv6 Router Solicit Messages Received	Number of ICMP Router Solicit messages received by the interface.
ICMPv6 Neighbor Advertisement Messages Received	Number of ICMP Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	Number of ICMP Redirect messages received by the interface.
ICMPv6 Group Membership Query Messages Received	Number of ICMPv6 Group Membership Query messages received by the interface.
ICMPv6 Group Membership Response Messages Received	Number of ICMPv6 Group Membership Response messages received by the interface.
ICMPv6 Group Membership Reduction Messages Received	Number of ICMPv6 Group Membership reduction messages received by the interface.
Total ICMPv6 Messages Transmitted	Total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
ICMPv6 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 IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	Number of ICMP Destination Unreachable messages sent by the interface.
ICMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP destination unreachable/communication administratively prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	Number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	Number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 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.
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 by the interface.
ICMPv6 Group Membership Query Messages Transmitted	Number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Transmitted	Number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	Number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	Number of duplicate addresses detected by the interface.

clear ipv6 route counters

The command resets to zero the IPv6 routing table counters reported in the *show ipv6 route summary* command. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format: `clear ipv6 route counters`

Command mode: Privileged

clear ipv6 snooping counters

This command clears the counters associated with IPv6 RA GUARD feature.

Format: `clear ipv6 snooping counters`

Command mode: Privileged

Global Config

clear ipv6 statistics

Use this command to clear IPv6 statistics for all interfaces or for a specific interface, including loopback, tunnel, and VLAN interfaces. IPv6 statistics display in the output of the *show ipv6 traffic* command. If you do not specify an interface, the counters for all IPv6 traffic statistics reset to zero.

Format: `clear ipv6 statistics [{`*`unit/slot/port`* `| loopback` *`loopback-id`* `| tunnel` *`tunnel-id`* `| vlan` *`id`*`}]`

Command mode: Privileged

Term	*Value*
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	Preference 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.

13.5 OSPFv3 configuration commands[1]

This section describes the commands you use to configure OSPFv3, which is a link-state routing protocol that you use to route traffic within a network.

13.5.1 Global OSPFv3 Commands

ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Format: `router ospf`

Command mode: Global Config

[1] This functionality is available with an OSPFv3 license. To activate the license, please contact the technical support.

area default-cost

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

Format: `area *areaid* default-cost *1-16777215*`

Command mode: Router OSPFv3 Config

area nssa

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

Format: `area *areaid* nssa`

Command mode: Router OSPFv3 Config

no area nssa

This command disables nssa from the specified area identifier.

Format: `no area *areaid* nssa`

Command mode: Router OSPFv3 Config

area nssa default-info-originate

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is 10. The metric type can be comparable (nssa-external 1) or noncomparable (nssa- external 2).

Format: `area *areaid* nssa default-info-originate [*metric*] [{comparable | non-comparable}]`

Command mode: Router OSPFv3 Config

no area nssa default-info-originate

This command disables the default route advertised into the NSSA.

Format: `no area *areaid* nssa default-info-originate [*metric*] [{comparable | non-comparable}]`

Command mode: Router OSPFv3 Config

area nssa no-redistribute

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

Format: `area *areaid* nssa no-redistribute`

Command mode: Router OSPFv3 Config

no area nssa no-redistribute

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format: `no area *areaid* nssa no-redistribute`

Command mode: Router OSPFv3 Config

area nssa no-summary

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

Format: `area areaid nssa no-summary`

Command mode: Router OSPFv3 Config

no area nssa no-summary

This command disables nssa from the summary LSAs.

Format: `no area areaid nssa no-summary`

Command mode: Router OSPFv3 Config

area nssa translator-role

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

Format: `area areaid nssa translator-role {always | candidate}`

Command mode: Router OSPFv3 Config

no area nssa translator-role

This command disables the nssa translator role from the specified area id.

Format: `no area areaid nssa translator-role {always | candidate}`

Command mode: Router OSPFv3 Config

area nssa translator-stab-intv

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

Format: `area areaid nssa translator-stab-intv stabilityinterval`

Command mode: Router OSPFv3 Config

no area nssa translator-stab-intv

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format: `no area areaid nssa translator-stab-intv stabilityinterval`

Command mode: Router OSPFv3 Config

area range

Use this command to configure a summary prefix that an area border router advertises for a specific area.

Default: No area ranges are configured by default. No cost is configured by default.

Format: area *area-id* range *prefix netmask* {summarylink | nssaexternallink} [advertise | not-advertise] [cost *cost*]

Command mode: Router OSPFv3 Config

Term	*Value*
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	[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.

no area range

The **no** form of this command to delete a summary prefix or remove a static cost.

Format: no area *areaid* range *prefix netmask* {summarylink | nssaexternallink} cost

Command mode: Router OSPFv3 Config

area stub

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

Format: area *areaid* stub

Command mode: Router OSPFv3 Config

no area stub

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

Format: no area *areaid* stub

Command mode: Router OSPFv3 Config

area stub no-summary

This command disables the import of Summary LSAs for the stub area identified by *areaid*.

Default: enabled

Format: `area areaid stub no-summary`

Command mode: Router OSPFv3 Config

no area stub no-summary

This command sets the Summary LSA import mode to the default for the stub area identified by *areaid*.

Format: `no area areaid stub summarylsa`

Command mode: Router OSPFv3 Config

area virtual-link

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

Format: `area areaid virtual-link neighbor`

Command mode: Router OSPFv3 Config

no area virtual-link

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

Format: `no area areaid virtual-link neighbor`

Command mode: Router OSPFv3 Config

area virtual-link dead-interval

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. Value range for *seconds* — from 1 to 65 535.

Default: 40

Format: `area areaid virtual-link neighbor dead-interval seconds`

Command mode: Router OSPFv3 Config

no area virtual-link dead-interval

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

Format: `no area areaid virtual-link neighbor dead-interval`

Command mode: Router OSPFv3 Config

area virtual-link hello-interval

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. Value range for *seconds* — from 1 to 65 535.

Default: 10

Format: `area areaid virtual-link neighbor hello-interval seconds`

Command mode: Router OSPFv3 Config

no area virtual-link hello-interval

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

Format: `no area areaid virtual-link neighbor hello-interval`

Command mode: Router OSPFv3 Config

area virtual-link retransmit-interval

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. Value range for *seconds* — from 1 to 3600.

Default: 5

Format: `area areaid virtual-link neighbor retransmit-interval seconds`

Command mode: Router OSPFv3 Config

no area virtual-link retransmit-interval

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

Format: `no area areaid virtual-link neighbor retransmit-interval`

Command mode: Router OSPFv3 Config

area virtual-link transmit-delay

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

Default: 1

Format: `area areaid virtual-link neighbor transmit-delay seconds`

Command mode: Router OSPFv3 Config

no area virtual-link transmit-delay

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

Format: `no area areaid virtual-link neighbor transmit-delay`

Command mode: Router OSPFv3 Config

auto-cost

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 for OSPF 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). The reference bandwidth range is 1-4294967 Mbps.

Default: 100 Mbps

Format: `auto-cost reference-bandwidth 1-4294967`

Command mode: Router OSPFv3 Config

no auto-cost reference-bandwidth

Use this command to set the reference bandwidth to the default value.

Format: `no auto-cost reference-bandwidth`

Command mode: Router OSPFv3 Config

clear ipv6 ospf

Use this command to disable and re-enable OSPF.

Format: `clear ipv6 ospf`

Command mode: Privileged

clear ipv6 ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format: `clear ipv6 ospf configuration`

Command mode: Privileged

clear ipv6 ospf counters

Use this command to reset global and interface statistics.

Format: `clear ipv6 ospf counters`

Command mode: Privileged

clear ipv6 ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter [neighbor-id].

Format: `clear ipv6 ospf neighbor` *`[neighbor-id]`*

Command mode: Privileged

clear ipv6 ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter [unit/slot/port]. The *unit/slot/port* argument 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 *unit/slot/port* format. To drop adjacency with a specific router ID on a specific interface, use the optional parameter *[neighbor-id]*.

Format: `clear ipv6 ospf neighbor interface [`*`unit/slot/port`*`|vlan` *`1-4093]`* *`[neighbor-id]`*

Command mode: Privileged

clear ipv6 ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and reoriginate prefixes as necessary.

Format: `clear ipv6 ospf redistribution`

Command mode: Privileged

default-information originate

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

Default: metric — unspecified;

type — 2

Format: `default-information originate [always] [metric` *`0-16777214`*`] [metric-type {1 | 2}]`

Command mode: Router OSPFv3 Config

no default-information originate

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

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

Command mode: Router OSPFv3 Config

default-metric

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

Format: `default-metric` *`1-16777214`*

Command mode: Router OSPFv3 Config

no default-metric

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

Format: `no default-metric`

Command mode: Router OSPFv3 Config

distance ospf

This command sets the route preference value of OSPF route types 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 external routes are assigned the same priority value. The range of *preference* value is 1 to 255.

Default: 110

Format: `distance ospf {intra-area` *`1-255`* `| inter-area` *`1-255`* `| external` *`1-255`*`}`

Command mode: Router OSPFv3 Config

no distance ospf

This command sets the default route preference value of OSPF routes in the router. The type of OSPF route can be intra, inter, or external. All external routes are assigned the same priority value.

Format: `no distance ospf {intra-area | inter-area | external}`

Command mode: Router OSPFv3 Config

enable

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

Default: enabled

Format: `enable`

Command mode: Router OSPFv3 Config

no enable

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

Format: `no enable`

Command mode: Router OSPFv3 Config

exit-overflow-interval

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

Default: 0

Format: `exit-overflow-interval` *`seconds`*

Command mode: Router OSPFv3 Config

no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format: `no exit-overflow-interval`

Command mode: Router OSPFv3 Config

external-lsdb-limit

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

Default: -1

Format: `external-lsdb-limit` *`limit`*

Command mode: Router OSPFv3 Config

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format: `no external-lsdb-limit`
Command mode: Router OSPFv3 Config

maximum-paths

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

Default: 4

Format: `maximum-paths` *`maxpaths`*

Command mode: Router OSPFv3 Config

no maximum-paths

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

Format: `no maximum-paths`

Command mode: Router OSPFv3 Config

passive-interface default

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF shall not form adjacencies over a passive interface.

Default: disabled

Format: `passive-interface default`

Command mode: Router OSPFv3 Config

no passive-interface default

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to nonpassive mode.

Format: `no passive-interface default`

Command mode: Router OSPFv3 Config

passive-interface

Use this command to set the interface or tunnel as passive. The *unit/slot/port* argument 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 *unit/ slot/port* format. It overrides the global passive mode that is currently effective on the interface or tunnel.

Default: disabled

Format: `passive-interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`|tunnel `*`tunnel-id`*`}`

Command mode: Router OSPFv3 Config

no passive-interface

Use this command to set the interface or tunnel as nonpassive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Format: `no passive-interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`|tunnel `*`tunnel-id`*`}`

Command mode: Router OSPFv3 Config

redistribute

This command configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers. If you use the bgp keyword to redistribute BGP routes into OSPFv3, only the external BGP routes are redistributed.

Default: metric — unspecified;

type — 2;

tag — 0.

Format: `redistribute {static | connected | bgp} [metric `*`0-16777214`*`] [metric-type {1 | 2}] [tag `*`0-4294967295`*`]`

Command mode: Router OSPFv3 Config

no redistribute

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

Format: `no redistribute {static | connected}` *`[metric] [metric-type] [tag]`*

Command mode: Router OSPFv3 Config

router-id

This command sets the unique identifier of the OSPF router.

Format: `router-id `*`ipaddress`*

Command mode: Router OSPFv3 Config

timers pacing lsa-group

Use this command to adjust how OSPFv3 groups LSAs for periodic refresh. OSPFv3 refreshes self-originated LSAs approximately once every 30 minutes. When OSPFv3 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 OSPFv3 to combine refreshed LSAs into a minimal number of LS Update packets. Minimizing the number of Update packets makes LSA distribution more efficient.

When OSPFv3 originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPFv3 refreshes the LSA. By selecting a random refresh delay, OSPFv3 avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.

Seconds is the width of the window in which LSAs are refreshed. The range is 10 to 1800 seconds.

Default: 60 seconds

Format: `timers pacing lsa-group` *`seconds`*

Command mode: Privileged

no timers pacing lsa-group

This command returns the LSA Group Pacing parameter to the factory default value of 60 seconds.

Format: `no timers pacing lsa-group`

Command mode: Privileged

timers throttle spf

The initial wait interval is set to an amount of delay specified by the spf-hold value. If an SPF calculation is not scheduled during the current wait interval, the next SPF calculation is scheduled at a delay of *spf-start*. If there has been an SPF calculation scheduled during the current wait interval, the wait interval is set to two times the current wait interval until the wait interval reaches the maximum time in milliseconds as specified in *spf-maximum*. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.

Default: *spf-start* = 2000 ms;
spf-hold = 5000 ms;
spf-maximum = 5000 ms.

Format: `timers throttle spf` *`spf-start spf-hold spf-maximum`*

Command mode: Privileged

Parameter	*Description*
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.

no timers throttle spf

This command returns the SPF throttling parameters to the factory default values.

Format: `no timers throttle spf`

Command mode: Privileged

trapflags

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group's specific trapflags to enable or disable, are listed in the following table.

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 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.

Default: disabled

Format: `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} | re-transmit {all | packets | virt-packets} |state-change {all | if-state-change | neighbor-state-change | virtif-state-change | virtneighbor-state-change}}`

Command mode: Router OSPFv3 Config

no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the group name followed by that particular flag.
- To disable all the flags in that group, give the group name followed by all.
- To disable all the flags, give the command as trapflags all.

Format: `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} | re-transmit {all | packets | virt-packets} |state-change {all | if-state-change | neighbor-state-change | virtif-state- change | virtneighbor-state-change}}`

Command mode: Router OSPFv3 Config

13.5.2 OSPFv3 Interface commands

ipv6 ospf area

This command sets the OSPF area to which the specified router interface or range of interfaces belongs. It also enables OSPF on the specified router interface or range of interfaces. The *area* is a 32-bit integer, formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0-4294967295. The *area* uniquely identifies the area to which the interface connects. Assigning an area ID for an area that does not yet exist, causes the area to be created with default values.

Format: `ipv6 ospf area` *`0-4294967295`*

Command mode: Interface Config

ipv6 ospf cost

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

Default: 10

Format: `ipv6 ospf cost` *`1-65535`*

Command mode: Interface Config

no ipv6 ospf cost

This command configures the default cost on an OSPF interface.

Format: `no ipv6 ospf cost`

Command mode: Interface Config

ipv6 ospf dead-interval

This command sets 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 for *seconds* is from 1 to 2147483647.

Default: 40

Format: `ipv6 ospf dead-interval` *1-2147483647*

Command mode: Interface Config

no ipv6 ospf dead-interval

This command sets the default OSPF dead interval for the specified interface or range of interfaces.

Format: `no ipv6 ospf dead-interval`

Command mode: Interface Config

ipv6 ospf hello-interval

This command sets the OSPF hello interval for the specified interface. 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 for *seconds* range from 1 to 65535.

Default: 10

Format: `ipv6 ospf hello-interval` *seconds*

Command mode: Interface Config

no ipv6 ospf hello-interval

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

Format: `no ipv6 ospf hello-interval`

Command mode: Interface Config

ipv6 ospf link-lsa-suppression

Use this command to enable Link LSA Suppression on an interface. When Link LSA Suppression is enabled on a point-to-point (P2P) interface, no Link LSA protocol packets are originated (transmitted) on the interface. This configuration does not apply to non-P2P interfaces.

Default: False

Format: `ipv6 ospf link-lsa-suppression`

Command mode: Privileged

no ipv6 ospf link-lsa-suppression

This command returns Link LSA Suppression for the interface to disabled. When Link LSA Suppression is disabled, Link LSA protocol packets are originated (transmitted) on the P2P interface.

Format: `no ipv6 ospf link-lsa-suppression`

Command mode: Privileged

ipv6 ospf mtu-ignore

This command 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.

Default: enabled

Format: `ipv6 ospf mtu-ignore`

Command mode: Interface Config

no ipv6 ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format: `no ipv6 ospf mtu-ignore`

Command mode: Interface Config

ipv6 ospf network

This command changes the default OSPF network type for the interface or range of interfaces. Normally, the network type is determined from the physical IP network type. By default all Ethernet networks are OSPF type broadcast. Similarly, tunnel interfaces default to point-to-point. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPF designated router election. It is normally not useful to set a tunnel to OSPF network type broadcast.

Default: broadcast

Format: `ipv6 ospf network {broadcast | point-to-point}`

Command mode: Interface Config

no ipv6 ospf network

This command sets the interface type to the default value.

Format: `no ipv6 ospf network {broadcast | point-to-point}`

Command mode: Interface Config

ipv6 ospf prefix-suppression

This command suppresses the advertisement of the IPv6 prefixes that are associated with an interface, except for those associated with secondary IPv6 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.

Default: prefix suppression is not configured.

Format: `ipv6 ospf prefix-suppression [disable]`

Command mode: Interface Config

no ipv6 ospf prefix-suppression

This command removes prefix-suppression configurations at the interface level. When the no ipv6 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.

Format: `no ipv6 ospf prefix-suppression`

Command mode: Interface Config

ipv6 ospf priority

This command sets the OSPF priority for the specified router interface or range of interfaces. 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.

Default: 1, which is the highest router priority

Format: `ipv6 ospf priority` *`0-255`*

Command mode: Interface Config

no ipv6 ospf priority

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

Format: `no ipv6 ospf priority`

Command mode: Interface Config

ipv6 ospf retransmit-interval

This command sets 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. Range — from 0 to 3600 seconds (1 hour).

Default: 5

Format: `ipv6 ospf retransmit-interval` *`seconds`*

Command mode: Interface Config

no ipv6 ospf retransmit-interval

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

Format: `no ipv6 ospf retransmit-interval`

Command mode: Interface Config

ipv6 ospf transmit-delay

This command sets 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).

Default: 1

Format: `ipv6 ospf transmit-delay` *seconds*

Command mode: Interface Config

no ipv6 ospf transmit-delay

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

Format: `no ipv6 ospf transmit-delay`

Command mode: Interface Config

13.5.3 OSPFv3 Graceful Restart Configuration Commands

The OSPFv3 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 to continues forwarding IPv6 packets using OSPFv3 routes while a backup switch takes over management unit responsibility.

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 OSPFv3 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.

nsf

Use this command to enable the OSPF graceful restart functionality on an interface.

Default: disabled

Format: `nsf [ietf] [planned-only]`

Command mode: Router OSPFv3 Config

Parameter	*Description*
ietf	This keyword is accepted but not required.
planned-only	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).

no nsf

Use this command to disable graceful restart for all restarts.

Format: `no nsf [ietf]`

Command mode: Router OSPFv3 Config

nsf restart-interval

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the initiate failover command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Default: 120 seconds

Format: `nsf [ietf] restart-interval` *`1-1800`*

Command mode: Router OSPFv3 Config

Parameter	*Description*
ietf	This keyword is accepted but not required.
seconds	The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is 1 to 1800 seconds.

no nsfrestart-interval

Use this command to revert the grace period to its default value.

Format: `no [ietf] nsf restart-interval`

Command mode: Router OSPFv3 Config

nsf helper

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default: OSPF may act as a helpful neighbor for both planned and unplanned restarts.

Format: `nsf helper [planned-only]`

Command mode: Router OSPFv3 Config

Parameter	*Description*
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

no nsf helper

Use this command to disable helpful neighbor functionality for OSPF.

Format: `no nsf helper`

Command mode: Router OSPFv3 Config

nsf ietf helper disable

Use this command to disable helpful neighbor functionality for OSPF.

The commands no nsf helper and nsf ietf helper disable are functionally equivalent. The command nsf ietf helper disable is supported solely for compatibility with other network software CLI.

Format: `nsf ietf helper disable`

Command mode: Router OSPFv3 Config

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.

Default: enabled.

Format: `nsf [ietf] helper strict-lsa-checking`

Command mode: Router OSPFv3 Config

Parameter	*Description*
ietf	This keyword is accepted but not required.

no nsf [ietf] helper strict-lsa-checking

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default: enabled.

Format: `nsf [ietf] helper strict-lsa-checking`

Command mode: Router OSPFv3 Config

Parameter	*Description*
external-lsa	(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	(Optional) Sends the maximum metric values for Inter-Area-Router LSAs.
on-startup	(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	(Optional) Sends the maximum metric values for Summary LSAs.

no max-metric router-lsa

Use this command in OSPFv3 Router Configuration mode to disable stub router mode. The command clears either type of stub router mode (always or on-startup) and resets all LSA options. 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** with the external-lsa, inter-area-lsas, or summary-lsa option **router-lsa summary-lsa** causes OSPF to send summary LSAs with metrics computed using normal procedures.

Format: `no max-metric router-lsa [external-lsa] [inter-area-lsas] [on-startup] [summary-lsa]`

Command mode: Router OSPFv3 Config

clear ipv6 ospf stub-router

Use this command to force OSPF to exit stub router mode 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. This command has no effect if OSPF is configured to be in stub router mode permanently.

Format: `clear ipv6 ospf stub-router`

Command mode: Privileged

13.5.4 OSPFv3 show commands

show ipv6 ospf

This command displays information relevant to the OSPF router.

Format: `show ipv6 ospf`

Command mode: Privileged

User

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

Term	*Value*
Router ID	An unique identifier of the router in the network.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.

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.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
Default Metric	Default value for redistributed routes.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not.
Always	Shows whether default routes are always advertised.
Metric	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.
Number of Active Areas	The 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	Shows if the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router.
Stub Router Status	The status of the stub router: Active or Inactive.
Stub Router Reason	This is displayed only if the stub router is active. Shows the reason for the stub router: Configured, Startup or Resource Limitation
Stub Router Startup Time Remaining	This is displayed only if the stub router is in startup stub router mode. The remaining time, in seconds, until OSPF exits stub router mode.
Stub Router Duration	This row is only listed if the stub router is active and the router entered stub mode because of a resource limitation. The time elapsed since the router last entered the stub router mode. The duration is displayed in DD:HH:MM:SS format.
External LSDB Overflow	When the number of non-default 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 non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link- state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
Retransmit List Entries	The 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	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
Retransmit Entries High Water Mark	The highest number of LSAs that have been waiting for acknowledgment.
Redistributing	This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.
Source	Shows source protocol/routes that are being redistributed. Possible values are: static, connected, BGP or RIP.
Metric	The metric of the routes being redistributed.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Tag	The decimal value attached to each external route.
Subnets	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
Distribute-List	The access list used to filter redistributed routes.
Prefix-suppression	Displays whether prefix-suppression is enabled or disabled on the given interface.
NSF Support	Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (Always).
NSF Restart Interval	The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful

	restart.
NSF Restart Status	The current graceful restart status of the router.
NSF Restart Age	Number of seconds until the graceful restart grace period expires.
NSF Restart Exit Reason	Indicates why the router last exited the last 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.
NSF Help 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.

show ipv6 ospf abr

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR). This command takes no options.

Format: `show ipv6 ospf abr`

Command mode: Privileged

User

Term	*Value*
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.

show ipv6 ospf area

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

Format: `show ipv6 ospf area areaid`

Command mode: Privileged

User

Term	*Value*
AreaId	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	The 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. 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.

Term	*Value*
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.

show ipv6 ospf asbr

This command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routers (ASBR). This command takes no options. This command takes no options.

Format: `show ipv6 ospf asbr`

Command mode: Privileged

User

Term	*Value*
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.

show ipv6 ospf database

This command displays information about the link state database when OSPFv3 is enabled. 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 other optional parameters to specify the type of link state advertisements to display. Use *external* to display the external LSAs. Use *inter-area* to display the inter-area LSAs. Use *link* to display the link LSAs. Use *network* to display the network LSAs. Use nssa-external to display NSSA external LSAs. Use *prefix* to display intra-area Prefix LSAs. Use *router* to display router LSAs. Use *unknown area, unknown as*, or *unknown link* to display unknown area, AS or link-scope LSAs, respectively. Use *lsid* to specify the link state ID (LSID). Use *adv-router* to show the LSAs that are restricted by the advertising router. Use *self-originate* to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled.

Format: `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}]`

Command mode: Privileged

User

For each link-type and area, the following information is displayed:

Term	*Value*
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 an IP address 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.

show ipv6 ospf database database-summary

Use this command to display the number of each type of LSA in the database and the total number of LSAs in the database.

Format: `show ipv6 ospf database database-summary`

Command mode: Privileged
User

Term	*Value*
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	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.

show ipv6 ospf interface

This command displays the information for the IFO object or virtual interface tables. The *unit/slot/port* argument 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 *unit/ slot/port* format.

Format: `show ipv6 ospf interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`|loopback `*`loopback-id`*` | tunnel `*`tunnel-id`*`}`

Command mode: Privileged

User

Term	*Value*
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 acknowledgment 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 information only displays if OSPF is initialized on the interface:

Term	*Value*
OSPF Interface Type	OSPF interface type will be broadcast or ptp.
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.

show ipv6 ospf interface brief

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

Format: `show ipv6 ospf interface brief`

Command mode: Privileged

User

Term	*Value*
Interface	The interface in *unit/slot/port* format.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The area id of this OSPF 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. 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 acknowledgment after receiving an LSA.

show ipv6 ospf interface stats

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

Format: `show ipv6 ospf interface stats {`*`unit/slot/port`* `|` `vlan` *`id`*`}`

Command mode: Privileged

User

Term	*Value*
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 LSA 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 nonbackbone 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	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 packet's 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.

show ipv6 ospf lsa-group

This command displays the number of self-originated LSAs within each LSA group.

Format: `show ipv6 ospf lsa-group`

Command mode: Privileged

User

show ipv6 ospf max-metric

This command displays the configured maximum metrics for stub-router mode.

Format: `show ipv6 ospf max-metric`

Command mode: Privileged

User

show ipv6 ospf neighbor

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays. The *unit/slot/port* argument 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 *unit/ slot/port* format. The *ip-address* is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Format: `show ipv6 ospf neighbor [interface {`*unit/slot/port*`|vlan` *1-4093*`|tunnel` *tunnel_id*`}[`*ip- address*`]`

Command mode: Privileged

User

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

Term	*Value*
Router ID	The input neighbor Router ID.
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	Local router interface in *unit/slot/port* format.
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. • **Init** — An Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet

	been established. • **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. • **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 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** — 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:

Term	*Value*
Interface	Local router interface in *unit/slot/port* format.
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	The 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.

show ipv6 ospf range

This command displays the set of OSPFv3 area ranges configured for a given area.

Format: `show ipv6 ospf range` *`areaid`*

Command mode: Privileged

Term	*Value*
Area ID	The area whose prefixes are summarized.
IPv6 Prefix/Prefix Length	The summary prefix and prefix length.
Type	**S** (Summary Link) or **E** (External Link)
Action	**Enabled** or **Disabled**
Cost	Metric to be advertised when the range is active.

show ipv6 ospf statistics

This command displays information about the 15 most recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation.

Format: `show ipv6 ospf statistics`

Command mode: Privileged

User

The command displays the following information with the most recent statistics displayed at the end of the table.

Term	*Value*
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 the 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

show ipv6 ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format: `show ipv6 ospf stub table`

Command mode: Privileged

User

Term	*Value*
Area ID	A 32-bit identifier for the created stub area.
Type of Service	The 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.

show ipv6 ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The areaid parameter identifies the area and the neighbor parameter identifies the neighbor's Router ID.

Format: `show ipv6 ospf virtual-link` *`areaid neighbor`*

Command mode: Privileged

User

Term	*Value*
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.

show ipv6 ospf virtual-link brief

This command displays the OSPFV3 Virtual Interface information for all areas in the system.

Format: `show ipv6 ospf virtual-link brief`

Command mode: Privileged

User

Term	*Value*
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.

13.6 DHCPv6 configuration commands

This section describes the commands you use to configure the DHCPv6 server on the system and to view DHCPv6 information.

service dhcpv6

This command enables DHCPv6 configuration on the router.

Default: enabled

Format: `service dhcpv6`

Command mode: Global Config

no service dhcpv6

This command disables DHCPv6 configuration on router.

Format: `no service dhcpv6`

Command mode: Global Config

ipv6 dhcp client pd

Use this command to enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process (if the process is not currently running) and to enable requests for prefix delegation through a specified interface. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the automatic argument.

The Prefix Delegation client is supported on only one IP interface.

rapid-commit enables the use of a two-message exchange method for prefix delegation and other configuration. If enabled, the client includes the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. If one of these functions is already enabled and a user tries to configure a different function on the same interface, a message is displayed.

Default: Disabled

Format: `ipv6 dhcp client pd [rapid-commit]`

Command mode: Interface Config

no ipv6 dhcp client pd

This command disables requests for prefix delegation.

Format: `no ipv6 dhcp client pd`

Command mode: Interface Config

ipv6 dhcp server

Use this command to configure DHCPv6 server functionality on an interface or range of interfaces. The pool-name is the DHCPv6 pool containing stateless and/or prefix delegation parameters, automatic enables the server to automatically determine which pool to use when allocating addresses for a client, rapid-commit is an option that allows for an abbreviated exchange between the client and server, and pref-value is a value used by clients to determine preference between multiple DHCPv6 servers. For a particular interface, DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

Format: `ipv6 dhcp server {`*`pool-name`*` | automatic}[rapid-commit] [preference `*`pref-value`*`]`

Command mode: Interface Config

ipv6 dhcp relay destination

Use this command to configure an interface for DHCPv6 relay functionality on an interface or range of interfaces. Use the destination keyword to set the relay server IPv6 address. The relay-address parameter is an IPv6 address of a DHCPv6 relay server. Use the interface keyword to set the relay server interface. The relay- interface parameter is an interface (unit/slot/port) to reach a relay server. The optional remote-id is the Relay Agent Information Option “remote ID” suboption to be added to relayed messages. This can either be the special keyword duid-ifid, which causes the “remote ID” to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

If *relay-address* is an IPv6 global address, then *relay-interface* is not required. If *relay-address* is a link-local or multicast address, then *relay-interface* is required. Finally, if you do not specify a value for *relay-address*, then you must specify a value for *relay-interface* and the DHCPV6-ALL-AGENTS multicast address (i.e. FF02::1:2) is used to relay DHCPv6 messages to the relay server.

Format: `ipv6 dhcp relay {destination [relay-address] interface [relay-interface]| interface [relay-interface]} [remote-id (duid-ifid | user-defined-string)]`

Command mode: Interface Config

ipv6 dhcp pool

Use this command from Global Config mode to enter IPv6 DHCP Pool Config mode. The pool-name should be less than 30 alpha-numeric characters. DHCPv6 pools are used to specify information for DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

Once the DHCP for IPv6 configuration information pool has been created, use the ipv6 dhcp server command to associate the pool with a server on an interface. If you do not configure an information pool, use the ipv6 dhcp server interface configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface. Not using any IPv6 address prefix means that the pool returns only configured options.

Format: `ipv6 dhcp pool pool-name`

Command mode: Global Config

no ipv6 dhcp pool

This command removes the specified DHCPv6 pool.

Format: `no ipv6 dhcp pool pool-name`

Command mode: Global Config

address prefix (IPv6)

Use this command to sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.

If lifetime values are not configured, the default lifetime values for valid-lifetime and preferred-lifetime are considered to be infinite.

Format: `address prefix ipv6-prefix [lifetime {valid-lifetime preferred-lifetime | infinite}]`

Command mode: IPv6 DHCP Pool Config

Term	*Value*
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.

domain-name (IPv6)

This command sets the DNS domain name which is provided to DHCPv6 client by DHCPv6 server. Domain name consist of no more than 31 alpha-numeric characters. DHCPv6 pool can have multiple number of domain names with maximum of 8.

Format: `domain-name` *`dns-domain-name`*

Command mode: IPv6 DHCP Pool Config

no domain-name

This command will remove dhcpv6 domain name from dhcpv6 pool.

Format: `no domain-name` *`dns-domain-name`*

Command mode: IPv6 DHCP Pool Config

dns-server (IPv6)

This command sets the ipv6 DNS server address which is provided to dhcpv6 client by dhcpv6 server. DHCPv6 pool can have multiple number of domain names with maximum of 8.

Format: `dns-server` *`dns-server-address`*

Command mode: IPv6 DHCP Pool Config

no dns-server

This command will remove DNS server address from DHCPv6 server.

Format: `no dns-server` *`dns-server-address`*

Command mode: IPv6 DHCP Pool Config

prefix-delegation (IPv6)

Multiple IPv6 prefixes can be defined within a pool for distributing to specific DHCPv6 Prefix delegation clients. Prefix is the delegated IPv6 prefix. DUID is the client's unique DUID value (Example: 00:01:00:09:f8:79:4e:00:04:76:73:43:76'). Name is 31 characters textual client’s name which is useful for logging or tracing only. Valid lifetime is the valid lifetime for the delegated prefix in seconds and preferred lifetime is the preferred lifetime for the delegated prefix in seconds.

Default: valid-lifetime — 2 592 000;

preferred-lifetime — 604 800.

Format: `prefix-delegation` *`prefix/prefixLength DUID`* `[name` *`hostname`*`][valid-lifetime` *`04294967295`*`][preferred-lifetime` *`0-4294967295`*`]`

Command mode: IPv6 DHCP Pool Config

no prefix-delegation

This command deletes a specific prefix-delegation client.

Format: `no prefix-delegation` *`prefix/prefix-delegation DUID`*

Command mode: IPv6 DHCP Pool Config

show ipv6 dhcp

This command displays the DHCPv6 server name and status.

Format: `show ipv6 dhcp`

Command mode: Privileged

Term	*Value*
DHCPv6 is Enabled (Disabled)	The status of the DHCPv6 server.
Server DUID	If configured, shows the DHCPv6 unique identifier.

show ipv6 dhcp statistics

This command displays the IPv6 DHCP statistics for all interfaces.

Format: `show ipv6 dhcp statistics`

Command mode: Privileged

Term	*Value*
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 DHCPv6 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.

show ipv6 dhcp interface

This command displays DHCPv6 information for all relevant interfaces or the specified interface. The *unit/slot/port* argument 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 *unit/ slot/port* format. If you specify an interface, you can use the optional statistics parameter to view statistics for the specified interface.

Format: `show ipv6 dhcp interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`} [statistics]`

Command mode: Privileged

Term	*Value*
IPv6 Interface	Interface name in *unit/slot/port* format.
Mode	Shows whether the interface is a IPv6 DHCP relay or server.

If the interface mode is server, the following information displays.

Term	*Value*
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.

If the interface mode is relay, the following information displays.

Term	*Value*
Relay Address	The IPv6 address of the relay server.
Relay Interface Number	The relay server interface in *unit/slot/port* format.
Relay Remote ID	If configured, shows the name of the relay remote.
Option Flags	Shows whether rapid commit is configured.

If you use the statistics parameter, the command displays the IPv6 DHCP statistics for the specified interface. See the show ipv6 dhcp statistics command for information about the output.

show ipv6 dhcp binding

This command displays configured DHCP pool.

Format: `show ipv6 dhcp binding `*`[ipv6-address]`*

Command mode: Privileged

Term	*Value*
DHCP Client Address	Address of DHCP Client.
DUID	String that represents the Client DUID.
IAID	Identity Association identifier.
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Prefix Type	IPV6 prefix type (IPAD, IANA or IATA).
Client Address	Address of DHCP Client.
Client Interface	IPv6 Address of DHCP Client.
Expiration	Address of DNS server.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.

show ipv6 dhcp pool

This command displays configured DHCP pool.

Format: `show ipv6 dhcp pool` *`pool-name`*

Command mode: Privileged

Term	*Value*
DHCP Pool Name	Unique pool name configuration.
Client DUID	Client's DHCP unique identifier. 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.
Domain Name	DNS domain name.

show network ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the network management interface.

Format: `show network ipv6 dhcp statistics`

Command mode: Privileged

User

Field	*Description*
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.
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.

show serviceport ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the serviceport management interface.

Format: `show serviceport ipv6 dhcp statistics`

Command mode: Privileged

User

Field	*Description*
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.

DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.
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.

clear ipv6 dhcp

Use this command to clear DHCPv6 statistics for all interfaces or for a specific interface. Use the unit/slot/port parameter to specify an interface and the vlan parameter to specify a VLAN.

Format: `clear ipv6 dhcp {statistics | interface {`*`unit/slot/port`*` | vlan `*`id`*`}}`

Command mode: Privileged

clear ipv6 dhcp binding

This command deletes an automatic address binding from the DHCP server database. address is a valid IPv6 address.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool;
- Updated when the client renews, rebinds, or confirms the prefix delegation;
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid life-times have expired, or an administrator runs the **clear ipv6 dhcp binding** command.

If the clear ipv6 dhcp binding command is used with the optional ipv6-address argument specified, only the binding for the specified client is deleted. If the clear ipv6 dhcp binding command is used without the ipv6- address argument, all automatic client bindings are deleted from the DHCP for IPv6 binding table.

Format: `clear ipv6 dhcp binding [`*`ipv6-address`*`]`

Command mode: Privileged

clear network ipv6 dhcp statistics

Use this command to clear the DHCPv6 statistics on the network management interface.

Format: `clear network ipv6 dhcp statistics`

Command mode: Privileged

clear serviceport ipv6 dhcp statistics

Use this command to clear the DHCPv6 client statistics on the service port interface.

Format: `clear serviceport ipv6 dhcp statistics`

Command mode: Privileged

13.7 DHCPv6 Snooping configuration commands

This section describes commands you use to configure IPv6 DHCP Snooping.

ipv6 dhcp snooping

Use this command to globally enable IPv6 DHCP Snooping.

Default: disabled

Format: `ipv6 dhcp snooping`

Command mode: Global Config

no ipv6 dhcp snooping

Use this command to globally disable IPv6 DHCP Snooping.

Format: `no ipv6 dhcp snooping`

Command mode: Global Config

ipv6 dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default: disabled

Format: `ipv6 dhcp snooping vlan` *`vlan-list`*

Command mode: Global Config

no ipv6 dhcp snooping vlan

Use this command to disable DHCP snooping on the specified VLANs.

Format: `no ipv6 dhcp snooping vlan` *`vlan-list`*

Command mode: Global Config

ipv6 dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default: enabled

Format: `ipv6 dhcp snooping verify mac-address`

Command mode: Global Config

no ipv6 dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format: `no ipv6 dhcp snooping verify mac-address`

Command mode: Global Config

ipv6 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.

Default: local

Format: `ipv6 dhcp snooping database {local|tftp://hostIP/filename}`

Command mode: Global Config

ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database is persisted. The interval value ranges from 15 to 86400 seconds.

Default: 300 seconds

Format: `ip dhcp snooping database write-delay` *`in seconds`*

Command mode: Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format: `no ip dhcp snooping database write-delay`

Command mode: Global Config

ipv6 dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format: `ipv6 dhcp snooping binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Command mode: Global Config

no ipv6 dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format: `no ipv6 dhcp snooping binding` *`mac-address`*

Command mode: Global Config

ipv6 dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default: disabled

Format: `ipv6 dhcp snooping trust`

Command mode: Interface Config

no ipv6 dhcp snooping trust

Use this command to configure the port as untrusted.

Format: `no ipv6 dhcp snooping trust`

Command mode: Interface Config

ipv6 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.

Default: disabled

Format: `ipv6 dhcp snooping log-invalid`

Command mode: Interface Config

no ipv6 dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format: `no ipv6 dhcp snooping log-invalid`

Command mode: Interface Config

ipv6 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. Rate limiting is configured on a physical port and may be applied to trusted and untrusted ports.

Default: disabled (no limit)

Format: `ipv6 dhcp snooping limit {rate pps [burst interval seconds]}`

Command mode: Interface Config

no ipv6 dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format: `no ipv6 dhcp snooping limit`

Command mode: Interface Config

ipv6 verify source

Use this command to configure the IPv6SG 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 is filtered based on the IP and MAC addresses. This command can be used to configure a single interface or a range of interfaces.

Default: Disabled

Format: `ipv6 verify source {port-security}`

Command mode: Interface Config

no ipv6 verify source

Use this command to disable the IPv6SG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format: `no ipv6 verify source`

Command mode: Interface Config

ipv6 verify binding

Use this command to configure static IPv6 source guard (IPv6SG) entries.

Format: `ipv6 verify binding` *`mac-address`* `vlan` *`vlan id ipv6 address`* `interface` *`interface id`*

Command mode: Global Config

no ipv6 verify binding

Use this command to remove the IPv6SG static entry from the IPv6SG database.

Format: `no ipv6 verify binding` *`mac-address`* `vlan` *`vlan id ipv6 address`* `interface` *`interface id`*

Command mode: Global Config

show ipv6 dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format: `show ipv6 dhcp snooping`

Command mode: Privileged

User

Term	*Value*
Interface	Interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

show ipv6 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.

Format: `show ipv6 dhcp snooping binding [{static/dynamic}] [interface` *`unit/slot/port`*`] [vlan id]`

Command mode: Privileged

User

Term	*Value*
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 (sec)	The remaining lease time for the entry.

show ipv6 dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistence.

Format: `show ipv6 dhcp snooping database`

Command mode: Privileged

User

Term	*Value*
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Format: `show ipv6 dhcp snooping interfaces [interface` *`unit/slot/port`*`]`

Command mode: Privileged

show ipv6 dhcp snooping statistics

Use this command to list statistics for IPv6 DHCP Snooping security violations on untrusted ports.

Format: `show ipv6 dhcp snooping statistics`

Command mode: Privileged

User

Term	*Value*
Interface	Interface IPv6 address in *unit/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 HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

clear ipv6 dhcp snooping binding

Use this command to clear all DHCPv6 Snooping bindings on all interfaces or on a specific interface.

Format: `clear ipv6 dhcp snooping binding [interface unit/slot/port]`

Command mode: Privileged

User

clear ipv6 dhcp snooping statistics

Use this command to clear all DHCPv6 Snooping statistics.

Format: `clear ipv6 dhcp snooping statistics`

Command mode: Privileged

User

show ipv6 verify

Use this command to display the IPv6 configuration on a specified unit/slot/port.

Format: `show ipv6 verify interface`

Command mode: Privileged

User

Term	*Value*
Interface	IP address of the interface in unit/slot/port format.
Filter Type	Is one of two values: • ip-v6mac: User has configured MAC address filtering on this interface. • ipv6: Only IPv6 address filtering on this interface.

show ipv6 verify source

Use this command to display the IPv6SG configurations on all ports. If the interface option is specified, the output is restricted to the specified unit/slot/port.

Format: `show ipv6 verify source {interface}`

Command mode: Privileged

User

Term	*Value*
Interface	The IP address of the interface in *unit/slot/port* format.
Filter Type	Is one of two values: • ip-v6mac: User has configured MAC address filtering on this interface. • ipv6: Only IPv6 address filtering on this interface.
IPv6 Address	The 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.

show ipv6 source binding

Use this command to display the IPv6SG bindings.

Format: `show ipv6 source binding [{dhcp-snooping|static}] [interface` *`unit/slot/port`*`] [vlan id]`

Command mode: Privileged

User

Term	***Value***
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	The IP address of the interface in *unit/slot/port* format.

14 QUALITY OF SERVICE CONFIGURATION COMMANDS

This chapter describes the Quality of Service (QoS) commands available in the CLI.

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.**

14.1 CoS (Class of Service) management 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.

- **Commands you issue in the Interface Config mode only affect a single interface.**
- **Commands you issue in the Global Config mode affect all interfaces.**

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The userpriority values can range from 0 to 7. The trafficclass values range from 0-6.

Format: `classofservice dot1p-mapping userpriority trafficclass`

Command mode: Global Config
Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format: `no classofservice dot1p-mapping`

Command mode: Global Config
Interface Config

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 range from 0-6.

Format: `classofservice ip-dscp-mapping ipdscp trafficclass`

Command mode: Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format: `no classofservice ip-dscp-mapping`

Command mode: Global Config

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 (802.1p), 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.

Default: dot1p

Format: `classofservice trust {dot1p | ip-dscp | untrusted}`

Command mode: Global Config
Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format: `no classofservice trust`

Command mode: Global Config
Interface Config

cos-queue max-bandwidth

This command specifies the maximum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no maximum bandwidth. The sum of all values entered must not exceed 100.

Format: `cos-queue max-bandwidth bw-0 bw-1 … bw-n`

Command mode: Global Config
Interface Config

no cos-queue max-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format: `no cos-queue max-bandwidth`

Command mode: Global Config
Interface Config

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. A value from 0-100 (percentage of link rate) must

be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format: `cos-queue min-bandwidth bw-0 bw-1 … bw-n`

Command mode: Global Config
Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format: `no cos-queue min-bandwidth`

Command mode: Global Config
Interface Config

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.

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).

Format: `cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]`

Command mode: Global Config
Interface Config

no cos-queue random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Format: `no cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]`

Command mode: Global Config
Interface Config

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.

Format: `cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]`

Command mode: Global Config
Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format: `no cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]`

Command mode: Global Config
Interface Config

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.

When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

Format: `random-detect`

Command mode: Global Config
Interface Config

no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

Format: `no random-detect`

Command mode: Global Config
Interface Config

random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

Format: `random-detect exponential-weighting-constant 0-15`

Command mode: Global Config
Interface Config

no random-detect exponential-weighting-constant

Use this command to set the WRED decay exponent back to the default.

Format: `no random-detect exponential-weighting-constant`

Command mode: Global Config
Interface Config

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).

Format: `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`

Command mode: Global Config
Interface Config

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.

Term	*Value*
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).

no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format: `no random-detect queue-parms queue-id-1 [queue-id-2 … queue-id-n]`

Command mode: Global Config
Interface Config

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. The bandwidth values are from 0-100 in increments of 1. 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 temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format: `traffic-shape bw`

Command mode: Global Config
Interface Config

no traffic-shape

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

Format: `no traffic-shape`

Command mode: Global Config
Interface Config

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. If unit/slot/port parameter is specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format: `show classofservice dot1p-mapping [unit/slot/port]`

Command mode: Privileged

Term	*Value*
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format: `show classofservice ip-dscp-mapping`

Command mode: Privileged

The following information is repeated for each user priority.

Term	*Value*
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

show classofservice trust

This command displays the current trust mode setting for a specific interface. If you specify an unit/slot/port 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.

Format: `show classofservice trust [unit/slot/port]`

Command mode: Privileged

Term	*Value*
Class of Service Trust Mode	The the trust mode, which is either Dot1P, IP DSCP, or Untrusted.
Non-IP Traffic Class	(IP DSCP mode only) The traffic class used for non-IP traffic.
Untrusted Traffic Class	(Untrusted mode only) The traffic class used for all untrusted traffic.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. If the unit/slot/port parameter is specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format: `show interfaces cos-queue [unit/slot/port]`

Command mode: Privileged

Term	*Value*
Interface Shaping Rate	The global interface shaping rate value.
WRED Decay Exponent	The global WRED decay exponent value.
Queue Id	An interface supports 7 queues numbered 0 to 6.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort.
Maximum Bandwidth	The maximum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort.
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.

Term	*Value*
Interface	The unit/slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface.
WRED Decay Exponent	The configured WRED decay exponent for a CoS queue interface.

show interfaces random-detect

This command displays the global WRED settings for each CoS queue. If you specify the unit/slot/port, the command displays the WRED settings for each CoS queue on the specified interface.

Format: `show interfaces random-detect [unit/slot/port]`

Command mode: Privileged

Term	*Value*
Queue Id	An interface supports 7 queues numbered 0 to 6.
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).

show interfaces tail-drop-threshold

This command displays the tail drop threshold information. If you specify the unit/slot/port, the command displays the tail drop threshold information for the specified interface.

Format: `show interfaces tail-drop-threshold [unit/slot/port]`

Command mode: Privileged

14.2 Differentiated Services configuration commands

This section describes the commands you use to configure QoS Differentiated Services (DiffServ). You configure DiffServ in several stages by specifying three DiffServ components:

1 Class

- Creating and deleting calsses.
- Defining match critetria for a class.

2 Policy

- Creating and deleting policies.
- Associating calsses with a policy.
- Defining policy statements for a policy/class combination.

3 Service

- Adding and removing a policy to/from an inbound interface.

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class.
- Class definitions do not support hierarchical service policies.

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

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.

diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format: `diffserv`

Command mode: Global Config

no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format: `no diffserv`

Command mode: Global Config

14.3 DiffServ Class configuration 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.

Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is `class-map`.

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.

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.

The optional keywords [{ipv4 | ipv6}] specify the Layer 3 protocol for this class. If not specified, this parameter defaults to ipv4.

The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the [{ipv4 | ipv6}] keyword specified.

Format: `class-map match-all class-map-name [{ipv4 | IPv6}]{}`

Command mode: Global Config

no class-map

This command eliminates an existing DiffServ class. The class-map-name is the name of an existing DiffServ class. (The class name default is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format: `no class-map class-map-name`

Command mode: Global Config

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.

Default: none

Format: `class-map rename class-map-name new-class-map-name`

Command mode: Global Config

match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The ethertype value is specified as one of the following keywords: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp or as a custom EtherType value in the range of 0x0600- 0xFFFF. Use the [not] option to negate the match condition.

Format: `match [not] ethertype {keyword | custom 0x0600-0xFFFF}`

Command mode: Class-Map Config
IPv6-Class-Map Config

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.

Default: none

Format: `match [not] any`

Command mode: Class-Map Config
IPv6-Class-Map Config

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.

Default: none

Format: `match class-map refclassname`

Command mode: Class-Map Config
IPv6-Class-Map Config

- **The parameters refclassname and class-map-name can not be the same.**
- **Only one other class may be referenced by a class.**
- **Any attempts to delete the refclassname class while the class is still referenced by any class- map-name fails.**
- **The combined match criteria of class-map-name and refclassname must be an allowed combination based on the class type.**
- **Any subsequent changes to the refclassname class match criteria must maintain this validity, or the change attempt fails.**
- **The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.**

no match class-map

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

Format: `no match class-map refclassname`

Command mode: Class-Map Config
IPv6-Class-Map Config

match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the [not] option to negate the match condition.

Default: none

Format: `match [not] cos 0-7`

Command mode: Class-Map Config
IPv6-Class-Map Config

match secondary-cos

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the [not] option to negate the match condition.

Default: none

Format: `match [not]secondary-cos 0-7`

Command mode: Class-Map Config
IPv6-Class-Map Config

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.

Default: none

Format: `match [not] destination-address mac macaddr macmask`

Command mode: Class-Map Config
IPv6-Class-Map Config

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.

Default: none

Format: `match [not] dstip ipaddr ipmask`

Command mode: Class-Map Config

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.

Default: none

Format: `match [not] dstip6 destination-IPv6-prefix/prefix-length`

Command mode: IPv6-Class-Map Config

match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for portkey is one of the supported port name keywords. The currently supported portkey values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [not] option to negate the match condition.

Default: none

Format: `match [not] dstl4port {portkey | 0-65535}`

Command mode: Class-Map Config
IPv6-Class-Map Config

match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The dscpval value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef. Use the [not] option to negate the match condition.

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.

Default: none

Format: `match [not] ip dscp dscpval`

Command mode: Class-Map Config
IPv6-Class-Map Config

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.

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.

Default: none

Format: `match [not] ip precedence 0-7`

Command mode: Class-Map Config

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.

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.

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.

Default: none

Format: `match [not] ip tos tosbits tosmask`

Command mode: Class-Map Config

match ip6flowlbl

Use this command to enter an IPv6 flow label value. Use the [not] option to negate the match condition.

Default: none

Format: `match [not] ip6flowlbl label 0-1048575`

Command mode: IPv6-Class-Map Config

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.

This command does not validate the protocol number value against the current list defined by IANA.

Default: none

Format: `match [not] protocol {protocol-name | 0-255}`

Command mode: Class-Map Config

IPv6-Class-Map Config

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 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.

Default: none

Format: `match [not] source-address mac address macmask`

Command mode: Class-Map Config

IPv6-Class-Map Config

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.

Default: none

Format: `match [not] srcip ipaddr ipmask`

Command mode: Class-Map Config

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.

Default: none

Format: `match [not] srcip6 source-IPv6-prefix/prefix-length`

Command mode: IPv6-Class-Map Config

match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for portkey is one of the supported port name keywords (listed below). The currently supported portkey values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [not] option to negate the match condition.

Default: none

Format: `match [not] srcl4port {portkey | 0-65535}`

Command mode: Class-Map Config
IPv6-Class-Map Config

match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 0 to 4093. Use the [not] option to negate the match condition.

Default: none

Format: `match [not] vlan 0-4093`

Command mode: Class-Map Config
IPv6-Class-Map Config

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 4093. Use the [not] option to negate the match condition.

This command is not available on the 5630x platform.

Default: none

Format: `match [not] secondary-vlan 0-4093`

Command mode: Class-Map Config
IPv6-Class-Map Config

14.4 DiffServ Policy configuration 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.

The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policyattribute can be changed without removing the class instance.

The CLI command root is `policy-map`.

assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The queueid parameter is an integer from 0 to 6.

Format: `assign-queue queueid`

Command mode: Policy-Class-Map Config

Incompatible commands: Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format: `drop`

Command mode: Policy-Class-Map Config

Incompatible commands: Assign Queue, Mark (all forms), Mirror, Police, Redirect

mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Format: `mirror unit/slot/port`

Command mode: Policy-Class-Map Config

Incompatible commands: Drop, Redirect

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).

Format: `redirect unit/slot/port`

Command mode: Policy-Class-Map Config

Incompatible commands: Drop, Mirror

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.

This command may only be used after specifying a police command for the policy-class instance.

Format: `conform-color class-map-name`
Command mode: Policy-Class-Map Config

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.

This command causes the specified policy to create a reference to the class definition.

Format: `class classname`

Command mode: Policy-Map configuration

no class

This command deletes the instance of a particular class and its defined treatment from the specified policy.

The *classname* is the name of an existing DiffServ class.

This command removes the reference to the class definition for the specified policy.

Format: `no class classname`

Command mode: Policy-Map configuration

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.

Default: 1

Format: `mark-cos 0-7`

Command mode: Policy-Class-Map Config

Incompatible commands: Drop, Mark IP DSCP, IP Precedence, Police

mark secondary-cos

This command marks the outer VLAN tags in the packets for the associated traffic stream as secondary CoS.

Default: 1

Format: `mark secondary-cos 0-7`

Command mode: Policy-Class-Map Config

Incompatible commands: Drop, Mark IP DSCP, IP Precedence, Police

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.

Format: `mark-cos-as-sec-cos`

Command mode: Policy-Class-Map Config

Incompatible commands: Drop, Mark IP DSCP, IP Precedence, Police

mark ip-dscp

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

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

Format: `mark ip-dscp` *`dscpval`*

Command mode: Policy-Class-Map Config

Incompatible commands: Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

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

This command may not be used on IPv6 classes. IPv6 does not have a precedence field.

Format: `mark ip-precedence 0-7`

Command mode: Policy-Class-Map Config

Incompatible commands: Drop, Mark IP DSCP, IP Precedence, Police

Policy Type: In

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 (the 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).

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.

Format: `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}]}`

Command mode: Policy-Class-Map Config

Incompatible commands: Drop, Mark (all forms)

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.

Format: `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 | 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-transmit| set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set- dscp-transmit 0-63 | transmit}]}`

Command mode: Policy-Class-Map Config

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.

Format: `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 | 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}]}`

Command mode: Policy-Class-Map Config

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, or the outbound traffic direction as indicated by the *out* parameter, respectively.

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

Format: `policy-map *policyname* {in|out}`

Command mode: Global Config

no policy-map

This command eliminates an existing DiffServ policy. The *policyname* parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format: `no policy-map *policyname*`

Command mode: Global Config

policy-map rename

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

Format: `policy-map rename *policyname newpolicyname*`

Command mode: Global Config

14.5 DiffServ Service configuration 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.

This set of commands consists of service addition/removal. The CLI command root is service-policy.

service-policy

This command attaches a policy to an interface in the inbound direction as indicated by the *in* parameter, or the outbound direction as indicated by the *out* parameter, respectively. The *policyname* parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

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.

Format: `service-policy {in|out} policymapname`

Command mode: Global Config
Interface Config

no service-policy

This command detaches a policy from an interface in the inbound direction as indicated by the *in* parameter, or the outbound direction as indicated by the *out* parameter, respectively. The *policyname* parameter is the name of an existing DiffServ policy.

This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction or an interface in the outbound direction.

There is no separate interface administrative 'mode' command for DiffServ.

Format: `no service-policy {in|out} policymapname`

Command mode: Global Config
Interface Config

14.6 DiffServ show commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

show class-map

This command displays all configuration information for the specified class. The *class-name* is the name of an existing DiffServ class.

Format: `show class-map` *`class-name`*

Command mode: Privileged
User

If the class-name is specified the following fields are displayed:

Term	*Value*
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.
Class Layer3 Protocol	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. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. Possible Match Criteria fields: Destination IP Address, Destination Layer 4 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 и 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:

Term	*Value*
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.

show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format: `show diffserv`

Command mode: Privileged

Term	*Value*
DiffServ Admin Mode	The current value of the DiffServ administrative mode.
Class Table Size Current/Max	The current and maximum number of entries (rows) in the Class Table.
Class Rule Table Size Current/Max	The current and maximum number of entries (rows) in the Class Rule Table.

Policy Table Size Current/Max	The current and maximum number of entries (rows) in the PolicyTable.
Policy Instance Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Instance Table.
Policy Attribute Table Size Current/Max	The current and maximum number of entries (rows) for the Policy Attribute Table.
Service Table Size Current/Max	The current and maximum number of entries (rows) in the Service Table.

show policy-map

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

Format: `show policy-map` *`[policyname]`*

Command mode: Privileged

If the Policy Name is specified the following fields are displayed:

Term	*Value*
Policy Name	The name of this policy.
Policy Type	The policy type.
Class Members	The class that is a member of the policy.

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Term	*Value*
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
Class Name	The name of this class.
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Committed Rate (Kbps)	The committed rate, used in simple policing.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Conform 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) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome.
Conform COS	The CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	The DSCP mark value if the conform action is set-dscp-transmit.
Conform IP Precedence Value	The IP Precedence mark value if the conform action is set-prec-transmit.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Exceed Action	The action taken on traffic that exceeds settings that the network administrator specifies.
Exceed Color Mode	The current setting for the color of exceeding traffic

	that the user may optionally specify.
Mark CoS	The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.
Mark CoS as Secondary CoS	The secondary 802.1p priority value (second/inner VLAN tag). Same as CoS (802.1p) marking, but the dot1p value used for remarking is picked from the dot1p value in the secondary (i.e. inner) tag of a double-tagged packet.
Mark IP DSCP	The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.
Mark IP Precedence	The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. This field does not display on 5630x platforms.
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 is not in use for the class under this policy.
Non-Conform COS	The CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	The DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	The IP Precedence mark value if the non-conform action is set-prec-transmit.

Term	*Value*
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 (per type 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 forwarding traffic could inflict on other traffic (e.g., a token bucket rate limiter). Traffic that exceeds this limit is discarded.
Policing Style	The style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Term	*Value*
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created).

Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

show diffserv service

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

Format: `show diffserv service` *unit/slot/port* `[in | out]`

Command mode: Privileged

Term	*Value*
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	Interface in format *unit/slot/port*
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).

show diffserv service brief

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

Format: `show diffserv service brief [in | out]`

Command mode: Privileged

Term	*Value*
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):

Term	*Value*
Interface	Interface in format *unit/slot/port*
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.

show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The *unit/slot/port* parameter specifies a valid interface for the system. Instead of *unit/slot/port*, *lag lag-intf-num* can be used as an alternate way to specify the LAG interface. *lag lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format: `show policy-map interface` *unit/slot/port* `[in | out]`

Command mode: Privileged

Term	Value
Interface	Interface in format *unit/slot/port*
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.

The following information is repeated for each class instance within this policy:

Term	Value
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.

show service-policy

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

Format: `show service-policy in`

Command mode: Privileged

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Term	Value
Interface	Interface in format *unit/slot/port*
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

14.7 MAC ACL Configuration 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 maximum number of rules per MAC ACL is hardware dependent.
- The system supports only Ethernet II frame types.

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. The rate-limit attribute configures the committed rate and the committed burst size.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Format: `mac access-list extended` *name*

Command mode: Global Config

no mac access-list extended

This command deletes a MAC ACL identified by *name* from the system.

Format: `no mac access-list extended` *name*

Command mode: Global Config

mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The *name* parameter is the name of an existing MAC ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. This command fails if a MAC ACL by the name *newname* already exists.

Format: `mac access-list extended rename` *name newname*

Command mode: Global Config

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.

If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default: 10

Format: `mac access-list resequence` *{name| id } starting-sequence-number increment*

Command mode: Global Config

Parameter	*Description*
starting-sequence- number	The sequence number from which to start. The range is 1–2147483647. Default: 10.
increment	The amount to increment. The range is 1–2147483647. Default: 10.

{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.

Format: [*sequence-number*] {deny|permit} {*srcmac* | any} {*dstmac* | any} [*ethertypekey* | *0x0600- 0xFFFF*] [vlan {eq *0-4095*}] [cos *0-7*] [[log] [time-range *time-range-name*] [assign-queue *queue-id*]] [{mirror | redirect} *unit/slot/port*][rate-limit *rate burst-size*]

Command mode: MAC-Access-List Config

An implicit deny all MAC rule always terminates the access list.

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).

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.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-6. The *assign-queue* parameter is valid only for a permit rule.

The *mirror* parameter allows the traffic matching this rule to be copied to the specified *unit/slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *unit/slot/port*. The *assign-queue* and *redirect* parameters are only valid for a permit 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.

no sequence-number

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format: no *sequence-number*

Command mode: MAC-Access-List Config

mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by *name* to an interface or 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.

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.

The keyword *control-plane* is only available in Global Config mode.

Format: mac access-group *name* {{control-plane|in|out} vlan *vlan-id* {in|out}} [sequence *1– 4294967295*]

Command mode: Global Config
Interface Config

Parameter	*Description*
name	The name of the Access Control List.
sequence	An optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction.

no mac access-group

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

Format: `no mac access-group` *name* `{{control-plane|in|out} vlan` *vlan-id* `{in|out}}`

Command mode: Global Config
Interface Config

remark

This command adds a new comment 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. 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. 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.

Default: none

Format: `remark` *comment*

Command mode: IPv4-Access-List Config
IPv6-Access-List Config
MAC-Access-List Config
ARP-Access-List Config

no remark

Use this command to 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.

Default: none

Format: `no remark` *comment*

Command mode: IPv4-Access-List Config
IPv6-Access-List Config
MAC-Access-List Config
ARP-Access-List Config

show mac access-lists

This command displays summary 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 counters, If an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/ 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 indicates the number of packets that fall under this rule, regardless of the speed limit for this record.

ACL counters do not interact with diffserv policies.

Use the access list name to display detailed information of a specific MAC ACL.

The command output varies based on the match criteria configured within the rules of an ACL.

Format: `show mac access-lists [`*name*`]`
Command mode: Privileged

Term	*Value*
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. 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 Size	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	The unit/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.

14.8 IP ACL configuration 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:

- Switch software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.

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.

IP Standard ACL:

Format: access-list *1-99* {remark *comment*} | {[*sequence-number*]}] {deny | permit} {every | *srcip srcmask* | host *srcip*} [time-range *time-range-name*] [log] [assign-queue *queue- id*] [{mirror | redirect} *unit/slot/port*] [rate-limit *rate burst-size*]

Command mode: Global Config

IP Extended ACL:

Format: 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*} {*porkey*|*endport*}{eq|neq|lt|gt}{portkey|0-65535} {dstipdstmask|any|hostdstip}[{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} unit/slot/port] [rate-limit rate burst-size]

Command mode: Global Config

IPv4 extended ACLs have the following limitations for egress ACLs:

- **Match on port ranges is not supported;**
- **The rate-limit command is not supported.**

Parameter	*Description*
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. 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	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 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. 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*]	Specifies the IP access list rule.
{deny | permit}	Specifies whether the IP ACL rule permits or denies an action. ***Note***. 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** ***scrip***	Specifies a source IP address and source netmask for match conditionof 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 |endport}|{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 *lt* is 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* is 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.

	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. 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*, *tos/tosmask*. ***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 icmp-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*	***Note.*** 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.
[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 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.

no access-list

This command deletes an IP ACL that is identified by the parameter *accesslistnumber* from the system. The range for *accesslistnumber* is 1-99 for standard access lists and 100-199 for extended access lists.

Format: `no access-list accesslistnumber [rule 1-1023]`

Command mode: Global Config

ip access-list

This command creates an extended IP Access Control List (ACL) identified by name, consisting of classification fields defined for the IP header of an IPv4 frame. The name parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format: `ip access-list name`

Command mode: Global Config

no ip access-list

This command deletes the IP ACL identified by name from the system.

Format: `no ip access-list name`

Command mode: Global Config

ip access-list rename

This command changes the name of an IP Access Control List (ACL). The *name* parameter is the names of an existing IP ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails is an IP ACL by the name *newname* already exists.

Format: `ip access-list rename name newname`

Command mode: Global Config

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.

If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default: 10

Format: `ip access-list resequence {name| id } starting-sequence-number increment`

Command mode: Global Config

Parameter	Description
starting-sequence- number	The sequence number from which to start. The range is 1–2147483647. Default: 10.
increment	The amount to increment. The range is 1–2147483647. Default: 10.

{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.

Format: `[sequence-number] {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]| [ttl eq 0-255]}} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} unit/slot/port] [rate-limit rate burst-size]`

Command mode: IPv4-Access-List Config

An implicit deny all IP rule always terminates the access list.

The *mirror* parameter allows the traffic matching this rule to be copied to the specified *unit/slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *unit/slot/port*. The *assign-queue* and *redirect* parameters are only valid for a permit rule.

For IPv4, the following are not supported for egress ACLs:

- **A match on port ranges.**
- **The rate-limit command.**

Parameter	Description
sequence-number	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 calcu-

	lated 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, 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.
every	Match every packet.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 -255*}	Specifies the protocol to match for the IP ACL rule.
srcip srcmask | any | host *srcip*	Specifies a source IP address and source netmask for match condition of the ACL rule. Specifying "any" implies specifying *srcip* as 0.0.0.0 and srcmask as 255.255.255.255. Specifying host A.B.C.D implies *srcip* as A.B.C.D and srcmask as 0.0.0.0.
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	***Note.*** This option is available only if the protocol is TCP or UDP. Specifies the layer 4 port match condition for the IP ACL rule. Port number can be used, which ranges from 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 and who. Each of these keywords translates into its equivalent port number. When range is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified port range. 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 to 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, IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is 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 is specified, 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. When neq is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or port key. 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*, *tos/tosmask*. tosmask is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	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. This option is available only if the protocol is TCP.
[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 *icmp-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. The ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type.
igmp-type *igmp-type*	***Note.*** 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.
ttl eq	Specifies that the IP ACL rule matches on packets with the specified Time To Live (TTL) value.
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 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.
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 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.

no sequence-number

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format: no *sequence-number*

Command mode: IPv4-Access-List Config

ip access-group

This command either attaches a specific IP Access Control List (ACL) identified by accesslistnumber or name 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.

The keyword *control-plane* is only available in Global Config mode.

Default: none

Format: ip access-group {*accesslistnumber*|*name*} {{*control-plane*|*in*|*out*}|vlan *vlan-id* {in|out}} [sequence *1-4294967295*]

Command mode: Interface Config

Global Config

Parameter	*Description*
accesslistnumber	Identifies a specific IP ACL. The range is 1 to 199.
sequence	Ат optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction. (Available only in Global Config mode).
name	The name of the Access Control List.

no ip access-group

This command removes a specified IP ACL from an interface.

Default: none

Format: no ip access-group {*accesslistnumber*|*name*} {{*control-plane*|*in*|*out*}|vlan *vlan-id*{in|out}}

Command mode: Interface Config
Global Config

acl-trapflags

This command enables the ACL trap mode.

Default: disabled

Format: acl-trapflags

Command mode: Global Config

no acl-trapflags

This command disables the ACL trap mode.

Format: no acl-trapflags

Command mode: Global Config

show ip access-lists

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. 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 count of forwarded/discarded packets (for example: If burst of 100 packets sent from IXIA, the Counter value is 100).

If the ACL rule is configured with RATE LIMIT, the counter value will reflect the number of packets that fall under the rule, regardless of the speed limit. 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. ACL counters do not interact with diffserv policies.

Format: show ip access-lists [*accesslistnumber* | *name*]

Command mode: Privileged

Term	*Value*
ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into

	the interface (ingress) or leaving the interface (egress).
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).

If you specify an IP ACL number or name, the following information displays:

The command output varies based on the match criteria configured within the rules of an ACL.

Term	*Value*
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. Possible values are: Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are: TRUE or FALSE.
Protocol	Filtering protocol.
ICMP Type	***Note.*** This is shown only if the protocol is ICMP. The ICMP message type for this rule.
Starting Source L4 port	The starting source layer 4 port.
Ending Source L4 port	The ending source layer 4 port.
Starting Destination L4 port	The starting destination layer 4 port.
Ending Destination L4 port	The ending destination layer 4 port.
ICMP Code	***Note.*** This is shown only if the protocol is ICMP. The ICMP message code 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 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 IP 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 unit/slot/port to which packets matching this rule are copied.
Redirect Interface	The unit/slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IP ACL rule.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction. Instead of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. Lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number. Use the **control-plane** keyword to display the ACLs applied on the CPU port.

Format: `show access-lists interface {`*`unit/slot/port`* `in|out | control-plane}`

Command mode: Privileged

Term	*Value*
ACL Type	Access list type (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.
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.

show access-lists vlan

This command displays Access List information for a particular VLAN ID. The *vlan-id* parameter is the VLAN ID of the VLAN with the information to view. The {in | out} options specifies the direction of the VLAN ACL information to view.

Format: `show access-lists vlan` *`vlan-id`* `in|out`

Command mode: Privileged

Term	*Value*
ACL Type	Access list type (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.

14.9 IPv6 ACL configuration 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 II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

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. The rate-limit attribute configures the committed rate and the committed burst size.

The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format: `IPv6 access-list` *name*

Command mode: Global Config

no IPv6 access-list

This command deletes the IPv6 ACL identified by *name* from the system.

Format: `no IPv6 access-list` *name*

Command mode: Global Config

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.

Format: `IPv6 access-list rename` *name newname*

Command mode: Global Config

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.

If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default: 10

Format: `IPv6 access-list resequence {`*name*`|` *id* `}` *starting-sequence-number increment*

Command mode: Global Config

Parameter	*Description*
starting-sequence- number	The sequence number from which to start. The range is 1–2147483647. Default: 10.
increment	The amount to increment. The range is 1–2147483647. Default: 10.

{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.

Format: {deny | permit} {every | {{icmpv6 | IPv6 | tcp | udp | *0-255*} {*source-IPv6-prefix/ prefix-length* | any | *host source-IPv6-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*]

Command mode: IPv6-Access-List Config

An implicit deny all IPv6 rule always terminates the access list.

Parameter	*Description*
{deny | permit}	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.
every	Specifies to match every packet.
{*protocolkey* | *number*}	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.
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	***Note.*** This option is available only if the 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 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. 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 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. It is equivalent to specifying the range as <specified port number + 1> to 65535. When neq is specified, IPv6 ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. 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/prefix-length **|** **any |** ***host destination-IPv6-address***	Specifies a destination IP address and netmask for match condition of the IP 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 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. 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 the IPv6 rule.

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. 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 hardware.
[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 0to 255. When *icmp-code* is specified, IPv6 ACL rule matches on the specified ICMP message code, a number from 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*, *mld- 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*.
Fragments	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (Packets that have the next header field is set to 44).
Routing	Specifies that IPv6 ACL rule matches on IPv6 packets that have routing extension headers (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 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.
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 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.
rate-limit ***rate burst-size***	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

no sequence-number

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format: no *sequence-number*

Command mode: IPv6-Access-List Config

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 for this interface and direction, the specified IPv6 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.

An option *control-plane* is specified to apply the ACL on CPU port. The IPv6 control packets like IGMPv6 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.

The keyword *control-plane* is only available in Global Config mode.

Format: IPv6 traffic-filter *name* {{control-plane |in|out}|vlan *vlan-id* {in|out}} [sequence *1-4294967295*]

Command mode: Global Config

Interface Config

no IPv6 traffic-filter

This command removes an IPv6 ACL identified by *name* from the interface(s) in a given direction.

Format: no IPv6 traffic-filter <*name*{{control-plane | in | out} | vlan <*vlan-id*>{in|out}}

Command mode: Global Config

Interface Config

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 count of forwarded/discarded packets (for example: If burst of 100 packets sent from IXIA, the Counter value is 100).

If the ACL rule is configured with RATE LIMIT, the counter value will reflect the number of packets that fall under the rule, regardless of the speed limit. 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. ACL counters do not interact with diffserv policies.

Format: `show IPv6 access-lists` *`[name]`*

Command mode: Privileged

The command output varies based on the match criteria configured within the rules of an ACL.

Term	*Value*
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. Possible values are: Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are: TRUE or FALSE.
Protocol	Filtering protocol.
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 L4 port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination L4 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 *unit/slot/port* to which packets matching this rule are copied.
Redirect Interface	The *unit/slot/port* to which packets matching this rule are forwarded.

Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Rule Status	IPv6 ACL rule status (Active/Unactive)
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

14.10 Management Access Control and Administration List management commands

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.

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. The *name* value can be up to 32 characters.

Format: `management access-list` *name*

Command mode: Global Config

no management access-list

This command deletes the MACAL identified by *name* from the system.

Format: `no management access-list` *name*

Command mode: Global Config

{deny | permit} (Management ACAL)

This command creates a new rule for the current management access list. 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.

Format: `{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*`]`

Command mode: MACAL configuration

Parameter	*Description*
ethernet	Ethernet port number.
ip-source	The source IP address.
port-channel	Port-channel number.

priority	Priority for rule.
service	Service type condition, which can be one of the following key words: • java • tftp • telnet • ssh • http • https • snmp • sntp • any
vlan	VLAN number.
mask	The network mask of the source IP address (0–32).
prefix-length	The number of bits that comprise the source IP address prefix. prefix length must be preceded by a forward slash (/).

management access-class

Use this command to restrict management connections. The active management list cannot be updated or removed. The console-only keyword specifies that the device can be managed only from the console.

Format: `management access-class {console-only | name}`

Command mode: Global Config

no management access-class

This command disables the management restrictions.

Format: `no management access-class`

Command mode: Global Config

show management access-list

This command displays management access-lists.

Format: `show management access-list [name]`

Command mode: Privileged

show management access-class

This command displays information about the active management access list.

Format: `show management access-class [name]`

Command mode: Privileged

14.11 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.

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.

When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

Format: `time-range` *name*

Command mode: Global Config

no time-range

This command deletes a time-range identified by *name*.

Format: `no time-range` *name*

Command mode: Global Config

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. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format: `absolute [start` *time date*`] [end` *time date*`]`

Command mode: time range configuration

no absolute

This command deletes the absolute time entry in the time range.

Format: `no absolute`

Command mode: time range configuration

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 effect. 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.

The first occurrence of the time argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Format: `periodic` *`days-of-the-week time`* `to` *`time`*

Command mode: time range configuration

no periodic

This command deletes a periodic time entry from a time range.

Format: `no periodic` *`days-of-the-week time`* `to` *`time`*

Command mode: time range configuration

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. Use the *name* parameter to identify a specific time range to display. When *name* is not specified, all the time ranges defined in the system are displayed.

Format: `show time-range [`*`name`*`]`

Command mode: Privileged

The information in the following table displays when no time range name is specified.

Term	*Value*
Admin Mode	The administrative mode of the time range feature on the switch.

Current number of all Time Ranges	The number of time ranges currently configured in the system.
Maximum number of all Time Ranges	The maximum number of time ranges that can be configured in the system.
Time Range Name	Name of the time range.
Status	Status of the time range (active/inactive).
Periodic Entry count	The number of periodic entries configured for the time range.
Absolute Entry	Indicates whether an absolute entry has been configured for the time range (Exists).

14.12 Auto-Voice over IP commands

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

auto-voip

Use this command to configure auto VoIP mode. The supported modes are protocol-based and oui-based. Protocol-based auto VoIP prioritizes the voice data based on the layer 4 port used for the voice session. OUI based auto VoIP prioritizes the phone traffic based on the known OUI of the phone.

When both modes are enabled, if the connected phone OUI is one of the configured OUI, then the voice data is prioritized using OUI Auto VoIP, otherwise protocol-based Auto VoIP is used to prioritize the voice data.

Active sessions are cleared if protocol-based auto VoIP is disabled on the port.

Default: oui-based

Format: `auto-voip [protocol-based | oui-based]`

Command mode: Global Config

Interface Config

no auto-voip

Use the **no** form of the command to set the default mode.

Format: `auto-voip [protocol-based | oui-based]`

Command mode: Global Config

Interface Config

auto-voip oui

Use this command to configure an OUI for Auto VoIP. The traffic from the configured OUI will get the highest priority over the other traffic. The *oui-prefix* is a unique OUI that identifies the device manufacturer or vendor. The OUI is specified in three octet values (each octets represented as two hexadecimal digits) separated by colons. The *string* is a description of the OUI that identifies the manufacturer or vendor associated with the OUI.

Default: A list of known OUIs is present.

Format: `auto-voip oui` *`oui-prefix`* `oui-desc` *`string`*

Command mode: Global Config

no auto-voip oui

Use the **no** form of the command to remove a configured OUI prefix from the table.

Format: `no auto-voip oui` *`oui-prefix`*

Command mode: Global Config

auto-voip oui-based priority

Use this command to configure the global OUI based auto VoIP priority. If the phone OUI is matches one of the configured OUI, then the priority of traffic from the phone is changed to OUI priority configured through this command. The *priority-value* is the 802.1p priority used for traffic that matches a value in the known OUI list.

Default: Highest available priority (7).

Format: `auto-voip oui-based priority` *`priority-value`*

Command mode: Global Config

no auto-voip oui-based priority

Use the **no** version of the command to return global priority of VoIP to the default value.

Format: `no auto-voip oui` *`oui-prefix`*

Command mode: Global Config
Interface Config

auto-voip protocol-based

Use this command to configure the global protocol-based auto VoIP remarking priority or traffic-class. If remark priority is configured, the voice data of the session is remarked with the priority configured through this command.

The *remark-priority* is the 802.1p priority used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device marks traffic in that session with the specified 802.1p priority value to ensure voice traffic always gets the highest priority throughout the network path.

The *tc* value is the traffic class used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device assigns the traffic in that session to the configured Class of Service (CoS) queue. Traffic classes with a higher value are generally used for time-sensitive traffic.

The CoS queue associated with the specified traffic class should be configured with the appropriate bandwidth allocation to allow priority treatment for VoIP traffic.

Default: Traffic Class 7

Format: `auto-voip protocol-based {remark` *`remark-priority`* `| traffic-class` *`tc`*`}`

Command mode: Global Config
Interface Config

no auto-voip protocol-based

Use this command to reset the global protocol based auto VoIP remarking priority or traffic-class to the default.

Format: `no auto-voip protocol-based {remark` *`remark-priority`* `| traffic-class` *`tc`*`}`

Command mode: Global Config
Interface Config

auto-voip vlan

Use this command to configure the global Auto VoIP VLAN ID. The VLAN behavior is depend on the configured auto VoIP mode. The auto-VoIP VLAN is the VLAN used to segregate VoIP traffic from other non-voice traffic. All VoIP traffic that matches a value in the known OUI list gets assigned to this VoIP VLAN.

Default: none

Format: `auto-voip vlan` *`vlan-id`*

Command mode: Global Config

no auto-voip vlan

Use the **no** form of the command to reset the auto-VoIP VLAN ID to the default value.

Format: `no auto-voip vlan`

Command mode: Global Config

show auto-voip

Use this command to display the auto VoIP settings on the interface or interfaces of the switch.

Format: `show auto-voip {protocol-based|oui-based} interface {`*`unit/slot/port`*`|all}`

Command mode: Privileged

Field	*Description*
VoIP VLAN ID	The global VoIP VLAN ID.
Prioritization Type	The type of prioritization used on voice traffic.
Class Value	• If the **Prioritization Type** is configured as traffic-class, then this value is the queue value. • If the **Prioritization Type** is configured as remark, then this value is 802.1p priority used to remark the voice traffic.
Priority	The 802.1p priority. This field is valid for OUI auto VoIP.
AutoVoIP Mode	The Auto VoIP mode on the interface.

show auto-voip oui-table

Use this command to display the VoIP oui-table information.

Format: `show auto-voip oui-table`

Command mode: Privileged

Parameter	*Description*
OUI	OUI of the source MAC address.
Status	Default or configured entry.
OUI Description	Description of the OUI.

14.13 iSCSI optimization commands

This section describes commands you use to monitor iSCSI sessions and prioritize iSCSI packets. ISCSI Optimization provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

iscsi aging time

This command sets the aging time for iSCSI sessions. Behavior when changing aging time:

- When aging time is increased, current sessions will be timed out according to the new value.
- When aging time is decreased, any sessions that have been dormant for a time exceeding the new setting will be immediately deleted from the table. All other sessions will continue to be monitored against the new time out value.

Default: 10 minutes

Format: `iscsi aging time` *`time`*

Command mode: Global Config

Parameter	*Description*
time	The number of minutes a session must be inactive prior to its removal. The range is 1–43 200.

no iscsi aging time

Use the no form of the command to reset the aging time value to the default value.

Format: `no iscsi aging time`

Command mode: Global Config

iscsi cos

This command sets the quality of service profile that will be applied to iSCSI flows. ISCSI flows are assigned by default to the highest VPT/DSCP mapped to the highest queue not used for stack management. The user should also take care of configuring the relevant Class of Service parameters for the queue in order to complete the setting.

Setting the VPT/DSCP sets the QoS profile which determines the egress queue to which the frame is mapped. The switch default setting for egress queues scheduling is Weighted Round Robin (WRR).

You may complete the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes via the Class of Service settings. Depending on the platform, these choices may include strict priority for the queue used for iSCSI traffic. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic may get starved. In WRR the queue to which the flow is assigned to can be set to get the required percentage.

Format: `iscsi cos {vpt vpt | dscp dscp} [remark]`

Command mode: Global Config

Parameter	*Description*
vpt/dscp	The VLAN Priority Tag or DSCP to assign iSCSI session packets.
remark	Mark the iSCSI frames with the configured VPT/DSCP when egressing the switch.

no iscsi cos

Use the no form of the command to return to the default.

Format: `no iscsi cos`

Command mode: Global Config

iscsi enable

This command globally enables iSCSI awareness.

Default: disabled

Format: `iscsi enable`

Command mode: Global Config

no iscsi enable

This command disables iSCSI awareness. When you use the no iscsi enable command, iSCSI resources will be released.

Format: `no iscsi enable`

Command mode: Global Config

iscsi target port

This command configures an iSCSI target port and, optionally, a target system's IP address and IQN name. When working with private iSCSI ports (not IANA-assigned ports 3260/860), it is recommended to

specify the target IP address as well, so that the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, and the destination IP is the target's IP address. This way the CPU will not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these un-reserved ports.

When a port is already defined and not bound to an IP address, and you want to bind it to an IP address, you should first remove it by using the no form of the command and then add it again, this time together with the relevant IP address.

Target names are only for display when using the **show iscsi** command. These names are not used to match with the iSCSI session information acquired by snooping.

A maximum of 16 TCP ports can be configured either bound to IP or not.

Default: ISCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target.

Format: `iscsi target port` *`tcp-port-1 [tcp-port-2...tcp-port-16]`* `[address` *`ip-address]`* `[name` *`targetname`*`]`

Command mode: Global Config

Parameter	*Description*
tcp-port-n	TCP port number or list of TCP port numbers on which the iSCSI target listens to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.
ip-address	IP address of the iSCSI target. When the no form of this command is used, and the tcp port to be deleted is one bound to a specific IP address, the address field must be present.
targetname	iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSNS or from sendTargets response. The initiator must present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection.

no iscsi target port

Use the no form of the command to delete an iSCSI target port, address, and name.

show iscsi

This command displays the iSCSI settings.

Format: `show iscsi`

Command mode: Privileged

show iscsi sessions

This command displays the iSCSI sessions.

Default: If not specified, sessions are displayed in short mode (not detailed).

Format: `show iscsi sessions [detailed]`

Command mode: Privileged

15 SYSTEM MESSAGES

This chapter lists common log messages, 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 in determining the root cause of such a problem. The most recent log messages are displayed first.

This chapter is not a complete list of all syslog messages.

15.1 Core

BSP log messages

Component	*Message*	*Cause*
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting software application.

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 event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system.
NIM	NIM: failed to send message to NIM message Queue	NIM message queue full or non-existent.
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase.
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase.
NIM	NIM: Component(x) failed on event(x) for interface	A component responded with a fail indication for an interface event.
NIM	NIM: Timeout event(x), interface remainingMask = xxxx	A component did not respond before the NIM timeout occurred.

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.

System log messages

Component	*Message*	*Cause*
SYSTEM	Configuration file system.cfg size is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file *file name* version *version num*	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.
SYSTEM	File *filename*: same version (*version num*) but the sizes (*version size – expected version size*) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. A message may be displayed after updating the code image to a newer version of the product.
SYSTEM	Migrating config file *filename* from version *version num* to *version num*	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. A message may be displayed after updating the code image to a newer version of the product.
SYSTEM	Building Defaults	The configuration for the specified option is missing or cannot be read. Default configuration values will be used.
SYSTEM	sysapiCfgFileGet failed size = *expected size of file* version = *expected version*	The configuration for the specified option is missing or cannot be read. This message is usually followed by a message indicating that default configuration values will be used.

15.2 Utilities

Trap Mgr log message

Component	*Message*	*Cause*
Trap Mgr	Link Up/Down: unit/slot/port	An interface changed link state.

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.

NVStore log messages

Component	*Message*	*Cause*
NVStore	Building defaults for file XXX	A component's configuration file does notexist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	Error on call to osapiFsWrite routine on file XXX	Either the file cannot be opened or the OS's file I/O returned an error trying to write to the file.
NVStore	Error on call to osapiFsWrite routine on file XXX	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.

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.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Error while attempting to read data from the RADIUS server.
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	RADIUS Client received a server response from an unconfigured server.

TACACS+ log messages

Component	*Message*	*Cause*
(TACACS+)	TACACS+: authentication error, no server to contact	RADIUS Client received a server response from an unconfigured server.
(TACACS+)	TACACS+: connection 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.

LLDP log message

Component	*Message*	*Cause*
LLDP	lldpTask(): invalid message type:xx.xxxxxx:xx	Unsupported LLDP packet received.

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.

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 IP6Map 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 aDNS6 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 DHCPv6 Server to the DNS6 Client fails.

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.

15.3 Control

SNMP log message

Component	*Message*	*Cause*
SNMP	EDB Callback: Unit Join: x	A new unit has joined the stack.

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	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection	Socket receive failure.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending: EWOULDBLOCK error sending data	Socket error on send.
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	EmWeb handle index not valid.
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	The receive buffer limit has been reached. Bad request or DoS attack.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

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.

WEB system messages

Component	*Message*	*Cause*
Web	Max clients exceeded	This message is shown when the maximum allowed java client connections to the switch is exceeded.
Web	Error on send to sockfd XXXX, closing connection	Failed to send data to the java clients through the socket.
Web	# (XXXX) Form Submission Failed. No Action Taken.	The form submission failed and no action is taken. XXXX indicates the file under consideration.
Web	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	Unknown error returned while downloading file using TFTP from web interface.
Web	ewaFormServe_file_upload() - Unknown return code from tftp upload result	Unknown error returned while uploading file using TFTP from web interface.
Web	Web UI Screen with unspecified access attempted to be brought up	Failed to get application-specific authorization handle provided to EmWeb/Server by the application in ewsAuthRegister(). The specified web page will be served in read-only mode.

CLI_WEB_MGR log messages

Component	*Message*	*Cause*
CLI_WEB_MGR	File size is greater than 2K	The banner file size is greater than 2K bytes.
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	When the number of rows exceeds the maximum allowed rows.

SSHD log messages

Component	*Message*	*Cause*
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent.
SSHD	SSHD: Unknown UI event in message, event = XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it's an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd	Failed to send the message to the SSHD message queue.

SSLT system messages

Component	*Message*	*Cause*
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.
SSLT	SSLT: Error creating Secure server socket6	Failed to create secure server socket

		forIPV6.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.
SSLT	SSLT: Msg Queue is full, event = XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSL certificate from the XXXX file.
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.

User_Manager log messages

Component	*Message*	*Cause*
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX – username.
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 – 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.

15.4 Switching

Protected Ports log messages

Component	*Message*	*Cause*
Protected Ports	Protected Port: failed to save configuration	This appears when the protected portconfiguration cannot be saved.
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port	This appears when protectedPortCfgRWLock Fails.
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	nimRegisterIntfChange for VLAN failure.
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 aninterface 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.

IP Subnet VLANS log messages

Component	*Message*	*Cause*
IP subnet VLANs	ERROR vlanIpSubnetSubnetValid:Invalid subnet	This occurs when an invalid pair of subnet and netmask has come from the CLI.
IP subnet VLANs	IP Subnet Vlans: failed to save configuration	This message appears when saveconfiguration of subnet vlans failed.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
IP subnet VLANs	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
IP subnet VLANs	vlanIpSubnetDtlVlanCreate: Failed	This appears when a dtl call fails to add an entry into the table.
IP subnet VLANs	vlanIpSubnetSubnetDeleteApply: Failed	This appears when a dtl fails to delete anentry from the table.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to add an entry	This appears when a dtl fails to add an entry for a vlan add notify event.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to delete an entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Mac-based VLANs log messages

Component	*Message*	*Cause*
MAC based VLANs	MAC VLANs: Failed to save configuration	This message appears when save configuration of Mac vlans failed.
MAC based VLANs	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	This appears when a read/write lock creations fails.
MAC based VLANs	Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
MAC based VLANs	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
MAC based VLANs	vlanMacAddApply: Failed to add an entry	This appears when a dtl call fails to add an entry into the table.
MAC based VLANs	vlanMacDeleteApply: Unable to delete an Entry	This appears when a dtl fails to delete anentry from the table.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to add an entry	This appears when a dtl fails to add an entry for a vlan add notify event.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to delete an entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

802.1X log messages

Component	*Message*	*Cause*
802.1X	*function*: Failed calling dot1xIssueCmd	802.1X message queue is full.
802.1X	*function:* EAP message not received from server	RADIUS server did not send required EAP message.
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	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server.
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx	Failed sending accounting start to RADIUS server.
802.1X	*function*: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server.

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	snoopCnfgrInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets.

GARP/GVRP/GMRP log messages

Component	*Message*	*Cause*
GARP/GVRP/GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	The garpQueue is full, logs specifics of the message content like internal interface number, type of message, etc.
GARP/GVRP/GMRP	GarpSendPDU: QUEUE SEND FAILURE	The garpPduQueue is full, logs specific oftheGPDU, internal interface number, vlan id, buffer handle, etc.
GARP/GVRP/GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing	A default configuration doesn't exist for this interface. Typically a case when a

	GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	new interface is created and has no preconfiguration.
GARP/GVRP/GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Traces the build up of message queue. Helpful in determining the load on GARP.
GARP/GVRP/GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	Mismatch between the gmd (gmrp database) and MFDB.
GARP/GVRP/GMRP	gmd_create_entry**:** GMRP failure adding MFDB entry: vlan %d and address %s	MFDB table is full.

802.3ad log messages

Component	*Message*	*Cause*
802.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully.

FDP 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.

Double VLAN Tag log message

Component	*Message*	*Cause*
Double VLAN Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration doesn't exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

IPv6 Provisioning log message

Component	*Message*	*Cause*
IPV6 Provisioning	ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d	A default configuration doesn't exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

MFDP log message

Component	*Message*	*Cause*
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

802.1Q log message

Component	*Message*	*Cause*
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	Dot1qMsgQueue is full.

802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range	This accommodates for reserved vlan ID.
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration doesn't 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	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	If this vlan is a learnt via GVRP then we cannot modify its member set via management.
802.1Q	dtl failure when adding ports to vlan id %d - portMask = %s	Failed to add the ports to VLAN entry in hardware.
802.1Q	dtl failure when deleting ports from vlan id %d - portMask = %s	Failed to delete the ports for a VLAN entry from the hardware.
802.1Q	dtl failure when adding ports to tagged list for vlan id %d - portMask = %s	Failed to add the port to the tagged list in hardware.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d - portMask = %s"	Failed to delete the port to the tagged list from the hardware.
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x"	Failed to receive the dot1q message from dot1q message queue.
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Failed to create VLAN ID, VLAN Database reached maximum values.
802.1Q	Attempt to create a vlan (%d) that already exists	Creation of the existing Dynamic VLAN ID from the CLI.
802.1Q	DTL call to create VLAN %d failed with rc %d"	Failed to create VLAN ID in hardware.
802.1Q	Problem unrolling data for VLAN %d	Failed to delete VLAN from the VLAN database after failure of VLAN hardware creation.
802.1Q	VLan %d does not exist	Failed to delete VLAN entry.
802.1Q	VLan %d requestor type %d does not exist	Failed to delete dynamic VLAN ID if the given requestor is not valid.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Failed to delete, as some unknown component has taken the ownership.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Failed to delete the VLAN ID as the given requestor and VLAN entry status are not same.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Failed to delete VLAN ID from the hardware.
802.1Q	Problem deleting data for VLAN %d	Failed to delete VLAN ID from the VLAN database.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Failed to modify the VLAN group filter.
802.1Q	Cannot find vlan %d to convert it to static	Failed to convert Dynamic VLAN to static VLAN. VLAN ID not exists.
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	The VLAN ID does not exist.
802.1Q	VLAN create currently underway for VLAN ID %d	Creating a VLAN which is already under process of creation.
802.1Q	VLAN ID %d is already exists as static VLAN	Trying to create already existing static VLAN ID.
802.1Q	Cannot put a message on dot1q msg Queue, Returns:%d	Failed to send Dot1q message on Dot1q message Queue.
802.1Q	Invalid dot1q Interface: %s	Failed to add VLAN to a member of port.
802.1Q	Cannot set membership for user interface %s on management vlan %d	Failed to add VLAN to a member of port.
802.1Q	Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s	Incorrect tagmode for VLAN tagging.
802.1Q	Cannot set tagging for interface %d on non existent VLAN %d"	The VLAN ID does not exist.
802.1Q	Cannot set tagging for interface %d which is not a member of VLAN %d	Failure in Setting the tagging configuration for a interface on a range of VLAN.
802.1Q	VLAN create currently underway for VLAN ID %d"	Trying to create the VLAN ID which is already under process of creation.
802.1Q	VLAN ID %d already exists	Trying to create the VLAN ID which is already exists.
802.1Q	Failed to delete, Default VLAN %d cannot be deleted	Trying to delete Default VLAN ID.
802.1Q	Failed to delete, VLAN ID %d is not a static VLAN	Trying to delete Dynamic VLAN ID from CLI.
802.1Q	Requestor %d attempted to release internal VLAN %d: owned by %d	-

802.1S log messages

Component	*Message*	*Cause*
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU.
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers.

Port Mac Locking log message

Component	*Message*	*Cause*
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration doesn't exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Protocol-based VLANs log messages

Component	*Message*	*Cause*
Protocol based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.
Protocol based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with VLANs	Appears when VLANRegisterForChange fails to register pbVlan for VLAN changes.
Protocol based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

15.5 QoS

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.

CoS log message

Component	*Message*	*Cause*
COS	cosCnfgrInitPhase3Process: 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.

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.
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.

15.6 Routing/IPv6 Routing

DHCP Relay log messages

Component	*Message*	*Cause*
DHCP Relay	REQUEST hops field more than config value	The DHCP relay agent has processed aDHCP 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.

OSPFv2 system messages

Component	*Message*	*Cause*
OSPFv2	Best route client deregistration failed for OSPF Redist	OSPFv2 registers with the IPv4 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.
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.

OSPFv3 log messages

Component	*Message*	*Cause*
OSPFv3	Best route client deregistration failed for OSPFv3 Redist	OSPF registers with the IPv6 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 numder of Link State Advertisments (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	OSPFv3 periodically verifies the checksum of each LSA in

	for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.	memory. OSPFv3 logs this.

Routing Table Manager log messages

Component	*Message*	*Cause*
RTO	RTO is no longer full. Routing table contains xxx best routes, xxx total routes, xxx 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.

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 Virtualrouter 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.

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.

RIP log message

Component	*Message*	*Cause*
RIP	RIP: discard response from xxx via unexpected interface	When RIP response is received with a source address not matching the incoming interface's subnet.

15.7 Multicast

IGMP/MLD log messages

Component	*Message*	*Cause*
IGMP/MLD	MGMD Protocol Heap Memory Init Failed; Family – xxx.	MGMD Heap memory initialization Failed for the specified address family. This message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD Protocol Heap Memory De-Init 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 non-availability 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 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 Interpeak Stack Failed; rtrIfNum - xxx, intf – xxx.	Registration of this Group address with the Interpeak 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, rtrIfNum – 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.

15.8 Stacking

EDB log message

Component	*Message*	*Cause*
EDB	EDB Callback: Unit Join: *num*.	Unit *num* has joined the stack.

15.9 Technologies

Error messages

Component	*Message*	*Cause*
Broadcom	Invalid USP unit = x, slot = x, port = x	A port was not able to be translated correctly during the receive.
Broadcom	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. Cause: This should only happen when a hash collision occurs or the table is full.
Broadcom	Failed installing mirror action - rest of	A previously configured probe port is not being used in

	the policy applied successfully	the policy. The release notes state that only a single probe port can be configured.
Broadcom	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.
Broadcom	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x	An issue installing the policy due to a possible duplicate hash.
Broadcom	ACL x not found in internal table	Attempting to delete a non-existent ACL.
Broadcom	ACL internal table overflow	Attempting to add an ACL to a full table.
Broadcom	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it's capabilities.
Broadcom	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.
Broadcom	USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.
Broadcom	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.
Broadcom	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL.
Broadcom	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.
Broadcom	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn't exist.
Broadcom	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	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.
Broadcom	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: failed to sync dVLAN data on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	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.
Broadcom	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.
Broadcom	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI.
Broadcom	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
Broadcom	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
Broadcom	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.
Broadcom	Unable to Insert host H	Host H could not be inserted in hardware host table. A

		retry will be issued.
Broadcom	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.
Broadcom	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.
Broadcom	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.
Broadcom	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.
Broadcom	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.
Broadcom	USL: failed to sync ip-multicast 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.

15.10 OS Support

Linux BSP log message

Component	*Message*	*Cause*
Linux BSP	rc = 10	Second message logged at bootup, right after *Starting code…. Always logged*.

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	unable to open /proc/net/ipv6/conf/default/hop_limit	IPv6 MIB objects read, but /proc file system is not mounted, or running kernel does not have IPV6 support
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	osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: 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 for the UI 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_Init: 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 check-sum.
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.

TECHNICAL SUPPORT

Contact Eltex Service Centre to receive technical support regarding our products:

29v Okruzhnaya st., Novosibirsk, Russian Federation, 630020
Phone number:
+7(383) 274-47-87
+7(383) 272-83-31
E-mail: techsupp@eltex-co.ru

Visit Eltex official website to get the relevant technical documentation and software, benefit from our knowledge base, send us online request or consult a Service Centre Specialist in our technical forum.

Official website: http://eltex-co.com
Technical forum: http://eltex-co.ru/forum
Knowledge base: http://eltex-co.com/support/knowledge
Download center: http://eltex-co.com/support/downloads