



# VOSS Command Line Interface Commands Reference

For VSP 8600 Release 8.1

9037144-00 Rev AA  
February 2022



Copyright © 2022 Extreme Networks, Inc.

## Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

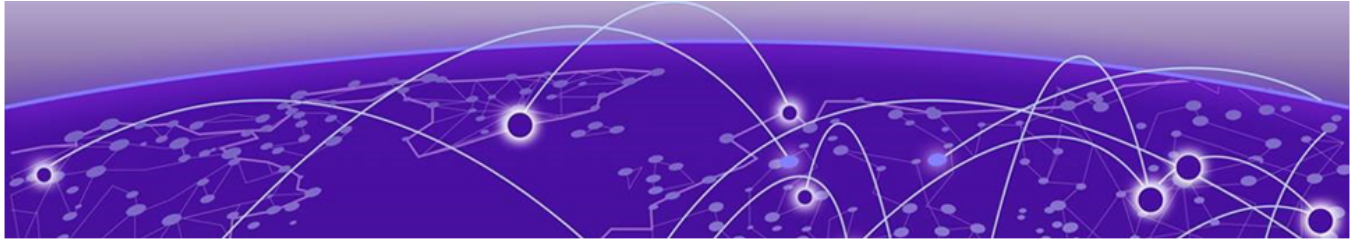
Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: [www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks)

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



# Table of Contents

---

About this Document.....	5
New in this Document.....	10
Application Configuration.....	11
BFD Router Configuration.....	18
BGP Router Configuration.....	19
DHCP-guard Configuration.....	61
Elan I-SID Configuration.....	64
Elan-Transparent Configuration.....	67
Fabric IPsec Gateway Configuration.....	69
GigabitEthernet Interface Configuration.....	102
Global Configuration.....	295
IS-IS Router Configuration.....	665
IS-IS Router Remote Configuration.....	714
Logical Interface Configuration.....	719
Loopback Interface Configuration.....	730
Management Instance Configuration.....	741
mgmtEthernet Interface Configuration.....	750
MKA Profile Configuration.....	762
MLT Interface Configuration.....	765
OSPF Router Configuration.....	778
OVSDB Configuration.....	806
Privileged EXEC.....	809
RA-guard Configuration.....	1020
RIP Router Configuration.....	1024
Route-Map Configuration.....	1034
User EXEC.....	1055
VLAN Interface Configuration.....	1610
VRF Router Configuration.....	1699

<b>VRRP Router Configuration.....</b>	<b>1809</b>
<b>VXLAN Configuration.....</b>	<b>1812</b>





# About this Document

---

[Purpose](#) on page 5

[Conventions](#) on page 6

[Documentation and Training](#) on page 8

[Help and Support](#) on page 8

[Send Feedback](#) on page 9

The topics in this section discuss the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

## Purpose

---

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- ExtremeSwitching 5420 Series
- ExtremeSwitching 5520 Series
- ExtremeSwitching VSP 4450 Series
- ExtremeSwitching VSP 4900 Series
- ExtremeSwitching VSP 7200 Series
- ExtremeSwitching VSP 7400 Series
- ExtremeSwitching VSP 8200 Series
- ExtremeSwitching VSP 8400 Series
- ExtremeSwitching VSP 8600 Series
- ExtremeSwitching XA1400 Series



### Note

VOSS is licensed on the XA1400 Series as a Fabric Connect VPN (FCVPN) application, which includes a subset of VOSS features. FCVPN transparently extends Fabric Connect services over third-party provider networks.

This guide describes the Command Line Interface (CLI) commands for the configuration of various features in VOSS. The chapters in this document correspond to a command mode in the CLI. Each chapter is organized alphabetically for those commands in that mode. If a command is available in all modes, like many **show** commands, it is documented in the mode that requires the lowest level of access privileges.






## Conventions

To help you better understand the information presented in this guide, the following topics describe the formatting conventions used for notes, text, and other elements.

### Text Conventions

The following tables list text conventions that can be used throughout this document.

**Table 1: Notes and warnings**

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product.
	Note	Useful information or instructions.
	Important	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.

**Table 2: Text Conventions**

Convention	Description
Angle brackets ( < > )	Angle brackets ( < > ) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is <code>cfm maintenance-domain maintenance-level &lt;0-7&gt;</code> , you can enter <code>cfm maintenance-domain maintenance-level 4</code> .
<b>Bold text</b>	Bold text indicates the GUI object name you must act upon. Examples: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>On the <b>Tools</b> menu, choose <b>Options</b>.</li> </ul>

**Table 2: Text Conventions (continued)**

Convention	Description
Braces ( { } )	Braces ( { } ) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is <code>ip address {A.B.C.D}</code> , you must enter the IP address in dotted, decimal notation.
Brackets ( [ ] )	Brackets ( [ ] ) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is <code>show clock [detail]</code> , you can enter either <code>show clock</code> or <code>show clock detail</code> .
Ellipses ( ... )	An ellipsis ( ... ) indicates that you repeat the last element of the command as needed. For example, if the command syntax is <code>ethernet/2/1 [ &lt;parameter&gt; &lt;value&gt; ] ...</code> , you enter <code>ethernet/2/1</code> and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
Plain Courier Text	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: <ul style="list-style-type: none"> <li><code>show ip route</code></li> <li><code>Error: Invalid command syntax [Failed] [2013-03-22 13:37:03.303 -04:00]</code></li> </ul>
Separator ( > )	A greater than sign ( > ) shows separation in menu paths. For example, in the Navigation tree, expand the <b>Configuration &gt; Edit</b> folders.
Vertical Line (   )	A vertical line (   ) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is <code>access-policy by-mac action { allow   deny }</code> , you enter either <code>access-policy by-mac action allow</code> or <code>access-policy by-mac action deny</code> , but not both.

---

## Documentation and Training

---

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and software compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other resources](#) such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit [www.extremenetworks.com/education/](http://www.extremenetworks.com/education/).

---

## Help and Support

---

If you require assistance, contact Extreme Networks using one of the following methods:

### Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

### The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

### Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

## Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.

3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

## Send Feedback

---

The Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, do either of the following:

- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at [documentation@extremenetworks.com](mailto:documentation@extremenetworks.com).

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



# New in this Document

---

## Notice about Feature Support on page 10

The following sections detail what is new in this document.

## New Commands

---

The following commands are newly added to this document:

OSPFv3 Support for CLIP Interfaces

- [ipv6 ospf](#) on page 738

## Updated Commands

---

The following commands are updated in this document:

**Table 3: Existing Command Updates**

Command	Update
<b>show khi performance</b>	Added new <i>rx-queue</i> parameter.
<b>show io resources</b>	added the following new parameters: <ul style="list-style-type: none"><li>• <i>l3-kaps-count</i></li><li>• <i>l3-lem-count</i></li><li>• <i>model-dnx-stats</i></li></ul>

## Notice about Feature Support

---

This document includes content for multiple hardware platforms across different software releases. As a result, the content can include features not supported by your hardware in the current software release. If a documented command or parameter does not appear on your hardware, it is not supported. For information about feature support, see [VOSS Feature Support Matrix](#).

For information about physical hardware restrictions, see your hardware documentation.

For more information about how individual commands and parameters apply to different products, see the configuration information in the [VOSS User Guide](#).



# Application Configuration

---

The following topics document commands available in Application Configuration mode of the command line interface (CLI).

## iqagent enable

---

Enables IQAgent.

### Syntax

- **iqagent enable**
- **no iqagent enable**

### Default

The default is enabled.

### Command Mode

Application Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## iqagent proxy

---

Configures the proxy parameters.

### Syntax

- **iqagent proxy address WORD<1-255> tcp-port <1-49151>**
- **iqagent proxy username WORD<1-64> password WORD <1-128>**
- **no iqagent proxy address WORD<1-255> tcp-port <1-49151>**
- **no iqagent proxy username**

## Command Parameters

**address WORD<1-255>**

Specifies the proxy IPv4 address or DNS name.

**username <WORD 1-64>**

Specifies the proxy server username.

**password <WORD 1-128>**

Specifies the proxy server password.

**tcp-port <1-49151>**

Specifies the TCP port to use for IQAgent.

## Default

None

## Command Mode

Application Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## iqagent server

---

Configures the IPv4 address or DNS name.

## Syntax

- **default iqagent server**
- **iqagent server address WORD<1-255>**
- **no iqagent server**

## Default

The default server address is hac.extremecloudiq.com.

## Command Mode

Application Configuration



## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## restconf

---

Enable or disable the Representational State Transfer Configuration Protocol (RESTCONF) server.

### Syntax

- **default restconf** <enable | tcp-port | tls | trap-notification>
- **no restconf** <enable | install-cert-file | tls | trap-notification>
- **restconf** <enable | install-cert-file WORD<1-128> | tcp-port <1-49151> | tls | trap-notification>

### Command Parameters

#### enable

Enables the RESTCONF server.

#### install-cert-file WORD <1-128>

Installs the certificate file for RESTCONF.

#### tcp-port <1-49151>

Specifies the TCP port to use for the RESTCONF server. The default is 8080.

#### tls

Enables or disables TLS/SSL for the RESTCONF server. The default is disable.

#### trap-notification

Enables or disables trap notification with the RESTCONF protocol is not available. The default is enable.

### Default

The default value is disable.

### Command Mode

Application Configuration

## slamon agent

---

Configures the SLA Mon agent.

## Syntax

- **default slamon agent ip address**
- **default slamon agent port**
- **slamon agent ip address {A.B.C.D}**
- **slamon agent ip address {A.B.C.D} vrf WORD<1-16>**
- **slamon agent port <0-65535>**

## Command Parameters

**ip address {A.B.C.D}**

Configures the SLA Mon agent IP address. You must configure the IP address before the agent can process received discovery packets from the SLA Mon server. The agent IP address is a mandatory parameter if you enable SLA Mon. The default value is 0.0.0.0.

**port <0-65535>**

Configures the UDP port for SLA Mon agent-server communication. The agent receives discovery packets on this port. The default is port 50011. The server must use the same port.

**vrf WORD<1-16>**

Specifies a VRF name. The VRF parameter is optional.

## Default

None

## Command Mode

Application Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## slamon agent-comm-port

---

Controls the port used for Real Time Protocol (RTP) and New Trace Route (NTR) testing.

## Syntax

- **default slamon agent-comm-port**
- **slamon agent-comm-port <0-65535>**

## Command Parameters

**<0-65535>**

Configures the port used for RTP and NTR testing in agent-to-agent communication. The default port is 50012. If you configure this value to zero (0), the default port is used.

## Default

The default is 50012.

## Command Mode

Application Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## slamon install-cert-file

---

Installs a Secure Sockets Layer (SSL) certificate.

## Syntax

- **no slamon install-cert-file**
- **slamon install-cert-file WORD<0-128>**

## Command Parameters

**WORD<0-128>**

Specifies the file name and path of the certificate to install.

## Default

None

## Command Mode

Application Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## slamon oper-mode enable

---

Enables the SLA Mon agent.

## Syntax

- **default slamon oper-mode**
- **no slamon oper-mode**
- **no slamon oper-mode enable**
- **slamon oper-mode**
- **slamon oper-mode enable**

## Default

The default is disabled.

## Command Mode

Application Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## slamon server

Configures information about the SLA Mon server with which the agent communicates.

## Syntax

- **default slamon server ip address**
- **default slamon server port**
- **port <0-65535> <0-65535>**
- **slamon server ip address {A.B.C.D}**
- **slamon server ip address {A.B.C.D} {A.B.C.D}**
- **slamon server port <0-65535>**
- **slamon server port <0-65535> <0-65535>**

## Command Parameters

**ip address {A.B.C.D} {A.B.C.D}**

Restricts the SLA Mon agent to use one of this SLA Mon server IP address only. The default is 0.0.0.0, which means the agent can register with any server. The second {A.B.C.D} represents an optional secondary server. Omit this parameter if you use only one server.

**port <0-65535> <0-65535>**

Restricts the SLA Mon agent to use one of this registration port only. The default is 0, which means the agent disregards the source port information in server traffic. The SLA Mon server

must use the same port. The second <0-65535> represents the UDP port for an optional secondary server. Omit this parameter if you use only one server.

## Default

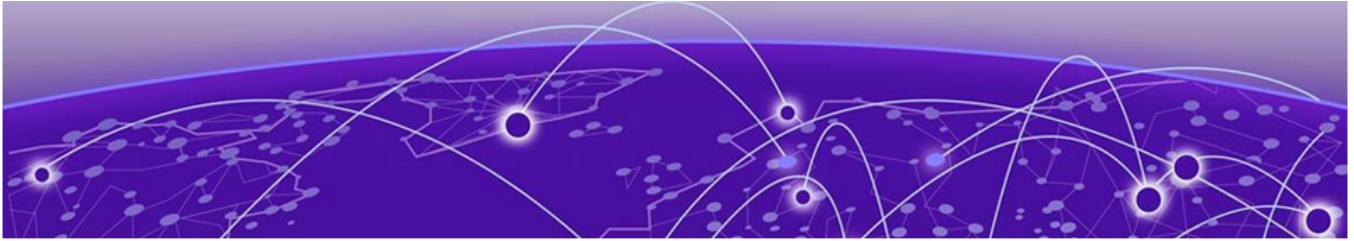
None

## Command Mode

Application Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



# BFD Router Configuration

---

The following topics document commands available in BFD Router Configuration mode of the command line interface (CLI).

## traps

---

Enables traps for Bidirectional Forwarding Detection (BFD).

### Syntax

- **default traps**
- **no traps [enable]**
- **traps [enable]**

### Command Parameters

**enable**

Enables traps.

### Default

The default is disabled.

### Command Mode

BFD Router Configuration



# BGP Router Configuration

---

The following topics document commands available in BGP Router Configuration mode of the command line interface (CLI).

## aggregate-address

---

Add or delete an aggregate address in a BGP routing table.

### Syntax

- `aggregate-address WORD<1-256>`
- `aggregate-address WORD<1-256> advertise-map WORD<0-1536>`
- `aggregate-address WORD<1-256> as-set`
- `aggregate-address WORD<1-256> attribute-map WORD<0-1536>`
- `aggregate-address WORD<1-256> summary-only`
- `aggregate-address WORD<1-256> suppress-map WORD<0-1536>`
- `default aggregate-address WORD<1-256>`
- `default aggregate-address WORD<1-256> advertise-map`
- `default aggregate-address WORD<1-256> as-set`
- `default aggregate-address WORD<1-256> attribute-map`
- `default aggregate-address WORD<1-256> summary-only`
- `default aggregate-address WORD<1-256> suppress-map`
- `no aggregate-address WORD<1-256>`
- `no aggregate-address WORD<1-256> advertise-map WORD<0-1536>`
- `no aggregate-address WORD<1-256> as-set`
- `no aggregate-address WORD<1-256> attribute-map WORD<0-1536>`
- `no aggregate-address WORD<1-256> summary-only`
- `no aggregate-address WORD<1-256> suppress-map WORD<0-1536>`

### Command Parameters

`advertise-map WORD<0-1536>`

Specifies the route map name (any string length between 0 and 64 characters) for route advertisements.

`as-set`

Enables autonomous system (AS) information.

**attribute-map WORD <0-1536>**

Specifies the route map name (string length between 0 and 64 characters).

**summary-only**

Enables the summarization of routes not included in routing updates. This parameter creates the aggregate route and suppresses advertisements of more specific routes to all neighbors. The default value is disable.

**suppress-map WORD<0-1536>**

Specifies the route map name (string length between 0 and 64 characters) for the suppressed route list.

**WORD <1-256>**

Specifies the IPv4 or the IPv6 address and an integer value in the range of 1 to 256.

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

## auto-peer-restart enable

---

Enable the process that automatically restarts a connection to a BGP neighbor.

## Syntax

- **auto-peer-restart enable**
- **default auto-peer-restart**
- **default auto-peer-restart enable**
- **no auto-peer-restart**
- **no auto-peer-restart enable**

## Command Parameters

**enable**

Enables the process that automatically restarts a connection to a BGP neighbor.

## Default

The default value is enable.



## Command Mode

BGP Router Configuration

### auto-summary

---

Summarize the networks based on class limits after BGP is enabled. (For example, Class A, B, C networks).

#### Syntax

- **auto-summary**
- **default auto-summary**
- **no auto-summary**

#### Default

The default value is enable.

## Command Mode

BGP Router Configuration

### bgp aggregation

---

Enables or disables the aggregation feature on the interface.

#### Syntax

- **bgp aggregation**
- **bgp aggregation enable**
- **default bgp aggregation**
- **default bgp aggregation enable**
- **no bgp aggregation**
- **no bgp aggregation enable**

#### Command Parameters

**enable**

Enables the aggregation feature on the interface.

#### Default

The default value is enable.

## Command Mode

BGP Router Configuration

### bgp always-compare-med

---

Enables the comparison of the multiexit discriminator (MED) parameter for paths from neighbors in different autonomous systems. A path with a lower MED is preferred over a path with a higher MED.

#### Syntax

- **bgp always-compare-med**
- **default bgp always-compare-med**
- **no bgp always-compare-med**

#### Default

The default value is disable.

## Command Mode

BGP Router Configuration

### bgp client-to-client reflection

---

Enables or disables route reflection between two route reflector clients. This option is applicable only if the route reflection value is set to enable.

#### Syntax

- **bgp client-to-client reflection**
- **default bgp client-to-client reflection**
- **no bgp client-to-client reflection**

#### Default

The default value is enable.

## Command Mode

BGP Router Configuration

### bgp cluster-id

---

Configures a cluster ID. This option applies only if the route reflection value is set to enable, and if multiple route reflectors are in a cluster.

## Syntax

- **bgp cluster-id {A.B.C.D}**
- **no bgp cluster-id {A.B.C.D}**

## Command Parameters

<A.B.C.D>

Specifies the cluster ID of the reflector router.

## Default

None

## Command Mode

BGP Router Configuration

---

## bgp confederation

Configures a BGP confederation.

## Syntax

- **bgp confederation identifier <0-4294967295>**
- **bgp confederation peers WORD<0-255>**
- **default bgp confederation**
- **default bgp confederation identifier**
- **default bgp confederation peers**
- **no bgp confederation**
- **no bgp confederation identifier**
- **no bgp confederation peers**

## Command Parameters

**identifier <0-4294967295>**

Specifies the confederation identifier. Identifier number 0-65535(2-Byte AS) 0-4294967295(4-Byte AS).

**peers WORD <0-255>**

Lists adjoining Autonomous Systems that are part of the confederation in the format (5500,65535,0,10,.....).

## Default

The default value is 0.

## Command Mode

BGP Router Configuration

### bgp default local-preference

---

Specifies the default value of the local preference attribute. You cannot change the default value when BGP is enabled.

#### Syntax

- **bgp default local-preference <0-2147483647>**
- **default bgp default local-preference**
- **no bgp default local-preference**
- **no bgp default local-preference <0-2147483647>**

#### Command Parameters

<0-2147483647>

Specifies the preference value.

#### Default

The default value is 100.

## Command Mode

BGP Router Configuration

### bgp deterministic-med enable

---

Enables deterministic Multiexit Discriminator (MED).

#### Syntax

- **bgp deterministic-med enable**
- **default bgp deterministic-med**
- **default bgp deterministic-med enable**
- **no bgp deterministic-med**
- **no bgp deterministic-med enable**

#### Default

The default value is enable.

## Command Mode

BGP Router Configuration

### bgp multiple-paths

---

Configures the maximum number of equal-cost-paths that are available to a BGP router by limiting the number of equal-costpaths that can be stored in the routing table.

#### Syntax

- **bgp multiple-paths <1-8>**
- **default bgp multiple-paths**

#### Command Parameters

<1-8>

Specifies the number of equal-cost-paths that are available to a BGP router.

#### Default

The default value is 1.

## Command Mode

BGP Router Configuration

### comp-bestpath-med-confed

---

When enabled, compares multiexit discriminator (MED) attributes within a confederation.

#### Syntax

- **comp-bestpath-med-confed enable**
- **default comp-bestpath-med-confed**
- **default comp-bestpath-med-confed enable**
- **no comp-bestpath-med-confed**
- **no comp-bestpath-med-confed enable**

#### Command Parameters

enable

Enables and compares multiexit discriminator attributes within a BGP confederation.

## Default

The default value is enable.

## Command Mode

BGP Router Configuration

## debug-screen

---

Display debug messages on the console, or saves them in a log file.

## Syntax

- **debug-screen { off | on }**
- **default debug-screen**
- **no debug-screen**

## Command Parameters

<on|off>

Disables BGP screen logging (off) or enable BGP screen logging (on).

## Default

The default value is off.

## Command Mode

BGP Router Configuration

## default-information

---

Enable the advertisement of a default route to peers, if it is present in the routing table.

## Syntax

- **default default-information originate**
- **default-information originate**
- **no default-information originate**

## Command Parameters

**originate**

Enables the origination default route.

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

## default-metric (for BGP)

---

Configure a value that is sent to a BGP neighbor to determine the cost of a route a neighbor is using.

## Syntax

- **default default-metric**
- **default-metric <-1-2147483647>**
- **no default-metric**
- **no default-metric <-1-2147483647>**

## Command Parameters

<-1-2147483647>

Specifies the range of the default metric. A default metric value helps solve the problems associated with redistributing routes that have incompatible metrics.

## Default

The default value is -1.

## Command Mode

BGP Router Configuration

## flap-dampening

---

Enable route suppression for routes that flap on and off.

## Syntax

- **default flap-dampening**
- **default flap-dampening enable**
- **flap-dampening**
- **flap-dampening enable**
- **no flap-dampening**
- **no flap-dampening enable**

## Command Parameters

### enable

Enables Border Gateway Protocol (BGP) flap-dampening.

## Default

The default value is enable.

## Command Mode

BGP Router Configuration

## global-debug mask

---

Display specific debug messages for your global BGP configuration.

## Syntax

- **default global-debug mask**
- **global-debug mask WORD<1-100>**
- **no global-debug mask**

## Command Parameters

### mask WORD <1-100>

Specifies one or more mask choices that you enter, separated by commas with no space between choices. For example, [<mask>,<mask>,<mask>...]. Options include:

- none
- all
- error
- packet
- event
- trace
- warning
- state
- init
- filter
- update

## Default

None



## Command Mode

BGP Router Configuration

### ibgp-report-import-rt

---

Configure BGP to advertise imported routes to an interior BGP (IBGP) peer. This command Enable or disables the advertisement of nonBGP imported routes to other IBGP neighbors.

#### Syntax

- **default ibgp-report-import-rt**
- **default ibgp-report-import-rt enable**
- **ibgp-report-import-rt enable**
- **no ibgp-report-import-rt**
- **no ibgp-report-import-rt enable**

#### Command Parameters

**enable**

Enables advertisement of non BGP imported routes to other IBGP neighbors.

#### Default

The default value is enable.

## Command Mode

BGP Router Configuration

### ignore-illegal-rtrid

---

Overlook an illegal router id after enabling BGP.

#### Syntax

- **default ignore-illegal-rtrid**
- **default ignore-illegal-rtrid enable**
- **ignore-illegal-rtrid enable**
- **no ignore-illegal-rtrid**
- **no ignore-illegal-rtrid enable**

#### Command Parameters

**enable**

Enables or disables the acceptance of a connection from a peer that sends an open message using a router ID of 0 (zero).

## Default

The default value is enable.

## Command Mode

BGP Router Configuration

---

## neighbor password

Configure a BGP peer or peer group password for Transmission Control Protocol (TCP) MD5 authentication between two peers.

## Syntax

- **default neighbor password** <nbr\_ipaddr|peer-group-name> WORD<0-1536>
- **neighbor password** <nbr\_ipaddr|peer-group-name> WORD<0-1536>
- **no neighbor password** <nbr\_ipaddr|peer-group-name> WORD<0-1536>

## Command Parameters

<nbr\_ipaddr|peer-group-name> WORD <0-1536>

Specifies a password for TCP MD5 authentication between two peers. WORD <0-1536> is an alphanumeric string length from 0 to 1536 characters.

To disable this option, use no operator with the command.

To configure this option to the default value, use default operator with the command.

## Default

None

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536>

Create a peer or peer group.

## Syntax

- **default neighbor** WORD<0-1536>
- **neighbor** WORD<0-1536>

- `no neighbor WORD<0-1536>`

## Default

None

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> address-family

Enables BGP address families for IPv6 or IPv4 (BGP) and L3 VPN (MP-BGP) support.

## Syntax

- `default neighbor WORD<0-1536> address-family ipv6`
- `default neighbor WORD<0-1536> address-family vpnv4`
- `neighbor WORD<0-1536> address-family ipv6`
- `neighbor WORD<0-1536> address-family vpnv4`
- `no neighbor WORD<0-1536> address-family ipv6`
- `no neighbor WORD<0-1536> address-family vpnv4`

## Default

None

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> advertisement-interval <5-120>

Specifies the time interval (in seconds) that transpires between each transmission of an advertisement from a BGP neighbor.

## Syntax

- `default neighbor WORD<0-1536> advertisement-interval`
- `neighbor WORD<0-1536> advertisement-interval <5-120>`

## Default

The default value is 5 seconds.

## Command Mode

BGP Router Configuration

### neighbor WORD<0-1536> default-ipv6-originate

---

Enables IPv6 BGP neighbor default originate.

## Syntax

- **default neighbor WORD<0-1536> default-ipv6-originate**
- **neighbor WORD<0-1536> default-ipv6-originate**
- **no neighbor WORD<0-1536> default-ipv6-originate**

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

### neighbor WORD<0-1536> default-originate

---

Enables the switch to send a default route advertisement to the specified neighbor. A default route does not have to be in the routing table. Do not use this command if you globally enable default-information originate.

## Syntax

- **default neighbor WORD<0-1536> default-originate**
- **neighbor WORD<0-1536> default-originate**
- **no neighbor WORD<0-1536> default-originate**

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

### neighbor WORD<0-1536> ebgp-multihop

---

Enables a connection to a Border Gateway Protocol (BGP) peer that is more than one hop away from the local router.

## Syntax

- **default neighbor WORD<0-1536> ebgp-multihop**
- **neighbor WORD<0-1536> ebgp-multihop**
- **no neighbor WORD<0-1536> ebgp-multihop**

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> enable

Enables the Border Gateway Protocol (BGP) neighbor.

## Syntax

- **default neighbor WORD<0-1536> enable**
- **neighbor WORD<0-1536> enable**
- **no neighbor WORD<0-1536> enable**

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

---

## neighbor word<0-1536> fall-over bfd

Enables Bidirectional Forwarding Detection (BFD) for BGP.

## Syntax

- **neighbor word<0-1536> fall-over bfd**
- **no neighbor word<0-1536> fall-over bfd**

## Command Parameters

**word<0-1536>**

Specifies the peer IP address or the peer group name.

## Default

The default is disable.

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> in-route-map WORD<0-256>

Applies a route policy rule to all incoming routes that are learned from, or sent to, the local BGP router peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates.

## Syntax

- **default neighbor WORD<0-1536> in-route-map**
- **neighbor WORD<0-1536> in-route-map WORD<0-256>**
- **no neighbor WORD<0-1536> in-route-map**

## Command Parameters

WORD<0-256>

Specifies an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.

## Default

None

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> ipv6-in-route-map WORD<0-256>

Creates IPv6 in route map.

## Syntax

- **default neighbor WORD<0-1536> ipv6-in-route-map**
- **neighbor WORD<0-1536> ipv6-in-route-map WORD<0-256>**
- **no neighbor WORD<0-1536> ipv6-in-route-map**

## Command Parameters

WORD <0-256>

Specifies the route map or policy name in an alphanumeric string.

## Default

None

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> ipv6-out-route-map WORD<0-256>

Applies a route policy to all outgoing routes.

## Syntax

- **default neighbor WORD<0-1536> ipv6-out-route-map**
- **default neighbor WORD<0-1536> ipv6-out-route-map**
- **neighbor WORD<0-1536> ipv6-out-route-map WORD<0-256>**
- **neighbor WORD<0-1536> ipv6-out-route-map WORD<0-256>**
- **no neighbor WORD<0-1536> ipv6-out-route-map**
- **no neighbor WORD<0-1536> ipv6-out-route-map**

## Command Parameters

**WORD<0-1536>**

Specifies the subscriber group. You must create the specified subscriber group before you issue this command.

**WORD<0-256>**

WORD<0-256> name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.

## Default

None

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> max-prefix <0-2147483647>

Sets a limit on the number of routes that can be accepted from a neighbor.

## Syntax

- **default neighbor WORD<0-1536> max-prefix**
- **neighbor WORD<0-1536> max-prefix <0-2147483647>**

## Command Parameters

<0-2147483647>

Sets a limit on the number of routes that can be accepted from a neighbor. A value of 0 (zero) indicates that there is no limit to the number of routes that can be accepted.

## Default

The default value is 12000 routes

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> MD5-authentication enable

Enables TCP MD5 authentication between two peers.

## Syntax

- **default neighbor WORD<0-1536> MD5-authentication enable**
- **neighbor WORD<0-1536> MD5-authentication enable**
- **no neighbor WORD<0-1536> MD5-authentication enable**

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> neighbor-debug-mask WORD<1-100>

Displays specified debug information for a BGP peer.

## Syntax

- **default neighbor WORD<0-1536> neighbor-debug-mask**
- **neighbor WORD<0-1536> neighbor-debug-mask WORD<1-100>**
- **no neighbor WORD<0-1536> neighbor-debug-mask**



## Command Parameters

### WORD<1-100>

WORD<1-100> is a list of mask choices separated by commas with no space between choices. For example, {<mask>,<mask>,<mask>...}. Mask choices are

- none - disables all debug messages
- all - enables all debug messages
- error - enables display of debug error messages
- packet - enables display of debug packet messages
- event - enables display of debug event messages
- trace - enables display of debug trace messages
- warning - enables display of debug warning messages
- state - enables display of debug state transition messages
- init - enables display of debug initialization messages
- filter - enables display of debug messages related to filtering
- update - enables display of debug messages related to sending and receiving updates

## Default

The default value is none.

## Command Mode

BGP Router Configuration

## neighbor WORD<0-1536> next-hop-self

---

When enabled, specifies that the next-hop attribute in an IBGP update is the address of the local router or the router that is generating the IBGP update. You can only configure the next-hop parameter if the neighbor is disabled.

## Syntax

- **default neighbor WORD<0-1536> next-hop-self**
- **neighbor WORD<0-1536> next-hop-self**
- **no neighbor WORD<0-1536> next-hop-self**

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> out-route-map WORD<0-256>

---

Applies a route policy rule to all outgoing routes that are learned from, or sent to, the local peers or peer groups, of the BGP router. The local BGP router is the BGP router that allows or disallows routes, and sets attributes in incoming or outgoing updates.

### Syntax

- **default neighbor WORD<0-1536> out-route-map**
- **neighbor WORD<0-1536> out-route-map WORD<0-256>**
- **no neighbor WORD<0-1536> out-route-map**

### Command Parameters

WORD<0-1536>

Specifies the neighbor IP address {a.b.c.d}, IPv6 address, or neighbor group name.

WORD<0-256>

WORD<0-256> name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.

### Default

None

### Command Mode

BGP Router Configuration

---

## neighbor WORD<0-1536> peer-group WORD<0-1536>

---

Adds a Border Gateway Protocol (BGP) peer to the specified subscriber group. You must create the specified subscriber group before you issue this command.

### Syntax

- **neighbor WORD<0-1536> peer-group WORD<0-1536>**
- **no neighbor WORD<0-1536> peer-group**

### Command Parameters

WORD<0-1536>

Specifies the subscriber group. You must create the specified subscriber group before you issue this command.

## Default

None

## Command Mode

BGP Router Configuration

## neighbor WORD<0-1536> remote-as WORD<0-11>

---

Configures the remote AS number of a Border Gateway Protocol (BGP) peer or a peer-group. You cannot configure this option when the admin-state is enable.

## Syntax

- **default neighbor WORD<0-1536> remote-as**
- **neighbor WORD<0-1536> remote-as WORD<0-11>**
- **no neighbor WORD<0-1536> remote-as**

## Command Parameters

WORD<0-11>

Specifies the remote AS number of a peer or a peer-group.

## Default

None

## Command Mode

BGP Router Configuration

## neighbor WORD<0-1536> remove-private-as enable

---

When enabled, strips private AS numbers when an update is sent. This feature is especially useful within a confederation.

## Syntax

- **default neighbor WORD<0-1536> remove-private-as enable**
- **neighbor WORD<0-1536> remove-private-as enable**
- **no neighbor WORD<0-1536> remove-private-as enable**

## Default

The default value is enable.

## Command Mode

BGP Router Configuration

### neighbor WORD<0-1536> retry-interval <1-65535>

---

Configures the time interval (in seconds) for the ConnectRetry Timer.

#### Syntax

- **default neighbor WORD<0-1536> retry-interval**
- **neighbor WORD<0-1536> retry-interval <1-65535>**

#### Default

The default value is 120 seconds.

## Command Mode

BGP Router Configuration

### neighbor WORD<0-1536> route-reflector-client

---

Configures the specified neighbor or group of neighbors as its route reflector client. All neighbors that are configured become members of the client group and the remaining IBGP peers become members of the nonclient group for the local route reflector.

#### Syntax

- **neighbor WORD<0-1536> route-reflector-client**
- **no neighbor WORD<0-1536> route-reflector-client**

#### Default

The default value is disable.

## Command Mode

BGP Router Configuration

### neighbor WORD<0-1536> route-refresh

---

Enables IP VPN Route Refresh for the Border Gateway Protocol (BGP) peer. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request.

## Syntax

- **default neighbor WORD<0-1536> route-refresh**
- **neighbor WORD<0-1536> route-refresh**
- **no neighbor WORD<0-1536> route-refresh**

## Default

The default value is disable

## Command Mode

BGP Router Configuration

## neighbor WORD<0-1536> send-community

---

Enables the switch to send the update message community attribute to the specified peer.

## Syntax

- **default neighbor WORD<0-1536> send-community**
- **neighbor WORD<0-1536> send-community**
- **no neighbor WORD<0-1536> send-community**

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

## neighbor WORD<0-1536> soft-reconfiguration-in enable

---

When enabled, the router relearns routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction.

## Syntax

- **default neighbor WORD<0-1536> soft-reconfiguration-in enable**
- **neighbor WORD<0-1536> soft-reconfiguration-in enable**
- **no neighbor WORD<0-1536> soft-reconfiguration-in enable**

## Default

The default value is disable.

## Command Mode

BGP Router Configuration

## neighbor WORD<0-1536> timers

---

Configures timers (in seconds) for the Border Gateway Protocol (BGP) speaker for this peer.

### Syntax

- **default neighbor WORD<0-1536> timers**
- **neighbor WORD<0-1536> timers <0-21845> <0-65535>**

### Command Parameters

<0-21845>

<0-21845> is the keepalive time. The default is 60.

<0-65535>

<0-65535> is the hold time. The default is 180.

### Default

None

## Command Mode

BGP Router Configuration

## neighbor WORD<0-1536> update-source

---

Specifies the source IP address when Border Gateway Protocol (BGP) packets are sent to this peer or peer group. You cannot configure this parameter when the admin-state is enable.

### Syntax

- **default neighbor WORD<0-1536> update-source**
- **neighbor WORD<0-1536> update-source WORD<1-256>**
- **no neighbor WORD<0-1536> update-source**

### Command Parameters

<A.B.C.D>

<A.B.C.D> is the specified source IP address.

## Default

None

## Command Mode

BGP Router Configuration

## neighbor WORD<0-1536> weight

---

Specifies the weight of a Border Gateway Protocol (BGP) peer or peer groups, or the priority of updates that can be received from that BGP peer.

## Syntax

- **default neighbor WORD<0-1536> weight**
- **neighbor WORD<0-1536> weight <0-65535>**
- **no neighbor WORD<0-1536> weight**

## Command Parameters

<0-65535>

Specifies the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer.

If you have particular neighbors that you want to prefer for most of your traffic, you can assign a higher weight to all routes learned from that neighbor.

## Default

The default value is 0.

## Command Mode

BGP Router Configuration

## neighbor-debug-all

---

Display specified debug information for BGP neighbors.

## Syntax

- **default neighbor-debug-all**
- **neighbor-debug-all mask WORD<1-100>**
- **no neighbor-debug-all**

## Command Parameters

**mask** <WORD 1-100>

<WORD 1-100> is a list of mask choices separated by commas with no space between choices.

## Default

The default value is none.

## Command Mode

BGP Router Configuration

## network (for BGP)

---

Specify the Interior Gateway Protocol (IGP) network prefixes for Border Gateway Protocol (BGP) to advertise for redistribution.

## Syntax

- **default network** WORD<1-256>
- **network** WORD<1-256>
- **network** WORD<1-256> **metric** <0-65535>
- **no network** WORD<1-256>

## Command Parameters

**metric** <0-65535>

Specifies the metric to use when the system sends an update for the routes in the network table. The metric configures the MED for the routes advertised to EBGp peers. The range is 0–65535.

**WORD** <1-256>

Specifies IGP network prefixes for Border Gateway Protocol (BGP) to advertise for redistribution. This command imports routes into BGP. WORD <1-256> is the IPv4 or the IPv6 network address and mask.

## Default

None

## Command Mode

BGP Router Configuration

## no-med-path-is-worst

---

Enable Border Gateway Protocol (BGP) to treat an update without a multiexit discriminator (MED) attribute as the worst path.



## Syntax

- `default no-med-path-is-worst`
- `default no-med-path-is-worst enable`
- `no no-med-path-is-worst`
- `no no-med-path-is-worst enable`
- `no-med-path-is-worst enable`

## Command Parameters

`enable`

Enables Border Gateway Protocol (BGP) to treat an update without a multiexit discriminator (MED) attribute as the worst path.

## Default

The default value is `enable`.

## Command Mode

BGP Router Configuration

---

## quick-start

Enable the quick-start flag for exponential backoff.

## Syntax

- `default quick-start`
- `default quick-start enable`
- `default quick-start enable`
- `no quick-start`
- `no quick-start enable`
- `quick-start enable`

## Command Parameters

`enable`

Enables the quick-start flag for exponential backoff.

## Default

The default value is `enable`.

## Command Mode

BGP Router Configuration

## redistribute direct (for BGP)

---

Redistribute routes learned from directly-connected networks into Border Gateway Protocol (BGP).

### Syntax

- `default redistribute direct`
- `default redistribute direct enable`
- `default redistribute direct metric`
- `default redistribute direct metric-type`
- `default redistribute direct route-map`
- `default redistribute direct vrf-src WORD<1-16>`
- `no redistribute direct`
- `no redistribute direct enable`
- `no redistribute direct vrf-src WORD<1-16>`
- `redistribute direct`
- `redistribute direct enable`
- `redistribute direct metric <0-65535>`
- `redistribute direct metric-type live-metric`
- `redistribute direct route-map WORD<0-64>`
- `redistribute direct vrf-src WORD<1-16>`

### Command Parameters

`enable`

Enables the redistribution.

`metric <0-65535>`

Specifies the value of the metric to be announced in the advertisement. The default is 0.

`metric-type live-metric`

Configures the route redistribution metric type. The default is disabled.

`route-map WORD<0-64>`

Configures the route policy to apply to redistributed routes.

`vrf-src WORD<1-16>`

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

## redistribute dvr (for BGP)

---

Redistribute DvR-learned routes into Border Gateway Protocol (BGP).

## Syntax

- `default redistribute dvr`
- `default redistribute dvr enable`
- `default redistribute dvr metric`
- `default redistribute dvr metric-type`
- `default redistribute dvr route-map`
- `default redistribute dvr vrf-src WORD<1-16>`
- `no redistribute dvr`
- `no redistribute dvr enable`
- `no redistribute dvr vrf-src WORD<1-16>`
- `redistribute dvr`
- `redistribute dvr enable`
- `redistribute dvr metric <0-65535>`
- `redistribute dvr metric-type live-metric`
- `redistribute dvr route-map WORD<0-64>`
- `redistribute dvr vrf-src WORD<1-16>`

## Command Parameters

### enable

Enables the redistribution.

### metric <0-65535>

Specifies the value of the metric to be announced in the advertisement. The default is 0.

### metric-type live-metric

Configures the route redistribution metric type. The default is disabled.

### route-map WORD<0-64>

Configures the route policy to apply to redistributed routes.

### vrf-src WORD<1-16>

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

## redistribute ipv6-direct (for BGP)

---

Redistribute routes learned from IPv6 directly-connected networks into Border Gateway Protocol (BGP).

## Syntax

- **default redistribute ipv6-direct metric-type**
- **default redistribute ipv6-direct**
- **default redistribute ipv6-direct enable**
- **default redistribute ipv6-direct metric**
- **default redistribute ipv6-direct route-map**
- **no redistribute ipv6-direct**
- **no redistribute ipv6-direct enable**
- **no redistribute ipv6-direct route-map**
- **redistribute ipv6-direct**
- **redistribute ipv6-direct enable**
- **redistribute ipv6-direct metric <0-65535>**
- **redistribute ipv6-direct metric-type live-metric**
- **redistribute ipv6-direct route-map WORD<0-64>**

## Command Parameters

**enable**

Enables the redistribution.

**metric <0-65535>**

Specifies the value of the metric to be announced in the advertisement. The default is 0.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

## redistribute ipv6-isis enable

---

Enables the BGP route redistribution instance.

## Syntax

- **default redistribute ipv6-isis enable**
- **no redistribute ipv6-isis enable**
- **redistribute ipv6-isis enable**

## Default

The default is none.

## Command Mode

BGP Router Configuration

## redistribute ipv6-isis metric

---

Configure the metric to apply to redistributed routes.

## Syntax

- **default redistribute ipv6-isis metric**
- **redistribute ipv6-isis metric <0-65535>**

## Command Parameters

**<0-65535>**

Specifies the BGP metric.

## Default

The default value is 0.

## Command Mode

BGP Router Configuration

---

## redistribute ipv6-isis route-map

---

Configure the route policy to apply to redistributed routes.

### Syntax

- **default redistribute ipv6-isis route-map**
- **no redistribute ipv6-isis route-map**
- **redistribute ipv6-isis route-map WORD<0-64>**

### Command Parameters

WORD<0-64>

Specifies the route policy name.

### Default

The default value is 0.

### Command Mode

BGP Router Configuration

---

## redistribute ipv6-static (for BGP)

---

Redistribute IPv6 static routes into Border Gateway Protocol (BGP).

### Syntax

- **default redistribute ipv6-static**
- **default redistribute ipv6-static enable**
- **default redistribute ipv6-static metric**
- **default redistribute ipv6-static route-map**
- **no redistribute ipv6-static**
- **no redistribute ipv6-static enable**
- **no redistribute ipv6-static route-map**
- **redistribute ipv6-static**
- **redistribute ipv6-static enable**
- **redistribute ipv6-static metric <0-65535>**
- **redistribute ipv6-static route-map WORD<0-64>**

### Command Parameters

enable

Enables the redistribution.

**metric <0-65535>**

Specifies the value of the metric to be announced in the advertisement. The default is 0.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

## redistribute isis (for BGP)

---

Redistribute learned routes into Border Gateway Protocol (BGP).

## Syntax

- **default redistribute isis**
- **default redistribute isis enable**
- **default redistribute isis metric**
- **default redistribute isis metric-type**
- **default redistribute isis route-map**
- **default redistribute isis vrf-src WORD<1-16>**
- **no redistribute isis**
- **no redistribute isis enable**
- **redistribute isis**
- **redistribute isis enable**
- **redistribute isis metric <0-65535>**
- **redistribute isis metric-type live-metric**
- **redistribute isis route-map WORD<0-64>**
- **redistribute isis vrf-src WORD<1-16>**

## Command Parameters

**enable**

Enables the redistribution of Intermediate-System-to-Intermediate-System (IS-IS) learned IP routes into BGP.

**metric <0-65535>**

Specifies the value of the metric to be announced in the advertisement. The default is 1.

**metric-type live-metric**

Configures the route redistribution metric type. The default is disabled.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

**vrf-src WORD<1-16>**

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

## redistribute ospf (for BGP)

---

Redistribute OSPF-learned routes into Border Gateway Protocol (BGP).

## Syntax

- **default redistribute ospf**
- **default redistribute ospf enable**
- **default redistribute ospf metric**
- **default redistribute ospf metric-type**
- **default redistribute ospf route-map**
- **default redistribute ospf vrf-src WORD<1-16>**
- **no redistribute ospf**
- **no redistribute ospf enable**
- **no redistribute ospf vrf-src WORD<1-16>**
- **redistribute ospf**
- **redistribute ospf enable**
- **redistribute ospf metric <0-65535>**
- **redistribute ospf metric-type live-metric**
- **redistribute ospf route-map WORD<0-64>**
- **redistribute ospf vrf-src WORD<1-16>**

## Command Parameters

**enable**

Enables the redistribution.



**metric <0-65535>**

Specifies the value of the metric to be announced in the advertisement. The default is 0.

**metric-type live-metric**

Configures the route redistribution metric type. The default is disabled.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

**vrf-src WORD<1-16>**

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

## redistribute ospfv3 (for BGP)

---

Redistribute OSPFv3-learned routes into Border Gateway Protocol (BGP).

## Syntax

- **default redistribute ospfv3**
- **default redistribute ospfv3 enable**
- **default redistribute ospfv3 metric**
- **default redistribute ospfv3 route-map**
- **no redistribute ospfv3**
- **no redistribute ospfv3 enable**
- **no redistribute ospfv3 route-map**
- **redistribute ospfv3**
- **redistribute ospfv3 enable**
- **redistribute ospfv3 metric <0-65535>**
- **redistribute ospfv3 route-map WORD<0-64>**

## Command Parameters

**enable**

Enables the redistribution.

**metric <0-65535>**

Specifies the value of the metric to be announced in the advertisement. The default is 0.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

## redistribute rip (for BGP)

---

Redistribute RIP-learned routes into Border Gateway Protocol (BGP).

## Syntax

- **default redistribute rip**
- **default redistribute rip enable**
- **default redistribute rip metric**
- **default redistribute rip metric-type**
- **default redistribute rip route-map**
- **default redistribute rip vrf-src WORD<1-16>**
- **no redistribute rip**
- **no redistribute rip enable**
- **no redistribute rip vrf-src WORD<1-16>**
- **redistribute rip**
- **redistribute rip enable**
- **redistribute rip metric <0-65535>**
- **redistribute rip metric-type live-metric**
- **redistribute rip route-map WORD<0-64>**
- **redistribute rip vrf-src WORD<1-16>**

## Command Parameters

**enable**

Enables the redistribution.

**metric <0-65535>**

Specifies the value of the metric to be announced in the advertisement. The default is 0.

**metric-type live-metric**

Configures the route redistribution metric type. The default is disabled.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

**vrf-src WORD<1-16>**

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

---

## redistribute ripng enable

Enable the BGP redistribution RIPng.

## Syntax

- **default redistribute ripng enable**
- **no redistribute ripng enable**
- **redistribute ripng enable**

## Default

None

## Command Mode

BGP Router Configuration

---

## redistribute ripng metric

Configure the metric to apply to redistributed routes.

## Syntax

- **default redistribute ripng metric**
- **redistribute ripng metric <0-65535>**

## Command Parameters

**<0-65535>**

Specifies the BGP route distribution metric.

## Default

The default value is 0.

## Command Mode

BGP Router Configuration

---

## redistribute ripng route-map

Configure the route policy to apply to redistributed routes.

## Syntax

- **default redistribute ripng route-map**
- **no redistribute ripng route-map**
- **redistribute ripng route-map WORD<0-64>**

## Command Parameters

WORD<0-64>

Specifies the route policy name.

## Default

The default value is 0.

## Command Mode

BGP Router Configuration

---

## redistribute static (for BGP)

Redistribute static routes into Border Gateway Protocol (BGP).

## Syntax

- **default redistribute static**
- **default redistribute static enable**
- **default redistribute static metric**
- **default redistribute static metric-type**
- **default redistribute static route-map**
- **default redistribute static vrf-src WORD<1-16>**
- **no redistribute static**
- **no redistribute static enable**

- `no redistribute static vrf-src WORD<1-16>`
- `redistribute static`
- `redistribute static enable`
- `redistribute static metric <0-65535>`
- `redistribute static metric-type live metric`
- `redistribute static route-map WORD<0-64>`
- `redistribute static vrf-src WORD<1-16>`

## Command Parameters

### `enable`

Enables the redistribution.

### `metric <0-65535>`

Specifies the value of the metric to be announced in the advertisement. The default is 0.

### `metric-type live-metric`

Configures the route redistribution metric type. The default is disabled.

### `route-map WORD<0-64>`

Configures the route policy to apply to redistributed routes.

### `vrf-src WORD<1-16>`

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

By default, route redistribution is disabled.

## Command Mode

BGP Router Configuration

## route-reflector enable

---

Enable the reflection of routes from IBGP neighbors.

## Syntax

- `default route-reflector`
- `default route-reflector enable`
- `no route-reflector`
- `no route-reflector enable`
- `route-reflector`
- `route-reflector enable`

## Command Parameters

### enable

Enables route-reflector to reflect routers from iBGP neighbors.

## Default

The default value is enable.

## Command Mode

BGP Router Configuration

---

## route-refresh

Enable or disable IP VPN Route Refresh. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request.

## Syntax

- **default route-refresh**
- **no route-refresh**
- **route-refresh**

## Default

The default value is disable

## Command Mode

BGP Router Configuration

---

## router-id (for BGP)

Specify the BGP router ID in IP address format.

## Syntax

- **default router-id**
- **no router-id**
- **router-id {A.B.C.D}**

## Command Parameters

### <A.B.C.D>

Identifies the router IP address.

## Default

None

## Command Mode

BGP Router Configuration

## synchronization

---

Enable the router to accept routes from BGP peers without waiting for an update from the IGP.

## Syntax

- **default synchronization**
- **no synchronization**
- **synchronization**

## Default

The default value is enable.

## Command Mode

BGP Router Configuration

## traps

---

Enable BGP traps.

## Syntax

- **default traps**
- **default traps enable**
- **no traps**
- **no traps enable**
- **traps enable**

## Command Parameters

**enable**

Enables BGP traps.

## Default

The default value is disable.

## Command Mode

BGP Router Configuration





# DHCP-guard Configuration

---

The following topics document commands available in DHCP-guard Configuration mode of the command line interface (CLI).

## match reply prefix-list

---

Enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. An empty prefix list is treated as a permit.

### Syntax

- **default match reply prefix-list**
- **match reply prefix-list WORD<1-64>**
- **no match reply prefix-list**

### Command Parameters

**WORD<1-64>**

Specifies the prefix list name.

### Default

None

### Command Mode

DHCP-guard Configuration

## match server access-list

---

Enables the verification of sender IPv6 address in inspected messages.

### Syntax

- **default match server access-list**
- **match server access-list WORD<1-64>**
- **no match server access-list**

## Command Parameters

**WORD<1-64>**

Specifies the access list name.

## Default

None

## Command Mode

DHCP-guard Configuration

## preference max-limit

---

Enables verification that the advertised preference is less than the specified limit. If not specified, this check will be bypassed.

## Syntax

- **default preference max-limit**
- **preference max-limit <0-255>**

## Command Parameters

**<0-255>**

Specifies the maximum limit value.

## Default

None

## Command Mode

DHCP-guard Configuration

## preference min-limit

---

Enables verification that the advertised preference is greater than the specified limit. If not specified, this check will be bypassed.

## Syntax

- **default preference min-limit**
- **preference min-limit <0-255>**

## Command Parameters

<0-255>

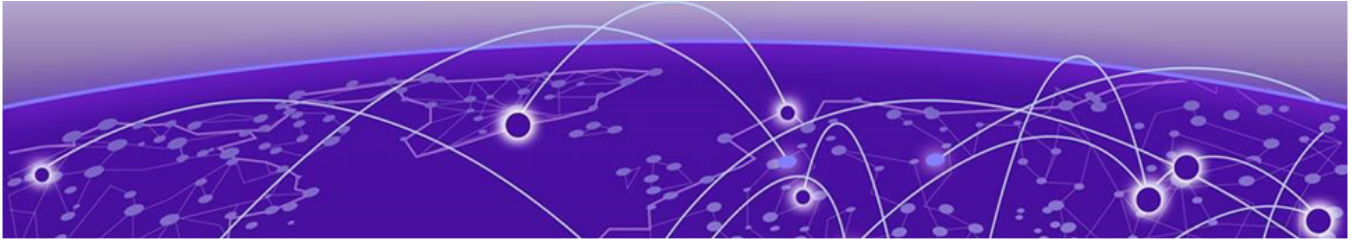
Specifies the minimum limit value.

## Default

None

## Command Mode

DHCP-guard Configuration



# Elan I-SID Configuration

---

The following topics document commands available in Elan I-SID Configuration mode of the command line interface (CLI).

## c-vid (for an mlt)

---

Associate (VID, mlt) end points to the Switched UNI (S-UNI) service instance identifiers (I-SID).

### Syntax

- **c-vid** *<c-vid>* **mlt** *<1-512>*
- **no c-vid** *<c-vid>* **mlt** *<1-512>*

### Command Parameters

*<c-vid>*

Specifies the customer VLAN ID. Different hardware platforms support different customer VLAN ID ranges. Use the CLI Help to see the available range for the switch.

**mlt** *<1-512>*

Add mlt to Elan-based service.

### Default

None

### Command Mode

Elan I-SID Configuration

## c-vid (for a port)

---

Associate (VID, portList) end points to the Switched UNI (S-UNI) service instance identifiers (I-SID).

### Syntax

- **c-vid** *<c-vid>* **port** {**slot/port**[/sub-port] [-**slot/port**[/sub-port]] [,...]}
- **no c-vid** *<c-vid>* **port** {**slot/port**[/sub-port] [-**slot/port**[/sub-port]] [,...]}

## Command Parameters

`<c-vid>`

Specifies the customer VLAN ID. Different hardware platforms support different customer VLAN ID ranges. Use the CLI Help to see the available range for the switch.

**port** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Add ports to Elan-based service.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Elan I-SID Configuration

---

## untagged-traffic (for an mlt)

Associate (VID, mlt) end points to the Switched UNI (S-UNI) service instance identifiers (I-SID).

## Syntax

- **no untagged-traffic mlt <1-512> [bpdu enable]**
- **untagged-traffic mlt <1-512> [bpdu enable]**

## Command Parameters

**bpdu**

Set bpdu forwarding.

**enable**

Enable bpdu forwarding.

**mlt <1-512>**

Add mlt to Elan-based service.

## Default

None

## Command Mode

Elan I-SID Configuration

---

## untagged-traffic (for a port)

---

Associate (VID, portList) end points to the Switched UNI (S-UNI) service instance identifiers (I-SID).

### Syntax

- **no untagged-traffic port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} [bpdu enable]
- **untagged-traffic port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} [bpdu enable]

### Command Parameters

#### bpdu

Set bpdu forwarding.

#### enable

Enable bpdu forwarding.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

Elan I-SID Configuration



# Elan-Transparent Configuration

---

The following topics document commands available in Elan-Transparent Configuration mode of the command line interface (CLI).

## mlt (T-UNI based)

---

Add MLT to elan-transparent (Transparent Port UNI) based service instance identifier (I-SID).

### Syntax

- **mlt** <1-512>
- **no mlt** <1-512>

### Command Parameters

<1-512>

Specifies the MLT ID in the range of 1-512 of the mlt being added to (or removed from) the Transparent Port UNI based service instance identifier (I-SID).

### Default

None

### Command Mode

Elan-Transparent Configuration

## port (T-UNI based)

---

Add ports to elan-transparent (Transparent Port UNI) based service instance identifier (I-SID).

### Syntax

- **no port** <{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}>
- **port** <{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}>

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Elan-Transparent Configuration





# Fabric IPsec Gateway Configuration

---

The following topics document commands available in Fabric IPsec Gateway Configuration mode of the command line interface (CLI).

## certificate ca <ca-trustpoint>

---

Configures certificate authority (CA) trustpoint actions on Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **certificate ca <ca-trustpoint> {caAuth | clean | enroll <subject-label> | remove <subject-label>}**

### Command Parameters

**ca <ca-trustpoint>**

Specifies the certificate authority (CA) trustpoint.

**caAuth**

Configures the trustpoint, authenticates the trustpoint CA by getting the certificate of the CA, and stores the CA certificate locally.

**clean**

Removes all certificates from the CA trustpoint.

**enroll <subject-label>**

Generates the certificate enrollment request, get the digital certificate, and store it locally, associating with the trustpoint CA.

**remove <subject-label>**

Releases the locally stored certificate associated with the trustpoint CA post revocation.

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## certificate generate

---

Generates a key or certificate signing request (CSR) on Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **certificate generate {csr <subject-label> | key <type> <size> <key-label>}**

### Command Parameters

**csr <subject-label>**

Generates a CSR and stores it in a file.

**key <type> <size> <key-label>**

Generates the private and public key pair for the specific cryptography type. By default, VOSS generates a 2,048 RSA key when the system starts. Use this parameter to generate a new key.

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## certificate get

---

Specifies the location from which to obtain certificates for Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **certificate get cacert-from <A.B.C.D> <user> <file-path>**
- **certificate get crl-from <A.B.C.D> <user> <file-path> <cacert-filename>**
- **certificate get signedcert-from <A.B.C.D> <user> <file-path> <subject-label>**

## Command Parameters

**cacert-from** <A.B.C.D> <user> <file-path>

Specifies where to obtain the CA certificate. Specify the IP address, username, and remote file path.

**crl-from** <A.B.C.D> <user> <file-path> <cacert-filename>

Specifies where to obtain the Certificate Revocation List. Specify the IP address, username, remote file path, and the CA certificate file to verify the CRL.

**signedcert-from** <A.B.C.D> <user> <file-path> <subject-label>

Specifies where to obtain the subject certificate. Specify the IP address, username, remote file path, and subject label.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## certificate remove

---

Removes keys or certificates from Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **certificate remove** {**key** <key-label> | **offline-cacert** <filename> | **offline-crl** <filename> | **offline-subject-certs** <subject-label>}

## Command Parameters

**key** <key-label>

Specifies the key name to remove.

**offline-cacert** <filename>

Specifies the certificate filename to remove.

**offline-crl** <filename>

Specifies the Certificate Revocation List (CRL) certificate filename to remove.

**offline-subject-certs** <subject-label>

Specifies the subject label for which to remove signed certificates.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## certificate send-csr-to

Configures where to send the certificate signing request (CSR) for signing for Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **certificate send-csr-to <A.B.C.D> <user> <remote-path> <subject-label>**

## Command Parameters

**<A.B.C.D>**

Specifies the IP address for the certificate authority.

**<remote-path>**

Specifies the file path on the certificate authority.

**<subject-label>**

Specifies the subject identity.

**<user>**

Specifies the username for the certificate authority.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## delete certificate

---

Deletes the certificate configuration on Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **delete certificate ca-trustpoint <ca-label>**
- **delete certificate subject <subject-label>**

### Command Parameters

**ca-trustpoint <ca-label>**

Specifies the certificate authority (CA) trustpoint.

**subject <subject-label>**

Specifies the subject identity.

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## delete global

---

Deletes the parameters that you configure globally on the Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **delete global fe-tunnel-gw-ip**
- **delete global fe-tunnel-src-ip**
- **delete global ipsec-disable**
- **delete global ipsec-tunnel-src-ip**
- **delete global ipsec-tunnel-src-vlan**
- **delete global ipsec-tunnel-src-vlan**
- **delete global lan-intf-gw-ip**
- **delete global lan-intf-ip**
- **delete global lan-intf-vlan**

- **delete global mtu**
- **delete global virtual-reassembly-intf-ip**
- **delete global virtual-reassembly-intf-vlan**
- **delete global wan-intf-gw-ip**

## Command Parameters

### fe-tunnel-gw-ip

Deletes the global gateway IP address for Fabric Extend (FE) tunnel.

### fe-tunnel-src-ip

Deletes the global source IP address for FE tunnel.

### ipsec-disable

Deletes the global IPsec configuration.

### ipsec-tunnel-src-ip

Deletes the global source IP address and subnet mask for IPsec tunnel.

### ipsec-tunnel-src-vlan

Deletes the global source VLAN configuration for IPsec tunnel.

### lan-intf-gw-ip

Deletes the global gateway IP address on the Local Area Network (LAN) interface.

### lan-intf-ip

Deletes the global IP address and subnet mask on LAN interface.

### lan-intf-vlan

Deletes the global VLAN configuration on LAN interface.

### mtu

Resets the Maximum Transmission Unit (MTU) value to its default, that is 1950 bytes.

### virtual-reassembly-intf-ip

Deletes the global virtual-reassembly interface IP address and subnet mask.

### virtual-reassembly-intf-vlan

Deletes the global virtual-reassembly interface VLAN configuration.

### wan-intf-gw-ip

Deletes the global gateway IP address on the Wide Area Network (WAN) interface.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## delete ip route

Deletes an IP route.

## Syntax

- **delete ip route {A.B.C.D/X}**

## Command Parameters

{A.B.C.D/X}

Specifies the IP address and mask of the route to delete.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## delete ipsec

Deletes the configuration of a specific IPsec tunnel on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **delete ipsec <1-255> admin-state enable**
- **delete ipsec <1-255> auth-key**

- **delete ipsec <1-255> cert-subject**
- **delete ipsec <1-255> egress-shaping-rate**
- **delete ipsec <1-255> encryption-key-length**
- **delete ipsec <1-255> esp**
- **delete ipsec <1-255> fe-tunnel-dest-ip**
- **delete ipsec <1-255> fragment-before-encrypt enable**
- **delete ipsec <1-255> ipsec-dest-ip**
- **delete ipsec <1-255> mtu**
- **delete ipsec <1-255> responder-only**
- **delete ipsec <1-255> tunnel-name**

## Command Parameters

### **admin-state enable**

Disables the IPsec status on the specific IPsec tunnel.

### **auth-key**

Deletes the authentication key that you configure on the specific IPsec tunnel.

### **cert-subject**

Removes the certificate subject that you configure on the specific IPsec tunnel.

### **egress-shaping-rate**

Deletes the egress shaping rate for the IPsec tunnel.

### **encryption-key-length**

Resets the encryption key length for the specific IPsec tunnel to its default value, 128 bit.

### **esp**

Removes the ESP cipher suite that you configure on the specific IPsec tunnel.

### **fe-tunnel-dest-ip**

Deletes the destination IP address that you configure on the Fabric Extend (FE) tunnel.

### **fragment-before-encrypt enable**

Disables the fragmentation of packets before IPsec encryption on the tunnel. By default, fragmentation before encryption is disabled.

### **ipsec-dest-ip**

Deletes the destination IP address that you configure on the IPsec tunnel.

### **mtu**

Resets the Maximum Transmission Unit (MTU) value for the specific IPsec tunnel to the MTU value configured globally.

### **responder-only**

Deletes the mode that you configure for the IPsec session in FE tunnel.

### **tunnel-name**



Deletes the name that you configure for the IPsec tunnel.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

You must disable the IPsec administrative state on the tunnel before you can remove IPsec configuration.

## delete logical-intf-tunnel

---

Deletes the configuration of a specific logical interface tunnel on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **delete logical-intf-tunnel <1-255> fe-tunnel-dest-ip**
- **delete logical-intf-tunnel <1-255> mtu**
- **delete logical-intf-tunnel <1-255> egress-shaping-rate**

## Command Parameters

### fe-tunnel-dest-ip

Deletes the destination IP address that you configure on the logical interface tunnel.

### mtu

Resets the Maximum Transmission Unit (MTU) value for the specific logical interface tunnel to the MTU value configured globally.

### egress-shaping-rate

Deletes the egress shaping rate on the logical interface tunnel.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## exit

---

Logs out of the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **exit**

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ftp

---

Configures an FTP connection to a specific IP Address on Extreme Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **ftp {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies the IP Address to establish the FTP connection with.

## Default

None

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## load

---

Loads a configuration file to the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **load WORD <1-255>**

## Command Parameters

WORD <1-255>

Specifies the configuration file name.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ls

---

Lists the files and directories configured on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **ls**

## Default

None

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## more

---

Displays the data in a specific file on Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **more WORD <1-255>**

## Command Parameters

**WORD <1-255>**

Specifies the name of the file

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ping

---

Ping an IP Address on the the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **ping {A.B.C.D}**

## Command Parameters

**{A.B.C.D}**

Specifies the IP address.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## reboot

Reboots the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **reboot**

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## remove

Deletes a file from the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **remove WORD <1-255>**

## Command Parameters

**WORD <1-255>**

Specifies the file name that the system removes from the Fabric IPsec Gateway VM.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## reset-config

Resets the current configuration on Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **reset-config**

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## save config

Saves the current configuration of the Fabric IPsec Gateway Virtual Machine (VM) to a specific file.

## Syntax

- **save config [-y]**
- **save config file WORD <1-255> [-y]**

## Command Parameters

file WORD <1-255>

Specifies the file name to save the current configuration of the Fabric IPsec Gateway Virtual Machine (VM).

**-y**

Forces the switch to overwrite the file without confirmation.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## set certificate ca-trustpoint

---

Configures the certificate authority (CA) on Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **set certificate ca-trustpoint <ca-label> {ca-url <ca-url> | caname <caname> | get-method <post | get>}**

## Command Parameters

**<ca-label>**

Specifies the name of the CA.

**ca-url <ca-url>**

Specifies the trusted CA URL.

**caname <caname>**

Specifies the common name of the CA.

**get-method <post | get>**

Specifies the HTTP request type. You can use post for EJBCA or get for Win2012 CA. The default value is post.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## set certificate subject

Configures the subject identity on Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **set certificate subject <subject-label> {DN <name> | key-label <key-label>}**

## Command Parameters

### <subject-label>

Specifies the subject identity. You cannot use the following special characters:

- question mark (?)
- backslash (\)
- ampersand (&)
- less than (<)
- greater than (>)
- pound (#)

### DN <name>

Specifies the distinguished name. You can create a comma-separated list.

### key-label <key-label>

Specifies the key name of the generated key pair. This parameter is optional. If you do not configure one, the switch generates one the same as the subject-label.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



---

## set default-config-file

---

Loads the default configuration file to the Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **set default-config-file**

### Command Parameters

<default-config-file>

Specifies the name of the default configuration file.

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## set global

---

Configures the global parameters on the Fabric IPsec Gateway Virtual Machine.

### Syntax

- **set global fe-tunnel-gw-ip {A.B.C.D}**
- **set global fe-tunnel-src-ip {A.B.C.D}**
- **set global ipsec-disable**
- **set global ipsec-log-level <-1-5>**
- **set global ipsec-tunnel-src-ip {A.B.C.D/X}**
- **set global ipsec-tunnel-src-vlan <2-4059>**
- **set global lan-intf-gw-ip {A.B.C.D}**
- **set global lan-intf-ip {A.B.C.D/X}**
- **set global lan-intf-vlan <2-4059>**
- **set global mtu <750-9000>**
- **set global services sshd <disable | enable>**
- **set global virtual-reassembly-intf-ip {A.B.C.D/X}**

- **set global virtual-reassembly-intf-vlan** <2-4059>
- **set global wan-intf-gw-ip** {A.B.C.D}

## Command Parameters

### **fe-tunnel-gw-ip** {A.B.C.D}

Specifies the gateway IP address for Fabric Extend (FE) tunnel.

### **fe-tunnel-src-ip** {A.B.C.D}

Specifies the source IP address for FE tunnel.

### **ipsec-disable**

Disables IPsec globally on the Fabric IPsec Gateway VM.

### **ipsec-tunnel-src-ip** {A.B.C.D/X}

Specifies the source IP address and subnet mask for IPsec tunnel.

### **ipsec-tunnel-src-vlan** <2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

### **lan-intf-gw-ip** {A.B.C.D}

Specifies the gateway IP address for LAN interface.

### **lan-intf-ip** {A.B.C.D/X}

Specifies the IP address and subnet mask for Local Area Network (LAN) interface.

### **lan-intf-vlan** <2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

### **mtu** <750-9000>

Specifies the Maximum Transmission Unit (MTU) value.



#### Note

If an IPsec tunnel is not using the fragmentation and reassembly capabilities, the default MTU value is 1950.

### **services sshd** <disable | enable>

Enables or disables SSH access for Fabric IPsec Gateway. By default, SSH access is disabled.

### **virtual-reassembly-intf-ip** {A.B.C.D/X}

Specifies the virtual-reassembly interface IP address and subnet mask on the Fabric IPsec Gateway VM.

**Note**

You must configure the virtual reassembly interface IP address to use the fragmentation and reassembly service.

**virtual-reassembly-intf-vlan** <2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

**wan-intf-gw-ip** {A.B.C.D/X}

Specifies the gateway IP address and subnet mask for Wide Area Network (WAN) interface.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## set ip route

---

Adds an IP route.

## Syntax

- **set ip route** {A.B.C.D/X} **gw** {A.B.C.D}

## Command Parameters

{A.B.C.D/X}

Specifies the IP address and mask of the route to add.

**gw** {A.B.C.D}

Specifies the gateway IP address.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## set ipsec <1-255>

Configures parameters for IPsec tunnels on Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **set ipsec <1-255> admin-state enable**
- **set ipsec <1-255> auth-key WORD <1-32>**
- **set ipsec <1-255> auth-method <psk | rsasig>**
- **set ipsec <1-255> cert-subject <subject\_label>**
- **set ipsec <1-255> encryption-key-length <128 | 256>**
- **set ipsec <1-255> esp <aes128gcm16-sha256 | aes256-sha256 | aes256gcm16-sha256>**
- **set ipsec <1-255> fe-tunnel-dest-ip {A.B.C.D}**
- **set ipsec <1-255> fragment-before-encrypt enable**
- **set ipsec <1-255> ipsec-dest-ip {A.B.C.D}**
- **set ipsec <1-255> mtu <1300-9000>**
- **set ipsec <1-255> responder-only <true | false>**
- **set ipsec <1-255> tunnel-name WORD <1-64>**
- **set ipsec <1-255> egress-shaping-rage <1-1000>**

## Command Parameters

**admin-state enable**

Enables IPsec on the specific IPsec tunnel.

**auth-key WORD <1-32>**

Specifies the pre-shared authentication key.



### Note

Do not use special characters ?, \, &, <, >, #.

**auth-method <psk | rsasig>**

Specifies the authentication type for IPsec tunnels. The default is pre-shared key (psk).

**cert-subject <subject\_label>**

Specifies the certificate identity to use with the IPsec tunnel.

**egress-shaping-rate <1-1000>**

Specifies the egress shaping rate for the IPsec tunnel.

**encryption-key-length <128 | 256>**

Specifies the encryption key length for the IPsec tunnel. The default encryption key length is 128 bit. As a best practice, use the newer *esp* parameter instead.

**esp <aes128gcm16-sha256 | aes256-sha256 | aes256gcm16-sha256>**

Specifies the ESP cipher suites for the IPsec tunnel. The default is aes128gcm16-sha256. aes256-sha256 is not supported in the current release.

**fe-tunnel-dest-ip {A.B.C.D}**

Specifies the destination IP address for Fabric Extend (FE) tunnel.

**fragment-before-encrypt enable**

Enables the fragmentation of packets before IPsec encryption on the tunnel. By default, fragmentation before encryption is disabled.

**ipsec-dest-ip {A.B.C.D}**

Specifies the destination IP address for IPsec tunnel.

**mtu <1300-9000>**

Specifies the Maximum Transmission Unit (MTU) value for the FE tunnel with both IPsec and fragmentation and assembly capabilities.

**responder-only <true | false>**

Specifies if the IPsec session in the FE tunnel will be in responder only mode or initiator mode. When in responder mode the FE tunnel will only respond to the incoming request and not initiate the IPsec connection. By default both sides of IPsec connection will be initiators in the FE tunnel. Configure the IPsec tunnel to be in responder only mode when there is Network Address Translation (NAT) between the IPsec connection. For more information about NAT, see [VOSS User Guide](#).

**tunnel-name WORD <1-64>**

Specifies a name for the IPsec tunnel.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

You must disable the IPsec administrative state on the tunnel before you can remove IPsec configuration.

## set logical-intf-tunnel <1-255>

---

Configures a Fabric Extend (FE) tunnel with only fragmentation and reassembly capabilities, on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **set logical-intf-tunnel <1-255> fe-tunnel-dest-ip {A.B.C.D}**
- **set logical-intf-tunnel <1-255> mtu <750-9000>**
- **set logical-intf-tunnel <1-255> tunnel-name WORD <1-64>**
- **set logical-intf-tunnel <1-255> egress-shaping-rate <1-1000>**

## Command Parameters

**fe-tunnel-dest-ip {A.B.C.D}**

Specifies the Fabric Extend (FE) tunnel destination IP address for the logical interface.

**mtu <750-9000>**

Specifies the Maximum Transmission Unit (MTU) value for the FE tunnel with only fragmentation and assembly capabilities.

**tunnel-name WORD <1-64>**

Specifies the name of the logical interface tunnel.

**egress-shaping-rate<1-1000>**

Specifies the egress shaper rate for the logical interface tunnel.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show certificate-config

---

Displays the certificate configuration on Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **show certificate-config {ca-trustpoint [<ca-label>] | subject [<subject-label>]}**

### Command Parameters

**ca-trustpoint** [<ca-label>]

Displays the CA trustpoint configuration. If you do not specify the certificate authority (CA) name, the command displays the details of all configured CAs.

**subject** [<subject-label>]

Displays the subject-related configuration.

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show certificates

---

Displays valid installed certificates on Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **show certificates <all | cacert [<ca-label>] | crl [<ca-label>] | csr [<ca-label>] | keys | signed [<ca-label>]>**

### Command Parameters

all

Specifies all certificates.

**ca-cert**

Specifies certificates obtained from the certificate authority (CA).

**<ca-label>**

Specifies the name of the CA to filter the certificates. If you do not specify the name, the command displays the details for all configured CAs.

**crl**

Specifies Certificate Revocation List (CRL) certificates.

**csr**

Specifies certificate signing requests (CSR).

**keys**

Specifies keys.

**signed**

Specifies only signed certificates.

## Default

None.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## show default-config-file

Displays the default configuration file on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **show default-config-file**

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



## Example

The following example displays the default configuration file on the Fabric IPsec Gateway VM.

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

<cr>
FIGW> show default-config-file
coupled.cfg
```

## show ip route

---

Displays IP routes.

### Syntax

- **show ip route**

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show ipsec-config

---

Displays the IPsec configuration on the Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **show ipsec-config <1-255>**

### Command Parameters

<1-255>

Specifies the tunnel ID.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show ipsec-logs

Displays the IPsec session logs on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **show ipsec-logs**

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Example

The following example displays the IPsec session logs on the Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

<cr>
FIGW> show ipsec-logs
<<Month dd>> <<hh:mm:ss>> 15[IKE] <ipsec0-192.0.2.10|29> sending DPD request
<<Month dd>> <<hh:mm:ss>> 15[ENC] <ipsec0-192.0.2.10|29> generating INFORMATIONAL request 11832 [ ]
<<Month dd>> <<hh:mm:ss>> 15[NET] <ipsec0-192.0.2.10|29> sending packet: from 192.0.2.30[500] to
192.0.2.10[500] (76 bytes)
<<Month dd>> <<hh:mm:ss>> 13[NET] <ipsec0-192.0.2.10|29> received packet: from 192.0.2.10[500] to
192.0.2.30[500] (76 bytes)
<<Month dd>> <<hh:mm:ss>> 13[ENC] <ipsec0-192.0.2.10|29> parsed INFORMATIONAL response 11832 [ ]
<<Month dd>> <<hh:mm:ss>> 11[NET] <ipsec0-192.0.2.10|29> received packet: from 192.0.2.10[500] to
192.0.2.30[500] (76 bytes)
<<Month dd>> <<hh:mm:ss>> 11[ENC] <ipsec0-192.0.2.10|29> parsed INFORMATIONAL request 12924 [ ]
<<Month dd>> <<hh:mm:ss>> 11[ENC] <ipsec0-192.0.2.10|29> generating INFORMATIONAL response 12924 [ ]
<<Month dd>> <<hh:mm:ss>> 11[NET] <ipsec0-192.0.2.10|29> sending packet: from 192.0.2.30[500] to
192.0.2.10[500] (76 bytes)
<<Month dd>> <<hh:mm:ss>> 06[IKE] <ipsec0-192.0.2.10|29> sending DPD request
<<Month dd>> <<hh:mm:ss>> 06[ENC] <ipsec0-192.0.2.10|29> generating INFORMATIONAL request 11833 [ ]
<<Month dd>> <<hh:mm:ss>> 06[NET] <ipsec0-192.0.2.10|29> sending packet: from 192.0.2.30[500] to
```

```
192.0.2.10[500] (76 bytes)
--More-- (q = quit)
```

## show ipsec-routes

Displays the IPsec routes configured on the Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **show ipsec-routes**

### Command Mode

Fabric IPsec Gateway Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Example

The following example displays IPsec routes configured on the Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

<cr>
FIGW> show ipsec-routes
192.0.2.30 via 192.0.2.20 dev eth0.125 mtu lock 1950
192.0.2.1/24 dev eth0.30 proto kernel scope link src 192.0.2.2
192.0.2.10 via 192.0.2.45 dev eth0.30
192.0.2.100/24 dev eth0.125 proto kernel scope link src 192.0.2.60
192.0.2.11/16 dev docker0 proto kernel scope link src 192.0.2.12 linkdown
```

## show ipsec-stats

Displays the IPsec encryption statistics on the Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **show ipsec-stats**

### Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Example

The following example displays the IPsec encryption statistics on the Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

<cr>
FIGW> show ipsec-stats
src 192.0.2.30 dst 192.0.2.40
  proto esp spi 0xc0c2d9cd(3233995213) reqid 1(0x00000001) mode tunnel
  replay-window 32 seq 0x00000000 flag af-unspec (0x00100000)
  aead rfc4106(gcm(aes)) 0xa9c1923a4b4c5618ea2f3596de821261218bdea2 (160 bits) 128
  anti-replay context: seq 0x0, oseq 0x138, bitmap 0x00000000
  lifetime config:
    limit: soft (INF) (bytes), hard (INF) (bytes)
    limit: soft (INF) (packets), hard (INF) (packets)
    expire add: soft 3268(sec), hard 3600(sec)
    expire use: soft 0(sec), hard 0(sec)
  lifetime current:
    475650(bytes), 312(packets)
    add <<yyyy-mm-dd>> <<hh:mm:ss>> use <<yyyy-mm-dd>> <<hh:mm:ss>>
  stats:
    replay-window 0 replay 0 failed 0
src 192.0.2.40 dst 192.0.2.30
  proto esp spi 0xc92b08e5(3375040741) reqid 1(0x00000001) mode tunnel
  replay-window 32 seq 0x00000000 flag af-unspec (0x00100000)
  aead rfc4106(gcm(aes)) 0x9ca3568095298cefaaa709b9b932eb5141bd252c (160 bits) 128
  anti-replay context: seq 0x135, oseq 0x0, bitmap 0xffffffff
  lifetime config:
    limit: soft (INF) (bytes), hard (INF) (bytes)
    limit: soft (INF) (packets), hard (INF) (packets)
    expire add: soft 3341(sec), hard 3600(sec)
    expire use: soft 0(sec), hard 0(sec)
  lifetime current:
    470953(bytes), 309(packets)
    add <<yyyy-mm-dd>> <<hh:mm:ss>> use <<yyyy-mm-dd>> <<hh:mm:ss>>
  stats:
    replay-window 0 replay 0 failed 0
```

## show ipsec-status

Displays the status of configured IPsec tunnel on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **show ipsec-status**

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Example

The following example displays the status of configured IPsec tunnel on the Fabric IPsec Gateway VM:

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

<cr>
FIGW> show ipsec-status
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-128-generic, x86_64):
  uptime: 13 days, since <<month, day hh:mm:ss year>>
  malloc: sbrk 2433024, mmap 0, used 369408, free 2063616
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation
constraints
  pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgg dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr
  kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.0.2.40
  192.0.2.20
Connections:
ipsec0-192.0.2.5: 192.0.2.40...192.0.2.5 IKEv2, dpddelay=3s
ipsec0-192.0.2.5: local: [192.0.2.60] uses pre-shared key authentication
ipsec0-192.0.2.5: remote: [192.0.2.5] uses pre-shared key authentication
ipsec0-192.0.2.5: child: 192.0.2.60/32 === 192.0.2.5/32 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
ipsec0-192.0.2.5[29]: ESTABLISHED 21 hours ago, 192.0.2.40[192.0.2.60]...192.0.2.5[192.0.2.5]
ipsec0-192.0.2.5[29]: IKEv2 SPIs: dcf0a2d545d40679_i 55006e07252b9934_r*, pre-shared key
reauthentication in 2 hours
ipsec0-192.0.2.5[29]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
ipsec0-192.0.2.5{377}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c92b08e5_i c0c2d9cd_o
ipsec0-192.0.2.5{377}: AES_GCM_16_128, 291247 bytes_i (190 pkts, 6s ago), 297523 bytes_o (194 pkts,
1s ago), rekeying in 30 minutes
ipsec0-192.0.2.5{377}: 192.0.2.60/32 === 192.0.2.5/32
```

## show logical-intf-config

Displays the logical interface configurations on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **show logical-intf-config <1-255>**

## Command Parameters

<1-255>

Specifies the tunnel ID.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## show logical-intf-config

Displays the logical interface IPsec configurations on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **show ipsec-logical-intf-config**

## Command Parameters

<1-255>

Specifies the tunnel ID.

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## show running-config

Displays the default configuration file on the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **show running-config**

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Example

The following example displays the parameters configured currently on the Fabric IPsec Gateway VM.

```
Switch:1> enable
Switch:1# virtual-service figw console
Connected to domain figw
Escape character is ^Y

<cr>
FIGW> show running-config
set global ipsec-tunnel-src-vlan 125
set global ipsec-tunnel-src-ip 192.0.2.1/24
set global lan-intf-vlan 30
set global lan-intf-ip 192.0.2.10/24
set global lan-intf-gw-ip 192.0.2.25
set global fe-tunnel-src-ip 192.0.2.55
set global wan-intf-gw-ip 192.0.2.11
set global mtu 1950
set ipsec 1 auth-key *****
set ipsec 1 fe-tunnel-dest-ip 192.0.2.70
set ipsec 1 encryption-key-length 128
set ipsec 1 admin-state enable
```

## show version

Displays the current version of the Fabric IPsec Gateway Virtual Machine (VM).

## Syntax

- **show version**

## Command Mode

Fabric IPsec Gateway Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Example

The following example displays the default configuration file on the Fabric IPsec Gateway VM.

```
Switch:1> enable
Switch:1# virtual-service figw28 console
Connected to domain figw28
```

```
Escape character is ^Y
<cr>
FIGW> show version
FabricIPSecGW_VM_1.0
```

---

## system passwd-change rwa

Changes the user password for Fabric IPsec Gateway configuration access.

### Syntax

- **system passwd-change rwa**

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## system save-full tech <filename>

Captures the output of all show commands in Fabric IPsec Gateway configuration and saves to a file.

### Syntax

- **system save-full-tech <filename string:1-64>**

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



---

## traceroute

---

Trace route to an IP address on the Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **traceroute {A.B.C.D}**

### Command Parameters

{A.B.C.D}

Specifies the IP address.

### Default

None.

### Command Mode

Fabric IPsec Gateway Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## vi

---

Opens the vi editor to edit files on the Fabric IPsec Gateway Virtual Machine (VM).

### Syntax

- **vi <file name>**

### Command Parameters

<file name>

Specifies the name of the file to edit.

### Command Mode

Fabric IPsec Gateway Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



# GigabitEthernet Interface Configuration

---

The following topics document commands available in GigabitEthernet Interface Configuration mode of the command line interface (CLI).

## access-diffserv

---

Configure a port as trusted or untrusted to determine the Layer 3 QoS actions the switch performs. A trusted (core) port honors incoming Differentiated Services Code Point (DSCP) markings. An untrusted (access) port overrides DSCP markings.

### Syntax

- **access-diffserv**
- **access-diffserv enable**
- **access-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **access-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **default access-diffserv**
- **default access-diffserv enable**
- **default access-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **default access-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **no access-diffserv**
- **no access-diffserv enable**
- **no access-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no access-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

### Command Parameters

**enable**

If enabled, specifies an access port and overrides incoming DSCP bits. If disabled, specifies a core port and honors and handles incoming DSCP bits. The default is disabled.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default configuration is trusted (disabled).

## Command Mode

GigabitEthernet Interface Configuration

## action

---

Flush or clear the Address Resolution Protocol (ARP) tables for administrative and troubleshooting purposes. These actions are performed against a routed Gigabit Ethernet Interface. The related vlan action command performs similar functions against a VLAN interface.

## Syntax

- **action {none | flushMacFdb | flushArp | flushIp | triggerRipUpdate | flushAll | clearLoopDetectAlarm }**
- **action port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} { none | flushMacFdb | flushArp | flushIp | triggerRipUpdate | flushAll | clearLoopDetectAlarm}**
- **default action**
- **default action port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**

## Command Parameters

### ClearLoopDetectAlarm

Sets action to clear loop detect alarm.

### flushAll

Flush all tables.

### flushArp

Flush ARP tables.

### flushIp

Flush IP routing tables.

### flushMacFdb

Flush the MAC FDB.

### none

Sets action to none.

**port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### triggerRipUpdate

Force RIP to update the routing table so that the port or VLAN uses the latest routing information.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## auto-negotiate enable (on an Ethernet port)

---

Enable AutoNegotiation on the Ethernet port to optimally operate on the network.

## Syntax

- **auto-negotiate**
- **auto-negotiate enable**
- **auto-negotiate port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}
- **auto-negotiate port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]} **enable**
- **default auto-negotiate**
- **default auto-negotiate enable**
- **default auto-negotiate port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}
- **default auto-negotiate port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]} **enable**
- **no auto-negotiate**
- **no auto-negotiate enable**
- **no auto-negotiate port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}
- **no auto-negotiate port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]} **enable**

## Command Parameters

### enable

Enables or disables AutoNegotiation for the port or other ports of the module or both.

**port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default Auto-Negotiation behavior depends on the switch model and transceiver type. For more information, see [VOSS User Guide](#).

## Command Mode

GigabitEthernet Interface Configuration

## auto-negotiation-advertisements

Configure Auto-Negotiation advertisements after you enable Auto-Negotiation.



### Note

Because of port speed differences, not all parameters appear on all hardware platforms.

## Syntax

- **auto-negotiation-advertisements 10-full**
- **auto-negotiation-advertisements 10-half**
- **auto-negotiation-advertisements 100-full**
- **auto-negotiation-advertisements 100-half**
- **auto-negotiation-advertisements 1000-full**
- **auto-negotiation-advertisements 10000-full**
- **auto-negotiation-advertisements 2500-full**
- **auto-negotiation-advertisements 25000-full**
- **auto-negotiation-advertisements 5000-full**
- **auto-negotiation-advertisements none**
- **auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 10-full**
- **auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 10-half**
- **auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 100-full**

- `auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 100-half`
- `auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 1000-full`
- `auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 10000-full`
- `auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 2500-full`
- `auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 25000-full`
- `auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 5000-full`
- `auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} none`
- `default auto-negotiation-advertisements`
- `default auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `no auto-negotiation-advertisements`
- `no auto-negotiation-advertisements port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

## Command Parameters

### 10-full

Advertises 10 Mbps full-duplex.

### 10-half

Advertises 10 Mbps half-duplex.

### 100-full

Advertises 100 Mbps full-duplex.

### 100-half

Advertises 100 Mbps half-duplex.

### 1000-full

Advertises 1 Gbps full-duplex.

### 10000-full

Advertises 10 Gbps full-duplex.

### 2500-full

Advertises 2.5 Gbps full-duplex.

### 25000-full

Advertises 25 Gbps full-duplex.

### 5000-full

Advertises 5 Gbps full-duplex.

**none**

Configures the value to none.

**port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## auto-nni

Enable to have the node create an IS-IS interface, attach the interface to an SPBM instance, and then enable IS-IS on the port interface.

## Syntax

- **auto-nni**
- **no auto-nni**

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## auto-recover-port

Enable or disable autorecovery on a port.

## Syntax

- **auto-recover-port**
- **auto-recover-port enable**
- **auto-recover-port port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

- **auto-recover-port port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **default auto-recover-port**
- **default auto-recover-port enable**
- **default auto-recover-port port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **default auto-recover-port port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **no auto-recover-port**
- **no auto-recover-port enable**
- **no auto-recover-port port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no auto-recover-port port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

## Command Parameters

**enable**

Enables spoof detection on the port.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## auto-sense enable

Enables Auto-sense on a specific port.

## Syntax

- **auto-sense enable**
- **default auto-sense enable**
- **no auto-sense enable [convert-to-config]**



## Command Parameters

### **convert-to-config**

Disables Auto-sense on specific port(s), but retains the current configuration. The dynamic configuration becomes a manual configuration and is visible in the **show running-config** output.

## Default

By default, Auto-sense is disabled on the port(s).

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## auto-sense data (for port)

---

Configures an Auto-sense data I-SID on a port to separate data traffic.

## Syntax

- **auto-sense data i-sid <1-16777215>**
- **no auto-sense data i-sid**

## Command Parameters

**<1-16777215>**

Specifies the service interface identifier (I-SID).

## Default

None.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## brouter

Configure a port as a brouter port.

### Syntax

- **brouter port** {slot/port[/sub-port]} **vlan** <2-4059> **subnet** {A.B.C.D/X}
- **brouter port** {slot/port[/sub-port]} **vlan** <2-4059> **subnet** {A.B.C.D/X} **mac-offset** <MAC-offset>
- **brouter port** {slot/port[/sub-port]} **vlan** <2-4059> **subnet** {A.B.C.D/X} **name** WORD <0-64>
- **brouter port** {slot/port[/sub-port]} **vlan** <2-4059> **subnet** {A.B.C.D} {A.B.C.D}
- **brouter vlan** <2-4059> **subnet** {A.B.C.D/X}
- **brouter vlan** <2-4059> **subnet** {A.B.C.D/X} **mac-offset** <MAC-offset>
- **brouter vlan** <2-4059> **subnet** {A.B.C.D} {A.B.C.D}
- **no brouter**
- **no brouter port** {slot/port[/sub-port]}

### Command Parameters

**mac-offset** <MAC-offset>

Specifies a number by which to offset the MAC address from the chassis MAC address. This ensures that each IP address has a different MAC address. If you omit this variable, a unique MAC offset is automatically generated. Different hardware platforms support different ranges. To see which range is available on the switch, use the CLI command completion Help.

**name** WORD <0-64>

Specifies the IP address name in the range of 0 to 64 characters.

**port** {slot/port[/sub-port]}

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**subnet** <{A.B.C.D/X}|{A.B.C.D}>

Assigns an IP address and mask for the management port.

**vlan** <2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## channelize

---

Enable port channelization. Use this feature to configure a single port to operate as four logical interfaces.



### Note

Not all hardware platforms support this feature. For information about hardware support, see your hardware documentation.

## Syntax

- **channelize enable**
- **channelize port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **default channelize enable**
- **default channelize port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **no channelize enable**
- **no channelize port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

## Command Parameters

**enable**

Enable channelization for all ports.

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## clear mac-address-table dynamic

---

Clear the dynamic entries in the MAC address table.

### Syntax

- **clear mac-address-table dynamic 0x00:0x00:0x00:0x00:0x00:0x00 <1-4059>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

0x00:0x00:0x00:0x00:0x00:0x00

Specifies the MAC address.

### Default

None

## Command Mode

GigabitEthernet Interface Configuration

## default-vlan-id

---

Configure the default VLAN ID for the port.

### Syntax

- **default-vlan-id <0-4059>**
- **default-vlan-id port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} <0-4059>**

### Command Parameters

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<0-4059>

Specifies the VLAN ID.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## duplex

---

Configure the duplex mode on the Ethernet module. This command applies to 10/100/1000 Mb/s ports.

## Syntax

- **default duplex**
- **default duplex port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **duplex { half | full }**
- **duplex port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

<half|full>

Specifies half- or full-duplex mode. 1 and 10 Gb/s ports must use full-duplex mode.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is half.

## Command Mode

GigabitEthernet Interface Configuration

## eapol

Configure Extensible Authentication Protocol (EAP) on a specific port when you do not want EAPoL applied globally.

### Syntax

- `default eapol enable`
- `default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} supplicant-timeout`
- `default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} transmit-interval`
- `default eapol supplicant-timeout`
- `default eapol transmit-interval`
- `eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} fail-open-vlan <1-4059>`
- `eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} guest-vlan <1-4059>`
- `eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} max-request <1-10>`
- `eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} quiet-interval <1-65535>`
- `eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} supplicant-timeout <1-65535>`
- `eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} supplicant-timeout <1-65535>`
- `eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} transmit-interval <1-65535>`
- `eapol status authorized`
- `eapol supplicant-timeout <1-65535>`
- `eapol transmit-interval <1-65535>`
- `no eapol enable`

### Command Parameters

`fail-open-vlan <1-4059>`

Specifies the fail open VLAN ID.

`guest-vlan <1-4059>`

Specifies the guest VLAN ID.

`max-request <1-10>`

Specifies the maximum number of attempts to send the packet to the supplicant.

`quiet-interval <1-65535>`

Specifies the time in seconds to wait between authentication failure and start of a new authentication.

**supplicant-timeout <1-65535>**

Specifies the time in seconds to wait for response from supplicant for all EAP packets except EAP Request/Identity.

**transmit-interval <1-65535>**

Specifies the time in seconds to wait for response from supplicant for EAP Request/Identity packets.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## eapol fail-open-vlan

---

Specifies the Fail Open VLAN ID for this port. If the switch declares the RADIUS servers unreachable, then all new devices are allowed access into the configured Fail Open VLAN. 0 indicates that Fail Open VLAN is not enabled for this port.

## Syntax

- **default eapol fail-open-vlan**
- **eapol fail-open-vlan <1-4059>**
- **no eapol fail-open-vlan**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## eapol fail-open-isid

---

Specifies the Fail Open I-SID for this port. If the switch declares the RADIUS servers unreachable, all new devices are allowed access into the configured Fail Open I-SID.

### Syntax

- **default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} fail-open-isid <1-16000000>**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} fail-open-isid <1-16000000>**
- **no eapol fail-open-isid**

### Command Parameters

<1-600000>

Specifies the Fail Open I-SID. 0 indicates that Fail Open I-SID is not enabled for this port.

### Default

None

### Command Mode

GigabitEthernet Interface Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## eapol guest-isid

---

Configure the desired Guest I-SID.

### Syntax

- **default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} guest-isid <1-16000000>**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} guest-isid <1-16000000>**
- **no eapol guest-isid**

### Command Parameters

<1-16000000>



Specifies the Guest I-SID. 0 indicates that Guest I-SID is not enabled for this port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## eapol guest-vlan

---

Configure the desired Guest VLAN ID.

## Syntax

- **default eapol guest-vlan**
- **eapol guest-vlan <1-4059>**
- **no eapol guest-vlan**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## eapol max-request

---

Configures the maximum EAP requests sent to supplicant before timing out the session.

## Syntax

- **default eapol max-request**
- **default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} max-request**
- **eapol max-request <1-10>**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} max-request <1-10>**

## Command Parameters

<1-10>

Specifies the maximum EAP requests sent to supplicant before timing out the session.

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is 2.

## Command Mode

GigabitEthernet Interface Configuration

## eapol multihost eap-mac-max

---

Configure maximum EAPOL clients allowed on the port at one time.

## Syntax

- **default eapol multihost eap-mac-max**
- **eapol multihost eap-mac-max <0-32>**

## Command Parameters

<0-32>

Specifies the maximum EAPOL clients allowed on the port at one time. The default is 2.

## Default

The default is 2.

## Command Mode

GigabitEthernet Interface Configuration

### eapol multihost eap-oper-mode

---

Configure the EAPoL operational mode.

#### Syntax

- **default eapol multihost eap-oper-mode**
- **eapol multihost eap-oper-mode {mhmv | mhsa}**

#### Command Parameters

mhmv | mhsa

Specifies the EAPoL operational mode.

#### Default

The default is MHMV.

## Command Mode

GigabitEthernet Interface Configuration

### eapol multihost mac-max

---

Configures the maximum MAC clients, both EAP and NEAP, supported on a port.

#### Syntax

- **default eapol multihost mac-max**
- **eapol multihost mac-max <1-8192>**

#### Command Parameters

mac-max <1-8192>

Specifies the maximum number of EAP and NEAP MAC addresses allowed on the port. The maximum limit is 32 MAC addresses.

#### Default

The default is 1.

## Command Mode

GigabitEthernet Interface Configuration

### eapol multihost non-eap-mac-max

---

Configure the maximum Non EAPoL clients allowed on the port at one time.

#### Syntax

- **default eapol multihost non-eap-mac-max**
- **eapol multihost non-eap-mac-max <0-8192>**

#### Command Parameters

<1-8192>

Specifies the maximum non-EAPoL clients allowed on the port at one time. The default is 2.

#### Default

The default is 2.

## Command Mode

GigabitEthernet Interface Configuration

### eapol multihost radius-non-eap-enable

---

Enable RADIUS based non-EAP authentication.

#### Syntax

- **default eapol multihost radius-non-eap-enable**
- **eapol multihost radius-non-eap-enable**
- **no eapol multihost radius-non-eap-enable**

#### Default

The default is disable.

## Command Mode

GigabitEthernet Interface Configuration

### eapol quiet-interval

---

Specifies the time interval between authentication failure and start of a new authentication.

## Syntax

- **default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} quiet-interval**
- **default eapol quiet-interval**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} quiet-interval <1-65535>**
- **eapol quiet-interval <1-65535>**

## Command Parameters

**<1-65535>**

Specifies the time interval in seconds between authentication failure and start of a new authentication.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is 60.

## Command Mode

GigabitEthernet Interface Configuration

## eapol radius-dynamic-server enable

---

Enable EAP processing requests from the RADIUS Dynamic Authorization Server.

## Syntax

- **eapol radius-dynamic-server enable**

## Command Parameters

**enable**

Enable EAP processing requests from the RADIUS Dynamic Authorization Server.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

## eapol re-authentication

Configures reauthentication.

### Syntax

- **default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} re-authentication**
- **default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} re-authentication enable**
- **default eapol re-authentication**
- **default eapol re-authentication enable**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} re-authentication**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} re-authentication enable**
- **eapol re-authentication**
- **eapol re-authentication enable**
- **no eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} re-authentication**
- **no eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} re-authentication enable**
- **no eapol re-authentication**
- **no eapol re-authentication enable**

### Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### **enable**

Enables reauthenticating an existing supplicant at a specified time interval. The default is disabled.

### Default

None

## Command Mode

GigabitEthernet Interface Configuration

### eapol re-authentication-period

---

Reauthenticates an existing supplicant at the time interval specified in ReAuthPeriod. Specifies the time interval in seconds between successive reauthentications.

#### Syntax

- **default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} re-authentication-period**
- **default eapol re-authentication-period**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} re-authentication-period <60-65535>**
- **eapol re-authentication-period <1-65535>**

#### Default

The default is 3600 (1 hour ).

## Command Mode

GigabitEthernet Interface Configuration

### eapol status

---

Enable Extensible Authentication Protocol (EAPoL) on an interface.

#### Syntax

- **default eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} status**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} status authorized**
- **eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} status auto**
- **eapol status {authorized|auto}**
- **no eapol port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} status**

## Command Parameters

**authorized**

Specifies the port is always authorized.

**auto**

Specifies that port authorization depends on the results of the EAPoL authentication by the RADIUS server.

**port** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## eapol traffic-control

---

Configure Wake-On-LAN functionality.

## Syntax

- **default eapol traffic-control**
- **eapol traffic-control {in | in-out}**
- **no eapol traffic-control**

## Command Parameters

*in*

Specifies to block inbound traffic for unauthenticated devices.

*in-out*

Specifies to block inbound and outbound traffic for unauthenticated devices.

## Default

in-out

## Command Mode

GigabitEthernet Interface Configuration



## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## eapol voice lldp-auth

---

Enables Link Layer Discovery Protocol (LLDP) voice authentication of IP phones on a specific port.

### Syntax

- **default eapol voice lldp-auth**
- **eapol voice lldp-auth**
- **no eapol voice lldp-auth**

### Default

The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

## enable-diffserv

---

Enable DiffServ so that the switch provides DiffServ-based QoS on that port.

### Syntax

- **default enable-diffserv**
- **default enable-diffserv enable**
- **default enable-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **default enable-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} enable**
- **enable-diffserv**
- **enable-diffserv enable**
- **enable-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **enable-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} enable**
- **no enable-diffserv**
- **no enable-diffserv enable**

- **no enable-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no enable-diffserv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

## Command Parameters

### enable

Enables DiffServ for the specified port. The default is enabled.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## encapsulation dot1q

Enable tagging on the ports before configuring Untagged VLANs.

## Syntax

- **default encapsulation dot1q**
- **default encapsulation dot1q port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **encapsulation dot1q**
- **encapsulation dot1q port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no encapsulation dot1q**
- **no encapsulation dot1q port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

### dot1q

Sets encapsulation. dot1q enables trunking on the MLT.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## endpoint-tracking (for a port)

---

Create and enable Endpoint Tracking on ports. Creating and enabling Endpoint Tracking on ports can be accomplished using a one-step or two-step process; you can create and enable at the same time, or create but leave disabled, and then enable at a later time.

Use the no operator with **endpoint-tracking** to delete, and the no operator with **endpoint-tracking enable** to disable.

## Syntax

- **endpoint-tracking**
- **endpoint-tracking enable**
- **no endpoint-tracking**
- **no endpoint-tracking enable**

## Command Parameters

**enable**

Creates and enables Endpoint Tracking, or enables Endpoint Tracking previously created on a port.

## Default

Disabled

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## energy-saver (for port)

---

Enables Energy Saver on a specific port or range of ports.

### Syntax

- **default energy-saver port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **energy-saver port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **no energy-saver port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

### Command Parameters

**enable**

Enables energy savings on ports.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

Disabled

### Command Mode

GigabitEthernet Interface Configuration

---

## energy-saver eee enable

---

Enable Energy Efficient Ethernet (EEE) on a port.

### Syntax

- **energy-saver eee enable**
- **no energy-saver eee enable**

### Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## fa authentication-key (for a port)

---

Configure the Fabric Attach (FA) authentication key.

## Syntax

- **default fa authentication-key**
- **fa authentication-key WORD<0-32>**

## Command Parameters

**WORD<0-32>**

Configures the authentication key on the port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## fa enable (for a port)

---

Enable FA on a port.

## Syntax

- **fa enable**
- **no fa enable**

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## fa management (for a port)

---

Configure FA management on a port.

### Syntax

- **default fa management i-sid**
- **fa management i-sid<i-sid><c-vid>**
- **no fa management i-sid**

### Command Parameters

**c-vid** <c-vid>

Specifies the C-VLAN value of the port on the FA server. Different hardware platforms support different customer VLAN ID ranges. Use the CLI Help to see the available range for the switch.

**i-sid** <i-sid>

Specifies the management I-SID. Different hardware platforms support different customer I-SID ranges. To see the available range for the switch, use the CLI Help.

### Default

None

### Command Mode

GigabitEthernet Interface Configuration

---

## fa message-authentication (for a port)

---

Configure FA message authentication on port.

### Syntax

- **default no fa message-authentication**
- **fa message-authentication**
- **no fa message-authentication**

### Default

None

### Command Mode

GigabitEthernet Interface Configuration

---

## fec

---

Configures Forward Error Correction (FEC) on either a 100 GbE port or a channelized 100 GbE port operating at 25 Gbps speed. On the 100 GbE ports, only the Clause 91 and Clause 108 options are supported. On the channelized ports, you can configure either Clause 108 for extra latency or Clause 74 for reduced latency. You can also configure the auto option to automatically configure FEC based on port speed and pluggable module type.

FEC is not supported on 100 Gbps ports operating at 40 Gbps speed or on a management port. On ports that support FEC configuration, ensure that you configure the same option at both end points. Otherwise, the link does not come up.

### Syntax

- **default fec port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **fec {auto|cl91|cl108|cl74}**
- **no fec port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

{auto|cl91|cl108|cl74}

Configures FEC on either a 100 GbE port or a channelized 100 GbE port operating at 25 Gbps speed. On the 100 GbE ports, only the Clause 91 and Clause 108 options are supported. On the channelized ports, you can configure either Clause 108 for extra latency or Clause 74 for reduced latency. You can also configure the auto option to automatically configure FEC based on port speed and pluggable module type.

FEC is not supported on 100 Gbps ports operating at 40 Gbps speed or on a management port. On ports that support FEC configuration, ensure that you configure the same option at both end points. Otherwise, the link does not come up.

### Default

The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## high-secure enable

---

Protect the switch against IP packets with illegal IP addresses such as loopback addresses or a source IP address of ones, or Class D or Class E addresses from being routed.

### Syntax

- **default high-secure**
- **default high-secure enable**

- **default high-secure port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **default high-secure port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **high-secure**
- **high-secure enable**
- **high-secure port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **high-secure port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **no high-secure**
- **no high-secure enable**
- **no high-secure port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no high-secure port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

## Command Parameters

### enable

Enables the high secure feature that blocks packets with illegal IP addresses. This flag is disabled by default.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip arp-inspection

Sets the trust factor associated with a port for DAI feature.

## Syntax

- **default ip arp-inspection**
- **ip arp-inspection <trusted|untrusted>**
- **no ip arp-inspection**



## Command Parameters

### trusted

Sets the trust factor as trusted on the port for DAI.

### untrusted

Sets the trust factor as untrusted on the port for DAI.

## Default

The default is untrusted.

## Command Mode

GigabitEthernet Interface Configuration

## ip arp-proxy enable (for a port)

---

Configure an ARP proxy to allow a router to answer a local ARP request for a remote destination.

## Syntax

- **default ip arp-proxy**
- **default ip arp-proxy enable**
- **ip arp-proxy enable**
- **no ip arp-proxy**
- **no ip arp-proxy enable**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ip arp-response (for a port)

---

Enable Address Resolution Protocol (ARP) on the switch to allow a router to answer a local ARP request.

## Syntax

- **default ip arp-response**
- **ip arp-response**
- **no ip arp-response**

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip bfd (for a port)

---

Enable and configure Bidirectional Forwarding Detection (BFD) on a port.

## Syntax

- `default ip bfd enable`
- `default ip bfd interval`
- `default ip bfd min-rx`
- `default ip bfd multiplier`
- `default ip bfd port`
- `ip bfd enable`
- `ip bfd interval`
- `ip bfd min-rx`
- `ip bfd multiplier`
- `ip bfd port`
- `no ip bfd`
- `no ip bfd port`

## Command Parameters

### enable

Enable BFD on a port.

### interval

Specifies the transmit interval in milliseconds. The default is 200 ms.

The minimum value for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure the remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.

### min-rx

Specifies the receive interval in milliseconds. The default is 200 ms.

The minimum value for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure the remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.

### multiplier

Specifies the multiplier used to calculate the amount of time BFD waits before it declares a receive timeout. The default is 3.

If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

**port** {*slot/port[/sub-port]*[-*slot/port[/sub-port]*][,*...*]

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ip dhcp-relay (for a port)

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command `no ip dhcp-relay` disables DHCP Relay but does not delete the DHCP entry.

## Syntax

- **default ip dhcp-relay**
- **default ip dhcp-relay broadcast**
- **default ip dhcp-relay circuitId**
- **default ip dhcp-relay max-hop**
- **default ip dhcp-relay min-sec**
- **default ip dhcp-relay mode**
- **default ip dhcp-relay remoteId**
- **default ip dhcp-relay trusted**
- **ip dhcp-relay**
- **ip dhcp-relay broadcast**
- **ip dhcp-relay circuitId**
- **ip dhcp-relay clear-counter**
- **ip dhcp-relay max-hop <1-16>**
- **ip dhcp-relay min-sec <0-65535>**
- **ip dhcp-relay mode { bootp | dhcp | bootp\_dhcp }**
- **ip dhcp-relay remoteId**
- **ip dhcp-relay trusted**

- **no ip dhcp-relay**
- **no ip dhcp-relay broadcast**
- **no ip dhcp-relay circuitId**
- **no ip dhcp-relay remoteId**
- **no ip dhcp-relay trusted**

## Command Parameters

### **broadcast**

Enables the device to send the server reply as a broadcast to the end station. After you disable this variable, the device sends the server reply as a unicast to the end station.

### **circuitId**

Enables the device to insert the Option 82 Circuit ID into the packets sent to the server (enables DHCP Option 82). The default is disabled.

### **clear-counter**

Clears the dhcp-relay counter.

### **max-hop <1-16>**

Configures the maximum number of hops before a BootP/DHCP packet is discarded (1-16). The default is 4.

### **min-sec <0-65535>**

Configures the minimum seconds count for Dynamic Host Configuration Protocol (DHCP). If the secs field in the BootP/DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped (0- 65535). The default is 0 seconds.

### **mode <bootp|dhcp|bootp\_dhcp>**

Configures DHCP mode to forward BootP messages only, Dynamic Host Configuration Protocol (DHCP) messages only, or both. The default is both.

### **remoteId**

Enables the device to insert the Option 82 Remote ID into the packets sent to the server (enables DHCP Option 82). The default is disabled.

### **trusted**

Configures the circuit as trusted in an Option 82 context.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip dhcp-relay fwd-path (for a port)

---

Create the forwarding path from the client to the server.

## Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D}**
- **default ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>**
- **ip dhcp-relay fwd-path {A.B.C.D}**
- **ip dhcp-relay fwd-path {A.B.C.D} disable**
- **ip dhcp-relay fwd-path {A.B.C.D} enable**
- **ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>**
- **no ip dhcp-relay fwd-path {A.B.C.D}**
- **no ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>**

## Command Parameters

**{A.B.C.D}**

Creates a forwarding path to the Dynamic Host Configuration Protocol (DHCP) server. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface.



### Tip

If the relay is a virtual router configured on this interface, you must set the vrid.

**disable**

Disables the forwarding path.

**enable**

Enables the forwarding path.

**vrid <1-255>**

Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip dhcp-relay fwd-path mode (for a port)

Modify Dynamic Host Configuration Protocol (DHCP) mode to forward BootP messages only, DHCP messages only, or both.

## Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D} mode**
- **ip dhcp-relay fwd-path {A.B.C.D} mode bootp**

- **ip dhcp-relay fwd-path {A.B.C.D} mode bootp\_dhcp**
- **ip dhcp-relay fwd-path {A.B.C.D} mode dhcp**

## Command Parameters

**mode <bootp|dhcp|bootp\_dhcp>**

Configures DHCP mode to forward BootP messages only, Dynamic Host Configuration Protocol (DHCP) messages only, or both. The default is both.

## Default

The default mode is both.

## Command Mode

GigabitEthernet Interface Configuration

## ip dhcp-snooping (for port)

---

Sets the trust factor associated with a port for DHCP Snooping feature.

## Syntax

- **default ip dhcp-snooping**
- **ip dhcp-snooping <trusted|untrusted>**
- **no ip dhcp-snooping**

## Command Parameters

**trusted**

Sets the trust factor as trusted on the port for DHCP Snooping.

**untrusted**

Sets the trust factor as untrusted on the port for DHCP Snooping.

## Default

The default is untrusted.

## Command Mode

GigabitEthernet Interface Configuration

## ip directed-broadcast (for a port)

---

Configure the device to forward directed broadcasts for a VLAN.

## Syntax

- `default ip directed-broadcast`
- `default ip directed-broadcast enable`
- `ip directed-broadcast`
- `ip directed-broadcast enable`
- `no ip directed-broadcast`
- `no ip directed-broadcast enable`

## Command Parameters

### enable

Allows the device to forward directed broadcast frames to the specified VLAN. The default setting for this feature is enabled.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip forward-protocol udp (on a port)

Configure UDP protocols to determine which UDP broadcasts are forwarded

## Syntax

- `default ip forward-protocol udp`
- `ip forward-protocol udp`
- `no ip forward-protocol udp`

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ip forward-protocol udp broadcastmask (on a port)

Configure the broadcast mask on the IP forwarding list.

## Syntax

- `default ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D}`
- `default ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D} maxttl <1-16>`
- `ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D}`
- `ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D} maxttl <1-16>`
- `no ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D}`
- `no ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D} maxttl <1-16>`

## Command Parameters

`broadcastmask {A.B.C.D}`

Sets the interface broadcast mask (the interface broadcast mask can be different from the interface mask). A.B.C.D is an IP address in a.b.c.d format.

`maxttl <1-16>`

Sets the maximum time-to-live value (TTL) for the interface. The range is 1 to 16.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip forward-protocol udp maxttl (on a port)

---

Set the maximum time to live.

## Syntax

- `default ip forward-protocol udp maxttl <1-16>`
- `ip forward-protocol udp maxttl <1-16>`
- `no ip forward-protocol udp maxttl <1-16>`

## Command Parameters

`maxttl <1-16>`

Sets the maximum time-to-live value (TTL) for the interface. The range is 1 to 16.



## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip forward-protocol udp port

Configure a UDP port forward entry to add or remove a port forward entry.

## Syntax

- `default ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D}`
- `default ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D} maxttl <1-16>`
- `default ip forward-protocol udp port {slot/port[/sub-port]} maxttl <1-16>`
- `default ip forward-protocol udp port {slot/port} portfwddlist <1-1000>`
- `ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D}`
- `ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D} maxttl <1-16>`
- `ip forward-protocol udp port {slot/port[/sub-port]} maxttl <1-16>`
- `ip forward-protocol udp port {slot/port[/sub-port]} portfwddlist <1-1000>`
- `no ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D}`
- `no ip forward-protocol udp port {slot/port[/sub-port]} broadcastmask {A.B.C.D} maxttl <1-16>`
- `no ip forward-protocol udp port {slot/port[/sub-port]} maxttl <1-16>`
- `no ip forward-protocol udp port {slot/port[/sub-port]} portfwddlist <1-1000>`

## Command Parameters

`broadcastmask {A.B.C.D}`

Sets the interface broadcast mask (the interface broadcast mask can be different from the interface mask). A.B.C.D is an IP address in a.b.c.d format.

`maxttl <1-16>`

Sets the maximum time-to-live value (TTL) for the interface. The range is 1 to 16.

`portfwddlist <1-1000>`

Creates a port forwarding list in the range of 1 to 1000.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

# ip forward-protocol udp portfwldlist (on a port)

---

Configure the UDP port forwarding list.

## Syntax

- **default ip forward-protocol udp portfwldlist <1-1000>**
- **ip forward-protocol udp portfwldlist <1-1000>**
- **no ip forward-protocol udp portfwldlist <1-1000>**

## Command Parameters

**portfwldlist <1-1000>**

Creates a port forwarding list in the range of 1 to 1000.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

# ip igmp access-list (for a port)

---

Configure multicast access control for a Internet Group Management Protocol (IGMP) Ethernet port to restrict access to certain multicast streams and to protect multicast streams from spoofing (injecting data to the existing streams).

## Syntax

- **default ip igmp access-list WORD<1-64> {A.B.C.D/X}**
- **ip igmp access-list WORD<1-64> {A.B.C.D/X} {deny-tx | deny-rx | deny-both | allow-only-tx | allow-only-rx | allow-only-both}**
- **no ip igmp access-list WORD<1-64> {A.B.C.D/X}**

## Command Parameters

{A.B.C.D/X}

Creates an access control group entry for a specific Internet Group Management Protocol (IGMP) interface. Specifies the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.

**{deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}**

Indicates the action for the specified Internet Group Management Protocol (IGMP) interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic

**WORD<1-64>**

Specifies the name of the access list from 1-64 characters.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip igmp access-list mode (for a port)

---

Changes the mode for an existing access list on the Ethernet port.

## Syntax

- **default ip igmp access-list WORD<1-64> {A.B.C.D/X}**
- **ip igmp access-list WORD<1-64> {A.B.C.D/X} mode {deny-tx | deny-rx | deny-both | allowonly-tx | allow-only-rx | allow-only-both}**
- **no ip igmp access-list WORD<1-64> {A.B.C.D/X}**

## Command Parameters

**{A.B.C.D/X}**

Creates an access control group entry for a specific Internet Group Management Protocol (IGMP) interface. Specifies the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.

**deny-tx | deny-rx | deny-both | allowonly-tx | allowonly-rx | allowonly-both**

Indicates the action for the specified Internet Group Management Protocol (IGMP) interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.

**WORD<1-64>**

Specifies the name of the access list from 1-64 characters.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

### ip igmp compatibility-mode (for a port)

---

Enables IGMP v2-v3 compatibility mode.

#### Syntax

- **default ip igmp compatibility-mode**
- **ip igmp compatibility-mode**
- **no ip igmp compatibility-mode**

#### Default

The default value is disabled, which means IGMPv3 is not compatible with IGMPv1 or IGMPv2.

## Command Mode

GigabitEthernet Interface Configuration

### ip igmp dynamic-downgrade-version (for a port)

---

Configures the version of Internet Group Management Protocol (IGMP) to handle older query messages if the system downgrades. If the system downgrades, the host with IGMPv3 only capability does not work. If you do not configure the system to downgrade the version of IGMP, the system logs a warning.

#### Syntax

- **default ip igmp dynamic-downgrade-version**
- **ip igmp dynamic-downgrade-version**
- **no ip igmp dynamic-downgrade-version**

#### Default

Enabled

## Command Mode

GigabitEthernet Interface Configuration

### ip igmp igmpv3-explicit-host-tracking (for an Ethernet port)

---

Track all the source and group members. You must enable explicit-host-tracking to use fast leave for IGMPv3.

## Syntax

- **default ip igmp igmpv3-explicit-host-tracking**
- **ip igmp igmpv3-explicit-host-tracking**
- **no ip igmp igmpv3-explicit-host-tracking**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ip igmp immediate-leave (for an Ethernet port)

---

Enable fast (immediate) leave mode to specify if a port receives a leave message from a member of a group.

## Syntax

- **default ip igmp immediate-leave**
- **ip igmp immediate-leave**
- **no ip igmp immediate-leave**

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip igmp last-member-query-interval (for a port)

---

Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages.

## Syntax

- **default ip igmp last-member-query-interval**
- **ip igmp last-member-query-interval <0-255>**

## Command Parameters

<0-255>

Specifies the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. Decreasing the value reduces the time to detect the loss of the last member of a group. Configure this value between 3 to 10 (equal to 0.3 to 1.0 seconds). The default is 10 tenths of a second.

**Note**

You cannot configure this value for IGMPv1.

## Default

The default is 10 tenths of a second.

## Command Mode

GigabitEthernet Interface Configuration

## ip igmp port (for a port)

---

Configure Internet Group Management Protocol (IGMP) for a particular port.

## Syntax

- **default ip igmp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **ip igmp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no ip igmp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip igmp query-interval (for a port)

---

Configure the frequency (in seconds) at which the VLAN transmits host query packets.

## Syntax

- **default ip igmp query-interval**
- **ip igmp query-interval <1-65535>**

## Command Parameters

<1-65535>

Configures the frequency (in seconds) at which the VLAN transmits host query packets. The default is 125 seconds.

## Default

The default is 125 seconds.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip igmp query-max-response (for a port)

Configure the maximum response time advertised in IGMPv2 general queries on an interface.

## Syntax

- **default ip igmp query-max-response**
- **ip igmp query-max-response <0-255>**

## Command Parameters

<0-255>

Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. Smaller values enables a router to prune groups faster.



### Important

You must configure this value lower than the query-interval. The default is 100 tenths of a second (equal to 10 seconds).



### Note

You cannot configure this value for IGMPv1.

## Default

The default is 100 tenths of a second (equal to 10 seconds).

## Command Mode

GigabitEthernet Interface Configuration

---

## ip igmp robust-value (for a port)

Configure the expected packet loss of a network.

## Syntax

- **default ip igmp robust-value**
- **ip igmp robust-value <2-255>**

## Command Parameters

<2-255>

Configures the expected packet loss of a network. Increase the value if you expect the network to experience packet loss. The default is 2 seconds.

## Default

The default is 2 seconds.

## Command Mode

GigabitEthernet Interface Configuration

## ip igmp router-alert (for a port)

---

Configure the router to ignore Internet Group Management Protocol (IGMP) packets.

## Syntax

- **default ip igmp router-alert**
- **ip igmp router-alert**
- **no ip igmp router-alert**

## Default

Disabled

## Command Mode

VLAN Interface Configuration

## Usage Guidelines

To maximize network performance, configure this parameter according to the version of IGMP currently in use:

- IGMPv1 - Disable
- IGMPv2 - Enable
- IGMPv3 - Enable



## ip igmp stream-limit (for a port)

---

Configure multicast stream limitation on an Ethernet port to limit the number of concurrent multicast streams on the port.

### Syntax

- **default ip igmp stream-limit**
- **default ip igmp stream-limit stream-limit-max-streams**
- **ip igmp stream-limit**
- **ip igmp stream-limit stream-limit-max-streams <0-65535>**
- **no ip igmp stream-limit**

### Command Parameters

**stream-limit**

Enables the stream limit on the specified Ethernet port.

**stream-limit-max-streams <0-65535>**

Sets the maximum number of streams allowed on an interface. The value ranges from 0 to 65535.

### Default

None

### Command Mode

GigabitEthernet Interface Configuration

## ip igmp upnp-filter (for a port)

---

Configure Universal Plug and Play (uPnP) Filtering on an IGMP-enabled interface to drop all incoming multicast packets destined for any multicast group residing in a specific range.

### Syntax

- **default ip igmp upnp-filter**
- **ip igmp upnp-filter [ip <A.B.C.D/X>]**
- **no ip igmp upnp-filter**

### Command Parameters

**ip <A.B.C.D/X>**

Specifies the multicast destination IP address range to be filtered. The default multicast group address is 239.255.255.250/32.

## Default

The default is disabled.

## Command Mode

GigabitEthernet

## ip igmp version (for a port)

---

Configure the version of Internet Group Management Protocol (IGMP) on the interface.

## Syntax

- **default ip igmp version**
- **ip igmp version <1-3>**

## Command Parameters

<1-3>

Specifies the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is 2 (IGMPv2).

## Default

The default is 2 (IGMPv2).

## Command Mode

VLAN Interface Configuration

## ip ipsec enable (for a port)

---

Enable Internet Protocol Security (IPsec) for IPv4 on a port.

## Syntax

- **default ip ipsec enable**
- **ip ipsec enable**
- **no ip ipsec enable**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

### ip ipsec policy (for a port)

---

Link an Internet Protocol Security (IPsec) IPv4 policy to an interface.

#### Syntax

- **default ip ipsec policy WORD<1-32>**
- **ip ipsec policy WORD<1-32>**
- **ip ipsec policy WORD<1-32> dir both**
- **ip ipsec policy WORD<1-32> dir in**
- **ip ipsec policy WORD<1-32> dir out**
- **no ip ipsec policy WORD<1-32> dir both**
- **no ip ipsec policy WORD<1-32> dir in**
- **no ip ipsec policy WORD<1-32> dir out**

#### Command Parameters

**dir <both|in|out>**

Specifies the direction to which IPsec applies. Both specifies both ingress and egress traffic, in specifies ingress traffic, and out specifies egress traffic. By default, the direction is both.

**WORD<1-32>**

Specifies the IPsec policy name.

#### Default

None

## Command Mode

GigabitEthernet Interface Configuration

### ip irdp address (for a port)

---

Configure Internet Control Message Protocol (ICMP) Router Discovery to enable hosts attached to multicast or broadcast networks to discover the IP addresses of their neighboring routers.

#### Syntax

- **default ip irdp**
- **default ip irdp address**
- **ip irdp address {A.B.C.D}**

## Command Parameters

**address <A.B.C.D>**

Specifies the IP destination address use for broadcast or multicast router advertisements sent from the interface. The address is the all-systems multicast address, 224.0.0.1, or the limited-broadcast address, 255.255.255.255.

## Default

The default address is 255.255.255.255.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip irdp holdtime (for a port)

Configure the lifetime for advertisements.

## Syntax

- **default ip irdp holdtime**
- **ip irdp holdtime <4-9000>**

## Command Parameters

**<4-4000>**

Specifies the lifetime.

## Default

The default is 1800.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip irdp maxadvertinterval (for a port)

Specify the maximum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the router interface.

## Syntax

- **default ip irdp maxadvertinterval**
- **ip irdp maxadvertinterval <4-1800>**

## Command Parameters

<4-1800>

Specifies the maximum time in seconds.

## Default

The default is 600 seconds.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip irdp minadvertinterval (for a port)

Specify the minimum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the interface. The range is 3 seconds to maxadvertinterval.

## Syntax

- **default ip irdp minadvertinterval**
- **ip irdp minadvertinterval <3-1800>**

## Command Parameters

<3-1800>

Specifies the minimum time in seconds.

## Default

The default is 450 seconds.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip irdp multicast (for a port)

Specify if multicast advertisements are sent.

## Syntax

- **default ip irdp multicast**
- **ip irdp multicast**
- **no ip irdp multicast**

## Default

The default is enabled (true).

## Command Mode

GigabitEthernet Interface Configuration

---

## ip irdp preference (for a port)

Specify the preference (a higher number indicates more preferred) of the address as a default router address relative to other router addresses on the same subnet.

## Syntax

- **default ip irdp preference**
- **ip irdp preference <-2147483648-2147483647>**

## Command Parameters

<-2147483648-2147483647>

Specifies the preference value.

## Default

The default is 0.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip mroute (for a port)

Limit the number of multicast streams to protect a CPU from multicast data packet bursts generated by malicious applications.

## Syntax

- **default ip mroute max-allowed-streams**
- **default ip mroute max-allowed-streams-timer-check**
- **default ip mroute port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **default ip mroute stream-limit**
- **ip mroute max-allowed-streams <1-32768>**
- **ip mroute max-allowed-streams-timer-check <1-3600>**

- `ip mroute port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} max-allowed-streams <1-32768>`
- `ip mroute port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} max-allowed-streams-timer-check <1-3600>`
- `ip mroute port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} stream-limit`
- `ip mroute stream-limit`
- `no ip mroute port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `no ip mroute stream-limit`

## Command Parameters

### `max-allowed-streams <1-32768>`

Configures the maximum number of streams on the specified port. The port is shut down if the number of streams exceeds this limit. The value is a number between 1-32768. The default value is 1984 streams.

To set this option to the default value, use the default operator with the command.

### `max-allowed-streams-timer-check <1-3600>`

Configures the sampling interval, which is used to check if the number of ingress multicast streams to the CPU is under a configured limit or if the port needs to shut down. The range is between 1-3600. The default value is 10 seconds.

To set this option to the default value, use the default operator with the command.

### `port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### `stream-limit`

Enables stream limit on a particular interface.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf advertise-when-down enable (for a port)

Enable or disable AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. When you configure a port with no link and enable advertise-when-down, the route is not advertised until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

## Syntax

- **default ip ospf advertise-when-down enable**
- **ip ospf advertise-when-down enable**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} advertise-when-down enable**
- **no ip ospf advertise-when-down enable**

## Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf area (for a port)

---

Configure OSPF parameters on a port to control how OSPF behaves.

## Syntax

- **default ip ospf area**
- **ip ospf area {A.B.C.D}**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} area {A.B.C.D}**
- **no ip ospf area**

## Command Parameters

<A.B.C.D>

Configures the OSPF identification number for the area, typically formatted as an IP address.

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf authentication-key (for a port)

---

Configure the eight-character simple password authentication key for the port.

## Syntax

- **default ip ospf authentication-type**
- **ip ospf authentication-key WORD<0-8>**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} authentication-key WORD<0-8>**

## Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**WORD<0-8>**

Specifies the authentication key.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf authentication-type (for a port)

---

Configure the OSPF authentication type for the port. If you choose simple, you must configure the password with the ip ospf authentication-key WORD<0-8> command. If you choose MD5, you must configure the MD5 key with the ip ospf message-digest-key <1-255> md5 WORD<0-16> command.

## Syntax

- **ip ospf authentication-type message-digest**
- **ip ospf authentication-type none**
- **ip ospf authentication-type sha-1**
- **ip ospf authentication-type sha-2**
- **ip ospf authentication-type simple**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} authentication-type message-digest**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} authentication-type none**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} authentication-type sha-1**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} authentication-type sha-2**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} authentication-type simple**
- **no ip ospf authentication-type**

## Command Parameters

### message-digest

Configures the authentication-type to message-digest.

If you choose MD5, you must configure the MD5 key with the `ip ospf message-digest-key <1-255> md5 WORD<0-16> command`. Message Digest 5 (MD5) provides standards-based authentication using 128-bit encryption.

If you use MD5, each OSPF packet has a message digest appended to it. The digest must match between sending and receiving routers, or the packet is discarded.

### none

Configures the authentication-type to none.

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### sha-1

Configures the authentication-type to secure hash algorithm 1 (SHA-1). SHA-1 provides standards-based authentication using 128-bit encryption.

### sha-2

sha-2—Specifies SHA-2, which offers the hash function SHA-256.



#### Note

The parameter sha-2, an update of SHA-1, can offer six hash functions that include SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224,SHA 512/256, with hash values that are 224, 256, 384, or 512 bits. However, the current release supports only SHA-256.

#### simple

Configures the authentication-type to use a simple-text password. Only routers that contain the same authentication ID in their LSA can communicate with each other. Using a simple-text password is not a best practice for security. If you choose simple, you must configure the password with the **ip ospf authentication-key WORD<0-8>** command.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf bfd

---

Enable Bidirectional Forwarding Detection (BFD) for an OSPF GigabitEthernet IPv4 interface.

## Syntax

- **default ip ospf bfd**
- **ip ospf bfd**
- **ip ospf bfd disable**
- **no ip ospf bfd**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf cost (for a port)

---

Configure the OSPF cost associated with this interface and advertised in router link advertisements.

## Syntax

- **default ip ospf cost**
- **ip ospf cost <0-65535>**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} cost <0-65535>**

## Command Parameters

<1-65535>

Specifies the cost range.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is 0.

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf dead-interval (for a port)

Configure the router OSPF dead interval—the number of seconds the OSPF neighbors of a switch must wait before assuming that the OSPF router is down. The value must be at least four times the Hello interval.

## Syntax

- **default ip ospf dead-interval**
- **ip ospf dead-interval <0-2147483647>**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} dead-interval <0-2147483647>**

## Command Parameters

<0-2147483647>

Specifies the Dead interval in seconds. Dead Interval must be a multiple of Hello Interval.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is 40.

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf digest-key (for a port)

---

Configure the Digest algorithm key which can be of type MD5, SHA-1 or SHA-2. At most, you can configure two digest keys for an interface.

## Syntax

- **default ip ospf digest-key <1-255>**
- **ip ospf digest-key <1-255> WORD<0-16>**
- **no ip ospf digest-key <1-255>**

## Command Parameters

<1-255>

Specifies the ID for the digest key.

<WORD> <0-16>

Specifies an alphanumeric password of up to 16 bytes (string length 0 to 16).

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf enable (for a port)

---

Enable OSPF on the port.

## Syntax

- **default ip ospf**
- **default ip ospf enable**

- **default ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **ip ospf enable**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **no ip ospf**
- **no ip ospf enable**
- **no ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf hello-interval (for a port)

Configure the OSPF Hello interval, which is the number of seconds between Hello packets sent on this interface.

## Syntax

- **default ip ospf hello-interval**
- **ip ospf hello-interval <1-65535>**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} hello-interval <1-65535>**

## Command Parameters

**<1-65535>**

Specifies the Hello interval range in seconds. Dead Interval must be a multiple of Hello Interval.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is 10.

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf mtu-ignore enable (for a port)

---

Enable maximum transmission unit (MTU) ignore. To allow the switch to accept OSPF database description (DBD) packets with a different MTU size, enable mtu-ignore. Incoming OSPF DBD packets are dropped if their MTU is greater than 1500 bytes.

## Syntax

- **default ip ospf mtu-ignore enable**
- **ip ospf mtu-ignore enable**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} mtu-ignore enable**
- **no ip ospf mtu-ignore enable**

## Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf network (for a port)

---

Specify the type of OSPF interface.

## Syntax

- **default ip ospf network**
- **ip ospf network {broadcast | nbma | passive}**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} network {broadcast | nbma | passive}**

## Command Parameters

**<broadcast|nbma|passive>**

Specifies the interface type.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf poll-interval (for a port)

Configure the OSPF poll interval in seconds.

## Syntax

- **default ip ospf poll-interval**
- **ip ospf poll-interval <0-2147483647>**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} poll-interval <0-2147483647>**

## Command Parameters

**<0-2147483647>**

Specifies the poll interval range in seconds.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



## Default

The default is 120.

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf primary-digest-key (for a port)

---

Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the new digest key.

## Syntax

- **default ip ospf primary-digest-key**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} primary-md5-key <1-255>**
- **ip ospf primary-digest-key <1-255>**

## Command Parameters

<1-255>

Specifies the primary md5 key range.

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf priority (for a port)

---

Configure the OSPF priority for the port during the election process for the designated router. The port with the highest priority number is the best candidate for the designated router. If you configure the priority to 0, the port cannot become either the designated router or a backup designated router.

## Syntax

- **default ip ospf priority**

- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} priority <0-255>**
- **ip ospf priority <0-255>**

## Command Parameters

<0-255>

Specifies the priority range.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is 1.

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf retransmit-interval (for a port)

Configure the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions.

## Syntax

- **default ip ospf retransmit-interval**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} retransmit-interval <0-3600>**
- **ip ospf retransmit-interval <0-3600>**

## Command Parameters

<0-3600>

Specifies the retransmit interval range in seconds.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip ospf transit-delay (for a port)

---

Configure the transit delay for the virtual interface, which is the estimated number of seconds required to transmit a link-state update over the interface.

## Syntax

- **default ip ospf transit-delay**
- **ip ospf port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} transit-delay <0-3600>**
- **ip ospf transit-delay <0-3600>**

## Command Parameters

<0-3600>

Specifies the transit delay range.

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip pim (for a port)

---

Enable PIM and configure to perform multicasting operations.

## Syntax

- **default ip pim bsr-candidate preference <0-255>**
- **default ip pim enable**

- `default ip pim hello-interval`
- `default ip pim interface-type`
- `default ip pim join-prune-interval`
- `ip pim active`
- `ip pim bsr-candidate preference <0-255>`
- `ip pim enable`
- `ip pim hello-interval <0-18724>`
- `ip pim interface-type [active | passive]`
- `ip pim join-prune-interval <1-18724>`
- `ip pim passive`
- `no ip pim bsr-candidate`
- `no ip pim enable`
- `no ip pim fast-joinprune`

## Command Parameters

### active

Enables PIM and sets interface type to active.

### bsr-candidate <preference>

Enables BSR candidate on an interface.

### enable

Configure PIM for each interface to enable the interface to perform multicasting operations.

### hello-interval <0-18724>

Specifies the query interval in seconds.

### hello-interval <0-18724>

Specify how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches.

### interface-type [active | passive]

Specifies the pim interface-type on a interface.

### join-prune-interval <1-18724>

Specify how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors.

### passive

Enable PIM and configure the interface type to passive simultaneously. By default, an enabled interface is active.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

### ip pim bsr-candidate preference (for a port)

---

Configure additional routers as candidate BSRs (C-BSR) to provide backup protection in the event that the primary BSR fails.

#### Syntax

- **default ip pim bsr-candidate**
- **ip pim bsr-candidate preference <0-255>**
- **no ip pim bsr-candidate**

#### Command Parameters

**preference <0-255>**

Enables the C-BSR on this interface and configures its preference value, from 0-255, to become a Bootstrap Router (BSR). The C-BSR with the highest BSR preference and address is the preferred BSR.

#### Default

None

## Command Mode

GigabitEthernet Interface Configuration

### ip pim hello-interval (for a port)

---

Configure the hello-interval on a interface.

#### Syntax

- **default ip pim hello-interval**
- **ip pim hello-interval <0-18724>**

#### Command Parameters

**<0-18724>**

Specifies the duration in seconds before the PIM router sends out the next hello message to neighboring switches.

## Default

The default is 30 seconds.

## Command Mode

GigabitEthernet Interface Configuration

## ip pim interface-type (for a port)

---

Specifies whether the selected interface is active or passive. You can change the state of a PIM interface after you create the interface but only if you disable PIM on the interface. Use this feature when a high number of PIM interfaces exist and connect to end users, not to other switches.

- An active interface accepts PIM control transmitted and received traffic.
- A passive interface prevents PIM control traffic from transmitting or receiving, thereby reducing the load on a system.

## Syntax

- **default ip pim interface-type**
- **ip pim interface-type active**
- **ip pim interface-type passive**

## Command Parameters

<active|passive>

Specifies the interface type.

## Default

The default is active.

## Command Mode

GigabitEthernet Interface Configuration

## ip pim join-prune-interval (for a port)

---

Configure the frequency at which pim join/prune messages are sent

## Syntax

- **default ip pim join-prune-interval**
- **ip pim join-prune-interval <1-18724>**

## Command Parameters

<1-18724>

Specifies the duration in seconds before the PIM router sends out the next join or prune message to its upstream neighbors.

## Default

The default is 60 seconds.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip advertise-when-down enable (for a port)

Enable or disable AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled.

When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down.

To disable advertising based on link status, this parameter must be disabled.

## Syntax

- **default ip rip advertise-when-down enable**
- **ip rip advertise-when-down enable**
- **no ip rip advertise-when-down enable**

## Command Parameters

<enable|disable>

Enables or disables AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled.

When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down.

To disable advertising based on link status, this parameter must be disabled.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip auto-aggregation (for a port)

---

Enable or disable automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disabled.

### Syntax

- **default ip rip auto-aggregation enable**
- **ip rip auto-aggregation enable**
- **no ip rip auto-aggregation enable**

### Command Parameters

**enable**

Enables or disables automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disabled.

### Default

The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## ip rip cost (for a port)

---

Configure the RIP cost for this port (link).

### Syntax

- **default ip rip cost**
- **ip rip cost <1-15>**

### Command Parameters

**<1-15>**

Configures the RIP cost for this port (link).

### Default

None



## Command Mode

GigabitEthernet Interface Configuration

### ip rip default-listen (for a port)

---

Enable default listen: the switch accepts the default route learned through RIP on this interface. The default is disabled.

#### Syntax

- **default ip rip default-listen enable**
- **ip rip default-listen enable**
- **no ip rip default-listen enable**

#### Command Parameters

**enable**

Enables DefaultListen: the switch accepts the default route learned through RIP on this interface. The default is disabled.

#### Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

### ip rip default-supply enable (for a port)

---

Enable default supply. If enabled, a default route must be advertised from this interface.

The default route is advertised only if it exists in the routing table. The default route will not be advertised on RIP interfaces by default. You need to redistribute the default route and then configure the default-supply at the interface for the default route to be advertised to the neighbor.

#### Syntax

- **default ip rip default-supply enable**
- **ip rip default-supply enable**
- **no ip rip default-supply enable**

#### Command Parameters

**enable**

Enables DefaultSupply. If enabled, a default route must be advertised from this interface. The default is false. The default route is advertised only if it exists in the routing table.

## Default

The default is false.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip enable (for a port)

Enable RIP routing on the interface.

## Syntax

- **default ip rip enable**
- **ip rip enable**
- **no ip rip enable**

## Command Parameters

**enable**

Enables RIP routing on the interface.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip holddown (for a port)

Configure the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.

## Syntax

- **default ip rip holddown**
- **ip rip holddown <0-360>**

## Command Parameters

<0-360>

Configures the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.

## Default

The default is 120.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip in-policy (for a port)

Configures the rip in-policy on specific interface.

## Syntax

- **default ip rip in-policy**
- **ip rip in-policy WORD<0-64>**

## Command Parameters

WORD<0-64>

Configures the policy name for inbound filtering on this RIP interface. This policy determines whether to learn a route on this interface and specifies the parameters of the route when RIP adds it to the routing table.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip listen (for a port)

If enabled, the switch listens for a default route without listening for all routes. Specify that the routing switch learns RIP routes through this interface. The default is enable.

## Syntax

- **default ip rip listen enable**
- **ip rip listen enable**

- **no ip rip listen enable**

## Command Parameters

### enable

If enabled, the switch listens for a default route without listening for all routes. Specifies that the routing switch learns RIP routes through this interface. The default is enable.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip out-policy (for a port)

Configure the port RIP out-policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also specifies the parameters of the advertisement. Policy name is a string of length 0 to 64 characters.

## Syntax

- **default ip rip out-policy**
- **ip rip out-policy WORD<0-64>**

## Command Parameters

### WORD<0-64>

Configures the port RIP out-policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also specifies the parameters of the advertisement. Policy name is a string of length 0 to 64 characters.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip poison enable (for a port)

---

Enable Poison Reverse. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network.

If you disable Poison Reverse (no poison enable), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an immediate neighbor are not advertised back to the neighbor.

These mechanisms prevent routing loops.

### Syntax

- **default ip rip poison enable**
- **ip rip poison enable**
- **no ip rip poison enable**

### Command Parameters

#### enable

Enables Poison Reverse.

- If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network.
- If you disable Poison Reverse (no poison enable), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an immediate neighbor are not advertised back to the neighbor.

These mechanisms prevent routing loops.

### Default

The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## ip rip port

---

Configure RIP for a port.

### Syntax

- **default ip rip port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]**
- **ip rip port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]**

- **no ip rip port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip rip receive version (for a port)

---

Indicate which RIP update version is accepted on this interface. The default is rip1orrip2.

## Syntax

- **default ip rip receive version**
- **ip rip receive version { rip1 | rip2 | rip1orrip2 }**

## Command Parameters

**<rip1|rip2|rip1orrip2>**

Indicates which RIP update version is accepted on this interface. The default is rip1orrip2.

## Default

The default is rip1orrip 2.

## Command Mode

GigabitEthernet Interface Configuration

## ip rip send (for a port)

---

Indicate which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible.

## Syntax

- **default ip rip send version**
- **ip rip send version { notsend | rip1 | rip1comp | rip2 }**

## Command Parameters

<notsend|rip1|rip2|rip1comp|rip2>

Indicates which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible

## Default

The default is rip1Compatible.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip supply (for a port)

Specify that the switch advertises RIP routes through the port. The default is enable.

## Syntax

- **default ip rip supply enable**
- **ip rip supply enable**
- **no ip rip supply enable**

## Command Parameters

<enable|disable>

Specifies that the switch advertises RIP routes through the port. The default is enable.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip timeout (for a port)

Configure the RIP timeout interval in seconds.

## Syntax

- **default ip rip timeout**
- **ip rip timeout <15-259200>**

## Command Parameters

<15-259200>

Configures the RIP timeout interval in seconds.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rip triggered (for a port)

Enable automatic triggered updates for RIP.

## Syntax

- **default ip rip triggered enable**
- **ip rip triggered enable**
- **no ip rip triggered enable**

## Command Parameters

**enable**

Enables automatic triggered updates for RIP.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip rvs-path-chk

Configure unicast reverse path forwarding on a port (IPv4).



## Syntax

- **default ip rvs-path-chk**
- **default ip rvs-path-chk mode**
- **ip rvs-path-chk**
- **ip rvs-path-chk mode exist-only**
- **ip rvs-path-chk mode strict**
- **no ip rvs-path-chk**

## Command Parameters

**mode {strict|exist-only}**

Specifies the mode for Unicast Reverse Path Forwarding (uRPF).

- In strict mode, uRPF checks whether the source IP address of the incoming packet exists in the FIB. If the incoming interface is not the best reverse path, the packet check fails and uRPF drops the packet.
- In exist-only mode, uRPF checks whether the source IP address of the incoming packet exists in the FIB. The packet is dropped only if the source address is not reachable via any interface on that router.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip source verify

---

Configures IP Source Guard (IPSG) on a port, for IPv4 addresses. When you enable IPSG on the port, filters are automatically installed for the IPv4 addresses that are already learned on that interface.

## Syntax

- **default ip source verify**
- **ip source verify enable**
- **no ip source verify**

## Default

IPSG for IPv4 addresses is disabled by default.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip spb-multicast enable (for a port)

---

Enables Layer 3 VSN IP multicast over Fabric Connect.

### Syntax

- **default ip spb-multicast enable**
- **ip spb-multicast enable**
- **no ip spb-multicast enable**

### Default

The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## ip spb-pim-gw enable (for a port)

---

Enable SPB-PIM Gateway on a VLAN interface.

### Syntax

- **default p spb-pim-gw enable**
- **ip spb-pim-gw enable**
- **no ip spb-pim-gw enable**

### Default

The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## ip spb-pim-gw hello-interval (for a port)

---

Configures the SPB-PIM Gateway VLAN HELLO interval.

### Syntax

- **default ip spb-pim-gw hello-interval <0-18724>**
- **ip spb-pim-gw hello-interval <0-18724>**
- **no ip spb-pim-gw hello-interval <0-18724>**

## Command Parameters

<0-18724>

Specifies the HELLO interval in seconds. The default value is 30 seconds.

## Default

The default value is 30 seconds.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip spb-pim-gw ip join-prune-interval (for a port)

Configures the SPB-PIM Gateway VLAN JOIN PRUNE interval.

## Syntax

- **default ip spb-pim-gw ip join-prune-interval <1-18724>**
- **ip spb-pim-gw ip join-prune-interval <1-18724>**
- **no ip spb-pim-gw ip join-prune-interval <1-18724>**

## Command Parameters

<1-18724>

Specifies the JOIN PRUNE interval in seconds. The default value is 60 seconds.

## Default

The default value is 60 seconds.

## Command Mode

GigabitEthernet Interface Configuration

---

## ip vrrp (for a port)

Configure Virtual Router Redundancy Protocol (VRRP) on a port.

## Syntax

- **default ip vrrp <1-255>**
- **default ip vrrp <1-255> action**
- **default ip vrrp <1-255> adver-int**
- **default ip vrrp <1-255> backup-master enable**

- `default ip vrrp <1-255> critical-ip enable`
- `default ip vrrp <1-255> critical-ip-addr`
- `default ip vrrp <1-255> enable`
- `default ip vrrp <1-255> fast-adv enable`
- `default ip vrrp <1-255> fast-adv-int`
- `default ip vrrp <1-255> holddown-timer`
- `default ip vrrp <1-255> preempt-mode`
- `default ip vrrp <1-255> priority`
- `ip vrrp <1-255> action none`
- `ip vrrp <1-255> action preempt`
- `ip vrrp <1-255> adver-int <1-255>`
- `ip vrrp <1-255> backup-master enable`
- `ip vrrp <1-255> critical-ip enable`
- `ip vrrp <1-255> critical-ip-addr {A.B.C.D}`
- `ip vrrp <1-255> enable`
- `ip vrrp <1-255> fast-adv enable`
- `ip vrrp <1-255> fast-adv-int <200-1000>`
- `ip vrrp <1-255> holddown-timer <0-21600>`
- `ip vrrp <1-255> priority <1-255>`
- `ip vrrp <1-255> preempt-mode enable`
- `ip vrrp address <1-255> {A.B.C.D}`
- `no ip vrrp <1-255>`
- `no ip vrrp <1-255> backup-master enable`
- `no ip vrrp <1-255> critical-ip enable`
- `no ip vrrp <1-255> enable`
- `no ip vrrp <1-255> fast-adv enable`
- `no ip vrrp <1-255> preempt-mode enable`

## Command Parameters

`<vrid> preempt-mode enable`

Enables preempt mode for vrrp (v3).

`action {none|preempt}`

Use the action choice option to manually override the hold-down timer and force preemption. none|preempt can be set to preempt the timer or set to none to allow the timer to keep working.

`address <1-255> <A.B.C.D>`

Sets the IP address of the Virtual Router Redundancy Protocol (VRRP) interface that forwards packets to the virtual IP addresses associated with the virtual router. A.B.C.D is the IP address of the master VRRP.

`adver-int <1-255>`

Sets the the time interval between sending Virtual Router Redundancy Protocol (VRRP) advertisement messages. The range is between 1 and 255 seconds. This value must be the same on all the participating routers. The default is 1.

**backup-master enable**

Enables the Virtual Router Redundancy Protocol (VRRP) backup master. This option is supported only on Split MultiLink Trunking (SMLT) ports. Do not enable Backup Master if Critical IP is enabled.

**critical-ip enable**

Enables the critical IP address option. Do not enable critical IP if Backup Master is enabled.

**critical-ip-addr <A.B.C.D>**

Sets the critical IP address for VRRP. A.B.C.D is the IP address on the local router, which is configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface goes down).

**enable**

Enables Virtual Router Redundancy Protocol (VRRP) on the interface.

**fast-adv enable**

Enables the Fast Advertisement Interval. The default is disabled.

**fast-adv-int <200-1000>**

Sets the Fast Advertisement Interval, in milliseconds, the time interval between sending VRRP advertisement messages. The range must be the same on all participating routers. The default is 200. You must enter values in multiples of 200 milliseconds.

**holddown-timer<0-21600>**

Modifies the behavior of the Virtual Router Redundancy Protocol (VRRP) failover mechanism by allowing the router enough time to detect the OSPF or RIP routes. 0-21600 is the time interval (in seconds) a router is delayed when changing to master state.

**priority <1-255>**

Sets the port Virtual Router Redundancy Protocol (VRRP) priority. 1-255 is the value used by the VRRP router. The default is 100. Assign the value 255 to the router that owns the IP address associated with the virtual router.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip vrrp address (for a port)

---

Specify an address to associate with the virtual router.

## Syntax

- **default ip vrrp address <1-255>**
- **default ip vrrp address <1-255> {A.B.C.D}**
- **ip vrrp address <1-255> {A.B.C.D}**
- **no ip vrrp address <1-255>**
- **no ip vrrp address <1-255> {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies an address to associate with the virtual router.

<1-255>

Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ip vrrp version

---

Configure VRRP version on an interface.

## Syntax

- **default ip vrrp version**
- **ip vrrp version [2|3]**

## Command Parameters

[2|3]

Configure VRRP version 2 or 3 on an interface.

## Default

The default is version 2.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 bfd (for a port)

---

Enable and configure Bidirectional Forwarding Detection (BFD) on a port.

### Syntax

- **default ipv6 bfd enable**
- **default ipv6 bfd interval**
- **default ipv6 bfd min-rx**
- **default ipv6 bfd multiplier**
- **default ipv6 bfd port**
- **ipv6 bfd enable**
- **ipv6 bfd interval**
- **ipv6 bfd min-rx**
- **ipv6 bfd multiplier**
- **ipv6 bfd port**
- **no ipv6 bfd**
- **no ipv6 bfd port**

### Command Parameters

#### enable

Enable BFD on a port.

#### interval

Specifies the transmit interval in milliseconds. The default is 200 ms.

The minimum value for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure the remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.

#### min-rx

Specifies the receive interval in milliseconds. The default is 200 ms.

The minimum value for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure the remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.

#### multiplier

Specifies the multiplier used to calculate the amount of time BFD waits before it declares a receive timeout. The default is 3.

If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

**port** {*slot/port* [/sub-port] [-*slot/port* [/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

BFD for IPv6 interfaces is a demonstration feature on some products. For more information, see [VOSS Feature Support Matrix](#).

## ipv6 dhcp-relay (for a port)

---

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command `no ipv6 dhcp-relay` disables DHCP on the interface; it does not delete the entry.

## Syntax

- **default ipv6 dhcp-relay**
- **default ipv6 dhcp-relay fwd-path WORD<0-255>**
- **default ipv6 dhcp-relay max-hop**
- **default ipv6 dhcp-relay remote-id**
- **ipv6 dhcp-relay**
- **ipv6 dhcp-relay fwd-path WORD<0-255>**
- **ipv6 dhcp-relay fwd-path WORD<0-255> enable**
- **ipv6 dhcp-relay fwd-path WORD<0-255> vrid WORD<1-255>**
- **ipv6 dhcp-relay max-hop <1-32>**
- **ipv6 dhcp-relay remote-id**
- **no ipv6 dhcp-relay**
- **no ipv6 dhcp-relay fwd-path WORD<0-255>**
- **no ipv6 dhcp-relay fwd-path WORD<0-255> enable**
- **no ipv6 dhcp-relay remote-id**

## Command Parameters

`max-hop <1-32>`

Configures the maximum number of hops before a BootP/DHCP packet is discarded. The default is 32.

`remoteld`



Enables the Remote ID. The default is disabled.

**vrid WORD<1-255>**

Specifies the ID of the virtual router and is an integer from 1-255.

**WORD<0-255>**

Creates a forwarding path to the Dynamic Host Configuration Protocol (DHCP) server with a mode and a state. WORD<0-255> is the IPv6 address of the server. The default IP address of the relay is the address of the interface. If the relay is a Virtual Router configured on this interface, you must set the vrid.

By default, the forwarding path is disabled.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 fhs dhcp-guard

---

Enable device role verification attached to the port. By default, router is selected.

## Syntax

- **default ipv6 fhs dhcp-guard attach-policy**
- **ipv6 fhs dhcp-guard attach-policy WORD<1-64>**
- **ipv6 fhs dhcp-guard device-role {client | server}**
- **no ipv6 fhs dhcp-guard attach-policy**

## Command Parameters

**attach-policy**

Attach dhcp-guard policy to interface.

**Client**

Set device role as client.

**device-role**

Set dhcp-guard device-role.

**Server**

Set device role as server.

**WORD<1-64>**

Specify the name of the DHCP guard policy to be attached or detached.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 fhs nd-inspection enable (for a port)

---

Enables neighbor discovery (ND) inspection on a port or interface.

## Syntax

- **default ipv6 fhs nd-inspection enable**
- **ipv6 fhs nd-inspection enable**
- **no ipv6 fhs nd-inspection enable**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 fhs ra-guard

---

Enables verification of the role of the device attached to the port.

## Syntax

- **default ipv6 fhs ra-guard attach-policy**
- **ipv6 fhs ra-guard attach-policy WORD<1-64>**
- **ipv6 fhs ra-guard device-role {router|host}**
- **no ipv6 fhs ra-guard attach-policy**

## Command Parameters

### attach-policy

Attach RA Guard policy to interface.

### device-role

Set RA Guarddevice role.

### host

Set device role as host.

**router**

Set device role as router.

**WORD<1-64>**

Specifies the policy name.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 forwarding (for a port)

---

Configure IPv6 forwarding. By default, IPv6 forwarding is globally disabled, which means you can only use local IPv6 connections, and traffic does not traverse an IPv6 network.

## Syntax

- **default ipv6 forwarding**
- **ipv6 forwarding**
- **no ipv6 forwarding**

## Default

By default, forwarding is enabled on an interface. You must enable it globally before the interface configuration takes effect.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 interface (for a port)

---

Creates an IPv6 interface.

## Syntax

- **default ipv6 interface**
- **ipv6 interface**
- **no ipv6 interface**

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 interface address (for a port)

---

Configure the IPv6 address for a port.

### Syntax

- **ipv6 interface address WORD<0-255>**
- **no ipv6 interface address**
- **no ipv6 interface address WORD<0-255>**

### Command Parameters

WORD<0-255>

Assigns an IPv6 address to the port.

### Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 interface enable (for a port)

---

Enable IPv6 route advertisement on a port.

### Syntax

- **default ipv6 interface enable**
- **ipv6 interface enable**
- **ipv6 interface enable vlan <1-4059>**
- **no ipv6 interface enable**

### Command Parameters

vlan <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 interface hop-limit (for a port)

---

Configure the maximum number of hops before packets drop.

## Syntax

- **default ipv6 interface hop-limit**
- **ipv6 interface hop-limit <1-255>**

## Command Parameters

<1-255>

Configures the maximum hops.

## Default

The default is 64 hops.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 interface link-local (for a port)

---

Create a link-local address for the port.

## Syntax

- **ipv6 interface link-local WORD<0-19>**
- **ipv6 interface link-local WORD<0-19> address WORD<0-46>**
- **ipv6 interface link-local WORD<0-19> enable**
- **ipv6 interface link-local WORD<0-19> mac-offset <MAC-offset>**
- **ipv6 interface link-local WORD<0-19> name WORD<0-255>**
- **ipv6 interface link-local WORD<0-19> vlan <1-4059>**

## Command Parameters

address WORD<0-46>

Specifies the IPv6 address.

**enable**

Enables route advertisement.

**mac-offset** *<MAC-offset>*

Specifies a number by which to offset the MAC address from the chassis MAC address. This ensures that each IP address has a different MAC address. If you omit this variable, a unique MAC offset is automatically generated. Different hardware platforms support different ranges. To see which range is available on the switch, use the CLI command completion Help.

**name** **WORD***<0-255>*

Assigns a descriptive name. The network management system also configures this string.

**vlan** *<1-4059>*

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**WORD***<0-19>*

Specifies the 64-bit interface ID used to calculate the actual link-local address.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 interface mtu (for a port)

---

Configure the maximum transmission unit for the port.

## Syntax

- **default ipv6 interface mtu**
- **ipv6 interface mtu** *<1280-9500>*

## Command Parameters

*<1280-9500>*

Configures the maximum transmission unit for the interface: 1280-1500, 1850, or 9500.

## Default

The default is 1500.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 interface name (for a port)

---

Configure an interface description for the port.

## Syntax

- **ipv6 interface name WORD<0-255>**

## Command Parameters

**WORD<0-255>**

Assigns a descriptive name to the port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 interface reachable-time (for a port)

---

Configure the time a neighbor is considered reachable after receiving a reachability confirmation.

## Syntax

- **default ipv6 interface reachable-time**
- **ipv6 interface reachable-time <1-3600000>**

## Command Parameters

**<1-3600000>**

Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.

## Default

The default is 30000.

## Command Mode

GigabitEthernet Interface Configuration

### ipv6 interface retransmit-timer (for a port)

---

Configure the time, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

#### Syntax

- **default ipv6 interface retransmit-timer**
- **ipv6 interface retransmit-timer <1-4294967295>**

#### Command Parameters

<1-4294967295>

Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

#### Default

The default is 1000.

## Command Mode

GigabitEthernet Interface Configuration

### ipv6 interface vlan (for a port)

---

Configure the interface as part of an IPv6 VLAN.

#### Syntax

- **ipv6 interface vlan <1-4059>**

#### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.



## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 ipsec enable (for a port)

Enable Internet Protocol Security (IPsec) for IPv6 on a port.

## Syntax

- **default ipv6 ipsec enable**
- **ipv6 ipsec enable**
- **no ipv6 ipsec enable**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 ipsec policy (for a port)

Link an Internet Protocol Security (IPsec) IPv6 policy to an interface.

## Syntax

- **default ipv6 ipsec policy WORD<1-32>**
- **ipv6 ipsec policy WORD<1-32>**
- **ipv6 ipsec policy WORD<1-32> dir both**
- **ipv6 ipsec policy WORD<1-32> dir in**
- **ipv6 ipsec policy WORD<1-32> dir out**
- **no ipv6 ipsec policy WORD<1-32> dir both**
- **no ipv6 ipsec policy WORD<1-32> dir in**
- **no ipv6 ipsec policy WORD<1-32> dir out**

## Command Parameters

**dir <both|in|out>**

Specifies the direction to which IPsec applies. Both specifies both ingress and egress traffic, in specifies ingress traffic, and out specifies egress traffic. By default, the direction is both.

WORD<1-32>

Specifies the IPsec policy name.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 mld last-listener-query-interval (for a port)

Configure the last listener query interval for the MLD

## Syntax

- **default ipv6 mld last-member-query-interval**
- **ipv6 mld last-listener-query-interval <0-60>**
- **no ipv6 mld last-member-query-interval**

## Command Parameters

<0-60>

Indicates the last listener query interval in seconds.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 mld query-interval (for a port)

Configure the query interval for the MLD interface

## Syntax

- **default ipv6 mld query-interval**
- **ipv6 mld query-interval <1-65535>**
- **no ipv6 mld query-interval**

## Command Parameters

<1-65535>

Indicates the frequency at which MLD host query packets transmit on this interface.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 mld query-max-response (for a port)

Configure the query maximum response time for mld interface

## Syntax

- **default ipv6 mld query-max-response**
- **ipv6 mld query-max-response <0-60>**
- **no ipv6 mld query-max-response**

## Command Parameters

<0-60>

Indicates the query maximum response interval time in seconds.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 mld robust-value (for a port)

Configure the MLD robustness

## Syntax

- **default ipv6 mld robust-value**
- **ipv6 mld robust-value <2-255>**
- **no ipv6 mld robust-value**

## Command Parameters

<2-255>

Specifies a numerical value for MLD snooping robustness.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 mld version (for a port)

Configure MLD version

## Syntax

- **default ipv6 mld version**
- **ipv6 mld version <1-2>**
- **no ipv6 mld version**

## Command Parameters

<1-2>

Indicates the version of MLD that runs on this interface.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd (for a port)

Configure the neighbor discovery parameters of the interface.

## Syntax

- **default ipv6 nd**
- **default ipv6 nd hop-limit**
- **default ipv6 nd mtu**
- **default ipv6 nd reachable-time**

- **default ipv6 nd retransmit-timer**
- **ipv6 nd hop-limit <0-255>**
- **ipv6 nd mtu <0-9500>**
- **ipv6 nd reachable-time <0-3600000>**
- **ipv6 nd retransmit-timer <0-4294967295>**
- **no ipv6 nd**
- **no ipv6 nd hop-limit**
- **no ipv6 nd mtu**
- **no ipv6 nd reachable-time**
- **no ipv6 nd retransmit-timer**

## Command Parameters

**hop-limit <0-255>**

Sets the neighbor discovery hop-limit value for the interface.

**mtu <0-9500>**

Sets router advertisement MTU size.

**reachable-time <0-3600000>**

Sets router advertisement reachable time.

**retransmit-timer <0-4294967295>**

Sets router advertisement retransmit timer.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 nd dad-ns (for a port)

---

Configure the number of neighbor solicitation messages from duplicate address detection.

## Syntax

- **default ipv6 nd dad-ns**
- **ipv6 nd dad-ns <0-600>**

## Command Parameters

**<0-600>**

Configures the number of neighbor solicitation messages from duplicate address detection. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions.

## Default

The default is 1.

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd hop-limit (for a port)

Configure the hop limit sent in router advertisements.

## Syntax

- **default ipv6 nd hop-limit**
- **ipv6 nd hop-limit <0-255>**
- **no ipv6 nd hop-limit**

## Command Parameters

**hoplimit <0-255>**

Specifies the current hop limit field sent in router advertisements from this interface. The value must be the current diameter of the Internet. A value of zero indicates that the advertisement does not specify a hop-limit value.

## Default

The default is 64.

## Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd managed-config-flag (for a port)

Enable M-bit (managed address configuration) on the router.

## Syntax

- **default ipv6 nd managed-config-flag**
- **ipv6 nd managed-config-flag**
- **no ipv6 nd managed-config-flag**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 nd mtu (for a port)

---

Configure the maximum transmission unit (MTU) for router advertisements.

## Syntax

- **default ipv6 nd mtu**
- **ipv6 nd mtu <0-9500>**
- **no ipv6 nd mtu**

## Command Parameters

**mtu <0-9500>**

Shows the MTU value sent in router advertisements on this interface. A value of zero indicates that the system sends no MTU options. Valid values are: 0, 1280-1500, 1850, or 9500.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 nd other-config-flag (for a port)

---

Enable the O-bit (other stateful configuration) in the router advertisement. Other stateful configuration autoConfigure received information without addresses.

## Syntax

- **default ipv6 nd other-config-flag**
- **ipv6 nd other-config-flag**
- **no ipv6 nd other-config-flag**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 nd prefix (for a port)

---

Configure neighbor discovery prefixes. IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by ARP and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

## Syntax

- **default ipv6 nd prefix WORD<0-255>**
- **default ipv6 nd prefix WORD<0-255> no-advertise**
- **default ipv6 nd prefix WORD<0-255> preferred-life**
- **default ipv6 nd prefix WORD<0-255> valid-life**
- **ipv6 nd prefix WORD<0-255> infinite**
- **ipv6 nd prefix WORD<0-255> no-advertise**
- **ipv6 nd prefix WORD<0-255> preferred-life <0-4294967295>**
- **ipv6 nd prefix WORD<0-255> valid-life <0-4294967295>**
- **no ipv6 nd prefix WORD<0-255>**
- **no ipv6 nd prefix WORD<0-255> no-advertise**
- **no ipv6 nd prefix-interface WORD<0-255>**
- **no ipv6 nd prefix-interface WORD<0-255> no-advertise**

## Command Parameters

### **infinite**

Configures the prefix as infinite.

### **no-advertise**

Removes the prefix from the neighbor advertisement. The default for noadvertise is disabled.

### **preferred-life <0-4294967295>**

Configures the preferred life, in seconds. The valid range is 0-4294967295. The default preferred-life is 604800.

### **valid-life <0-4294967295>**

Configures the valid life, in seconds. The valid range is 0-4294967295. The default valid-life is 2592000.

## Default

None



## Command Mode

GigabitEthernet Interface Configuration

### ipv6 nd prefix-interface (for a port)

---

Configure neighbor discovery prefixes IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by Address Resolution Protocol (ARP) and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

#### Syntax

- **default ipv6 nd prefix-interface WORD<0-255>**
- **default ipv6 nd prefix-interface WORD<0-255> no-advertise**
- **ipv6 nd prefix-interface WORD<0-255>**
- **ipv6 nd prefix-interface WORD<0-255> eui <1-3>**
- **ipv6 nd prefix-interface WORD<0-255> no-advertise**
- **ipv6 nd prefix-interface WORD<0-255> no-autoconfig**
- **ipv6 nd prefix-interface WORD<0-255> no-onlink**
- **no ipv6 nd prefix-interface WORD<0-255> [no-advertise]**

#### Command Parameters

**eui <1-3>**

Specifies if extended unique identifier (EUI) is used. The values are:(1) EUI not used (2) EUI with Universal/Local bit (U/L) complement enabled (3) EUI used without U/L.

**no-advertise**

Removes the prefix from the neighbor advertisement. The default is disabled.

**no-autoconfig**

Configures if the prefix is used for autonomous address configuration.

**no-onlink**

Configures if onlink determination uses the prefix. This value is placed in the L-bit field in the prefix information option and is a 1-bit flag.

**WORD <0-255>**

Specifies the IPv6 address prefix.

#### Default

None

#### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd ra-lifetime (for a port)

---

Configure the router lifetime included in router advertisement. Other devices use this information to determine if the router can be reached.

### Syntax

- **default ipv6 nd ra-lifetime**
- **ipv6 nd ra-lifetime <0-9000>**

### Command Parameters

<0-9000>

Configures the router lifetime included in router advertisement. The range is 0 or <4-9000>.

### Default

The default is 1800.

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd reachable-time (for a port)

---

Configure the neighbor reachable time.

### Syntax

- **ipv6 nd reachable-time <0-3600000>**

### Command Parameters

reachable-time <0-3600000>

Specifies a value (in milliseconds) placed in the router advertisement message sent by the router. The value zero means unspecified (by this system).

Configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event.

### Default

None

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd retransmit-timer (for a port)

---

Configure the time between neighbor solicitation messages.

### Syntax

- **ipv6 nd retransmit-timer <0-4294967295>**

### Command Parameters

**retransmit-timer <0-4294967295>**

Specifies a value (in milliseconds) placed in the retransmit timer field in the router advertisement message sent from this interface. The value zero means unspecified (by this system).

The value configures the amount of time the system waits for the transmission to occur.

### Default

None

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd rtr-advert-max-interval (for a port)

---

Configure the maximum time allowed between sending unsolicited multicast router advertisements.

### Syntax

- **default ipv6 nd rtr-advert-max-interval**
- **ipv6 nd rtr-advert-max-interval <4-1800>**

### Command Parameters

**<4-1800>**

Specifies the maximum interval value.

### Default

The default is 600.

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd rtr-advert-min-interval (for a port)

---

Configure the minimum time allowed between sending unsolicited multicast router advertisements from the interface.

### Syntax

- **default ipv6 nd rtr-advert-min-interval**
- **ipv6 nd rtr-advert-min-interval <3-1350>**

### Command Parameters

<3-1350>

Configures the minimum time, in seconds.

### Default

The default is 200.

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd send-ra (for a port)

---

Enable or disables periodic router advertisement messages.

### Syntax

- **default ipv6 nd send-ra**
- **ipv6 nd send-ra**
- **no ipv6 nd send-ra**

### Default

The default is enabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 nd valid-life (for a port)

---

Modify an existing neighbor discovery prefix. Configure the valid lifetime in seconds that indicates the length of time this prefix is advertised.

## Syntax

- **ipv6 nd prefix WORD<0-255> valid-life <0-4294967295>**

## Command Parameters

**valid-life <0-4294967295>**

Configures the valid lifetime in seconds that indicates the length of time this prefix is advertised. The default is 2592000.

A valid lifetime is the length of time of the preferred and depreciated state of an auto configuration address.

**WORD<0-255>**

Specifies the IPv6 address and prefix.

## Default

The default is 2592000.

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 ospf (for a port)

---

Configure OSPFv3 on an interface.

## Syntax

- **default ipv6 ospf**
- **default ipv6 ospf cost**
- **default ipv6 ospf dead-interval**
- **default ipv6 ospf enable**
- **default ipv6 ospf hello-interval**
- **default ipv6 ospf link-lsa-suppression**
- **default ipv6 ospf nbma-nbr WORD<0-43>**
- **default ipv6 ospf poll-interval**
- **default ipv6 ospf priority**
- **default ipv6 ospf retransmit-interval**
- **default ipv6 ospf transit-delay**
- **ipv6 ospf cost <0-65535>**
- **ipv6 ospf dead-interval <1-65535>**
- **ipv6 ospf enable**
- **ipv6 ospf hello-interval <1-65535>**

- **ipv6 ospf nbma-nbr WORD<0-43> <0-255>**
- **ipv6 ospf nbma-nbr WORD<0-43> priority <0-255>**
- **ipv6 ospf poll-interval <0-65535>**
- **ipv6 ospf priority <0-255>**
- **ipv6 ospf retransmit-interval <1-1800>**
- **ipv6 ospf transit-delay <1-1800>**
- **no ipv6 ospf**
- **no ipv6 ospf enable**
- **no ipv6 ospf link-lsa-suppression**
- **no ipv6 ospf nbma-nbr WORD<0-43>**

## Command Parameters

### **cost <0-65535>**

Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. The default is 1.

### **dead-interval <1-65535>**

Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default is 40.

### **enable**

Enables the OSPF on the IPv6 interface.

### **hello-interval <1-65535>**

Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default is 10.

### **link-lsa-suppression**

Enables link lsa suppression

### **nbma-nbr WORD<0-43>**

Configures an NBMA neighbor. WORD<0-43> specifies the IPv6 address. Use priority <0-255> to change an existing priority value for an NBMA neighbor. Use <0-255> to assign the priority value when you create the neighbor.

### **poll-interval <0-65535>**

Configures the polling interval for the OSPF interface in seconds. The default is 120.

### **priority <0-255>**

Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router.

If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The default is 1.

### **retransmit-interval <1-1800>**

Specifies the retransmit interval, in seconds, for link-state advertisements. The default is 5.

**transit-delay <1-1800>**

Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default is 1.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 ospf area (for a port)

---

Configure an OSPFv3 area on an interface.

## Syntax

- **ipv6 ospf area {A.B.C.D}**
- **ipv6 ospf area {A.B.C.D} cost <0-65535>**
- **ipv6 ospf area {A.B.C.D} dead-interval <1-65535>**
- **ipv6 ospf area {A.B.C.D} hello-interval <1-65535>**
- **ipv6 ospf area {A.B.C.D} network eth**
- **ipv6 ospf area {A.B.C.D} network nbma**
- **ipv6 ospf area {A.B.C.D} network p2mp**
- **ipv6 ospf area {A.B.C.D} network p2p**
- **ipv6 ospf area {A.B.C.D} network passive**
- **ipv6 ospf area {A.B.C.D} priority <0-255>**
- **ipv6 ospf area {A.B.C.D} retransmit-interval <1-1800>**
- **ipv6 ospf area {A.B.C.D} transit-delay <1-1800>**

## Command Parameters

**area {A.B.C.D}**

Creates an IPv6 OSPF area.

**cost <0-65535>**

Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. The default is 1.

**dead-interval <1-65535>**

Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default is 40.

**hello-interval <1-65535>**

Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default is 10.

**network <eth|nbma|p2mp|p2p|passive>**

Configures the type of interface as one of the following: eth: broadcast, nbma: NBMA, p2mp: point-to-multipoint, p2p:pointto-point, or passive: passive interface.

**priority <0-255>**

Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router.

If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The default is 1.

**retransmit-interval <1-1800>**

Specifies the retransmit interval, in seconds, for link-state advertisements. The default is 5.

**transit-delay <1-1800>**

Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default is 1.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 ospf bfd

---

Enable Bidirectional Forwarding Detection (BFD) for an OSPF GigabitEthernet IPv6 interface.

## Syntax

- **ipv6 ospf bfd**
- **ipv6 ospf bfd disable**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration



## Usage Guidelines

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipv6 pim enable (for a port)

---

Enable PIM globally on the switch.

### Syntax

- **default ipv6 pim enable**
- **ipv6 pim enable**
- **no ipv6 pim enable**

### Default

The default is disabled

### Command Mode

GigabitEthernet Interface Configuration

## ipv6 pim hello-interval (for a port)

---

Configure the time between hello messages.

### Syntax

- **default ipv6 pim hello-interval**
- **ipv6 pim hello-interval <0-18724>**

### Command Parameters

<0-18724>

Specifies the duration in seconds before the PIM router sends out the next hello message to neighboring switches.

### Default

The default is 30 seconds

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 pim join-prune-interval (for a port)

---

Configure the interval for join and prune messages.

### Syntax

- **default ipv6 pim join-prune-interval**
- **ipv6 pim join-prune-interval <1-18724>**

### Command Parameters

<1-18724>

Specifies the duration in seconds before the PIM router sends out the next join or prune message to its upstream neighbors.

### Default

The default is disabled

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 rip cost (for a port )

---

Configure the RIPng cost for this port (link).

### Syntax

- **default ipv6 rip cost**
- **ipv6 rip cost <1-15>**

### Command Parameters

<1-15>

Specifies the cost value.

### Default

None

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 rip poison enable (for a port)

---

Enable poison reverse.

### Syntax

- **default ipv6 rip poison enable**
- **ipv6 rip poison enable**
- **no ipv6 rip poison enable**

### Default

The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## ipv6 rvs-path-chk

---

Configure unicast reverse path forwarding on a port (IPv4).

### Syntax

- **default ipv6 rvs-path-chk**
- **default ipv6 rvs-path-chk mode**
- **ipv6 rvs-path-chk**
- **ipv6 rvs-path-chk mode exist-only**
- **ipv6 rvs-path-chk mode strict**
- **no ipv6 rvs-path-chk**

### Command Parameters

**mode {strict|exist-only}**

Specifies the mode for Unicast Reverse Path Forwarding (uRPF).

- In strict mode, uRPF checks whether the source IP address of the incoming packet exists in the FIB. If the incoming interface is not the best reverse path, the packet check fails and uRPF drops the packet.
- In exist-only mode, uRPF checks whether the source IP address of the incoming packet exists in the FIB. The packet is dropped only if the source address is not reachable via any interface on that router.

### Default

None

## Command Mode

GigabitEthernet Interface Configuration

### ipv6 source-guard

---

Configures IP Source Guard (IPSG) on a port, for IPv6 addresses. When you enable IPSG on the port, filters are automatically installed for the IPv6 addresses that are already learned on that interface.

#### Syntax

- **default ipv6 source-guard enable**
- **ipv6 source-guard enable**
- **ipv6 source-guard max-allowed-addr <2-10>**
- **ipv6 source-guard overflow-count clear**
- **no ipv6 source-guard enable**

#### Command Parameters

##### enable

Enables IPSG on a port, for IPv6 addresses. When you enable IPSG on the port, filters are automatically installed for the IPv6 addresses that are already learned on that interface.

##### max-allowed-addr <2-10>

Configures the maximum number of IPv6 addresses allowed on the port. The default value is 4.

##### overflow-count clear

Clears the IPSG overflow counters. Overflow counters consists of IPv6 addresses that are not added to IPSG due to lack of filter resources.

On the switch, the total number of filters cannot exceed 256. This limit includes the filters for IPSG and the manually created ACLs.

#### Default

IPSG for IPv6 addresses is disabled by default.

## Command Mode

GigabitEthernet Interface Configuration

### ipv6 vrrp (for a port)

---

Configure Virtual Router Redundancy Protocol (VRRP) to provide fast failover of a default router for IPv6 LAN hosts. VRRP supports a virtual IPv6 address shared between two or more routers that connect the common subnet to the enterprise network. VRRP for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol.

## Syntax

- `default ipv6 vrrp <1-255>`
- `default ipv6 vrrp <1-255> accept-mode enable`
- `default ipv6 vrrp <1-255> action`
- `default ipv6 vrrp <1-255> adver-int`
- `default ipv6 vrrp <1-255> backup-master enable`
- `default ipv6 vrrp <1-255> critical-ipv6 enable`
- `default ipv6 vrrp <1-255> critical-ipv6-addr`
- `default ipv6 vrrp <1-255> enable`
- `default ipv6 vrrp <1-255> fast-adv enable`
- `default ipv6 vrrp <1-255> fast-adv-int`
- `default ipv6 vrrp <1-255> holddown-timer`
- `default ipv6 vrrp <1-255> preempt-mode`
- `default ipv6 vrrp <1-255> priority`
- `ipv6 vrrp <1-255> accept-mode enable`
- `ipv6 vrrp <1-255> action none`
- `ipv6 vrrp <1-255> action preempt`
- `ipv6 vrrp <1-255> adver-int <1..40>`
- `ipv6 vrrp <1-255> backup-master enable`
- `ipv6 vrrp <1-255> critical-ipv6 enable`
- `ipv6 vrrp <1-255> critical-ipv6-addr WORD<0-46>`
- `ipv6 vrrp <1-255> enable`
- `ipv6 vrrp <1-255> fast-adv enable`
- `ipv6 vrrp <1-255> fast-adv-int <200-1000>`
- `ipv6 vrrp <1-255> holddown-timer <0-21600>`
- `ipv6 vrrp <1-255> preempt-mode enable`
- `ipv6 vrrp <1-255> priority <1-255>`
- `no ipv6 vrrp <1-255>`
- `no ipv6 vrrp <1-255> accept-mode enable`
- `no ipv6 vrrp <1-255> backup-master enable`
- `no ipv6 vrrp <1-255> critical-ipv6 enable`
- `no ipv6 vrrp <1-255> enable`
- `no ipv6 vrrp <1-255> fast-adv enable`
- `no ipv6 vrrp <1-255> preempt-mode enable`

## Command Parameters

<1-255>

Specifies a number that uniquely identifies a virtual router on an interface. The virtual router acts as the default router for one or more assigned addresses.

**<1-255> preempt-mode enable**

Enable IPv6 vrrp preempt mode.

**accept-mode enable**

Controls whether a master router accepts packets addressed to the IPv6 address of the address owner as its own if it is not the IPv6 address owner. The default accept-mode enable is disabled.

**action <none|preempt>**

Lists options to override the holddown timer manually and force preemption. None does not override the timer. preempt preempts the timer. This parameter applies only if the holddown timer is active.

**adver-int <1-40>**

Specifies the time interval, in seconds, between sending advertisement messages. Only the master router sends advertisements. The default is 1.

**backup-master enable**

Uses the backup Virtual Router Redundancy Protocol (VRRP) switch for traffic forwarding. This option reduces the traffic on the IST link. The default backupmaster enable is disabled.

**critical-ip enable**

Enables or disables the use of critical IP. When disabled, the Virtual Router Redundancy Protocol (VRRP) ignores the availability of the address configured as critical IP. This address must be a local address.

**critical-ip-addr WORD<0-46>**

Specifies an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface stops responding. The default critical-ip enable is disabled.

**enable**

Enables IPv6 Virtual Router Redundancy Protocol (VRRP). The default is disabled.

**fast-adv enable**

Enables or disables the fast advertisement interval. When disabled, the regular advertisement interval is used. The default fast-adv-int is 200.

**fast-adv-int <200-1000>**

Configures the interval between Virtual Router Redundancy Protocol (VRRP) advertisement messages. You must configure the same value on all participating routers. This unit of measure must be in multiples of 200 milliseconds.

**holddown-timer<0-21600>**

Configures the amount of time, in seconds, to wait before preempting the current Virtual Router Redundancy Protocol (VRRP) master. The default holddown timer is 0.

**priority <1-255>**

Specifies the priority value used by this Virtual Router Redundancy Protocol (VRRP) router. The value 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default priority is 100.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## ipv6 vrrp address (for a port)

---

Specify a link-local address to associate with the virtual router. Optionally, you can also assign global unicast IPv6 addresses to associate with the virtual router. Network prefixes for the virtual router are derived from the global IPv6 addresses assigned to the virtual router.

## Syntax

- **default ipv6 vrrp address <1-255>**
- **ipv6 vrrp address <1-255> global WORD<0-225>**
- **ipv6 vrrp address <1-255> link-local WORD<0-127>**
- **no ipv6 vrrp address <1-255>**
- **no ipv6 vrrp address <1-255> global WORD<0-225>**

## Command Parameters

**<1-255>**

Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.

**global WORD<0-255>**

Specifies a global IPv6 address to associate with the virtual router.

**link-local WORD<0-127>**

Specifies a link-local IPv6 address to associate with the virtual router.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## i-sid (for a port)

---

Create Switched UNI (S-UNI) service instance identifiers (I-SID).

## Syntax

- **i-sid <1-16777215> elan**

## Command Parameters

<1-16777215>

Specifies the I-sid number.

**elan**

Create an elan based service.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## isis (on a port)

---

Create an Intermediate-System-to-Intermediate-System (IS-IS) circuit and interface on the selected ports.

## Syntax

- **default isis enable**
- **isis**
- **isis enable**
- **no isis**
- **no isis enable**

## Command Parameters

**enable**

Enables the Intermediate-System-to-Intermediate-System (IS-IS) circuit and interface on the selected ports.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration



## isis hello-auth (on a port)

Specify the authentication type used for Intermediate-System-to-Intermediate-System (IS-IS) hello packets on the interface. The type can be one of the following: none, hmac-md5, or hmac-sha-256.

### Syntax

- **default isis hello-auth**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 }**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 } key WORD<1-16>**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 } key WORD<1-16> key-id <1-255>**
- **no isis hello-auth**

### Command Parameters

**key WORD<1-16>**

Specifies the authentication key (password) used by the receiving router to verify the packet.

**key-id <1-255>**

Specifies the optional key ID.

**type { none | simple | hmac-md5 | hmac-sha-256 }**

Specifies the authentication type used for IS-IS hello packets on the interface. The type can be one of the following: none, simple, hmac-md5, or hmac-sha-256. The default type is none. Use the no or default options to set the hello-auth type to none.

- If simple is selected, you can also specify a key value. Simple password authentication uses a text password in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet.
- If hmac-md5 is selected, you can also specify a key value and key-id. MD5 authentication creates an encoded checksum in the transmitted packet. The receiving router uses an authentication key (password) to verify the MD5 checksum of the packet.
- If hmac-sha-256 is selected, you can also specify a key value and key-id. With SHA-256 authentication, the switch adds an HMAC-SHA256 digest to each Hello packet. The switch that receives the Hello packet computes the digest of the packet and compares it with the received digest. If the digests match, the packet is accepted. If the digests do not match, the receiving switch discards the packet.

### Default

The default is no authentication type (none).

### Command Mode

GigabitEthernet Interface Configuration

---

## isis l1-dr-priority (on a port)

---

Configure the Level 1 Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

### Syntax

- **default isis l1-dr-priority**
- **isis l1-dr-priority <0-127>**
- **no isis l1-dr-priority**

### Command Parameters

<0-127>

Configures the Level 1 Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

### Default

The default Level 1 designated router priority value is 64.

### Command Mode

GigabitEthernet Interface Configuration

---

## isis l1-hello-interval (on a port)

---

Configure the hello interval to change how often hello packets are sent out from an interface level.

### Syntax

- **default isis l1-hello-interval**
- **isis l1-hello-interval <1-600>**
- **no isis l1-hello-interval**

### Command Parameters

<1-600>

Configures the Level 1 hello interval.

### Default

The default Level 1 hello interval value is 9 seconds.

## Command Mode

GigabitEthernet Interface Configuration

### isis l1-hello-multiplier (on a port)

---

Configure the hello multiplier to specify how many hellos the switch must miss before it considers the adjacency with a neighboring switch down.

#### Syntax

- **default isis l1-hello-multiplier**
- **isis l1-hello-multiplier <1-600>**
- **no isis l1-hello-multiplier**

#### Command Parameters

<1-600>

Configures the Level 1 hello multiplier.

#### Default

The default Level 1 hello-multiplier value is 3 seconds.

## Command Mode

GigabitEthernet Interface Configuration

### isis remote

---

Enables the remote Intermediate-System-to-Intermediate-System (IS-IS) interface on the selected port(s).



#### Note

When the switch receives a Fabric Connect TLV through LLDP on a port that has remote IS-IS enabled on it, the port transitions to the Auto-sense NNI pending state. For more information about the Auto-sense port states, see [VOSS User Guide](#).

#### Syntax

- **default isis remote**
- **default isis remote enable**
- **isis remote**
- **isis remote enable**
- **no isis remote**
- **no isis remote enable**

## Command Parameters

### enable

Enables the remote Intermediate-System-to-Intermediate-System (IS-IS) interface on the selected ports.

## Default

The default is none.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis remote hello-auth

---

Specify the authentication type used for remote Intermediate-System-to-Intermediate-System (IS-IS) hello packets on the interface. The type can be none, simple, hmac-md5, or hmac-sha-256.

## Syntax

- **default isis remote hello-auth**
- **isis remote hello-auth type { none | simple | hmac-md5 | hmac-sha-256 }**
- **isis remote hello-auth type { none | simple | hmac-md5 | hmac-sha-256 } key WORD<1-16>**
- **isis remote hello-auth type { none | simple | hmac-md5 | hmac-sha-256 } key WORD<1-16> key-id <1-255>**
- **no isis remote hello-auth**

## Command Parameters

### key WORD<1-16>

Specifies the authentication key (password) that the receiving router uses to verify the packet.

### key-id <1-255>

Specifies the optional key ID.

### type { none | simple | hmac-md5 | hmac-sha-256 }

Specifies the authentication type used for remote IS-IS hello packets on the interface. The type can be one of the following:

- **Simple** - Simple password authentication uses a text password in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet. You can also specify a key value.
- **hmac-md5** - MD5 authentication creates an encoded checksum in the transmitted packet. The receiving router uses an authentication key (password) to verify the MD5 checksum of the packet. You can also specify a key value and key-id.
- **hmac-sha-256** - With SHA-256 authentication, the switch adds an HMAC-SHA256 digest to each Hello packet. The switch that receives the Hello packet computes the digest of the packet and compares it with the received digest. If the digests match, the packet is accepted. If the digests do not match, the receiving switch discards the packet. You can also specify a key value and key-id.

The default type is none.

## Default

The default is no authentication type (none).

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis remote l1-dr-priority

---

Configure the Level 1 remote Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

## Syntax

- **default isis remote l1-dr-priority**
- **isis remote l1-dr-priority <0-127>**
- **no isis remote l1-dr-priority**

## Command Parameters

<0-127>

Configures the Level 1 remote IS-IS designated router priority to the specified value.

## Default

The default Level 1 designated router priority value is 64.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis remote l1-hello-interval

---

Configure the remote hello interval to change how often hello packets are sent out from an interface level.

## Syntax

- **default isis remote l1-hello-interval**
- **isis remote l1-hello-interval <1-600>**
- **no isis remote l1-hello-interval**

## Command Parameters

<1-600>

Configures the Level 1 remote hello interval.

## Default

The default Level 1 remote hello interval value is 9 seconds.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis remote l1-hello-multiplier

---

Configures the remote hello multiplier to specify how many hellos the switch must miss before it considers the adjacency with a neighboring switch down.

## Syntax

- **default isis remote l1-hello-multiplier**
- **isis remote l1-hello-multiplier <1-600>**
- **no isis remote l1-hello-multiplier**

## Command Parameters

<1-600>

Configures the level 1 hello multiplier.

## Default

The default Level 1 hello multiplier value is 3.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis remote spbm

---

Enable the Shortest Path Bridging MAC (SPBM) instance on the remote Intermediate-System-to-Intermediate-System (IS-IS) interfaces.

## Syntax

- **default isis remote spbm <1-100> interface-type**
- **default isis remote spbm <1-100> l1-metric**
- **isis remote spbm <1-100>**
- **isis remote spbm <1-100> interface-type { broadcast | pt-pt }**
- **isis remote spbm <1-100> l1-metric <1-16777215>**
- **no isis remote spbm <1-100>**
- **no isis remote spbm <1-100> interface-type**
- **no isis remote spbm <1-100> l1-metric**

## Command Parameters

spbm <1-100>

Specifies the SPBM instance ID.

interface-type { broadcast | pt-pt }

Configures the remote SPBM instance interface type.

**l1-metric <1-16777215>**

Configures the cost for the remote SPBM instance.

## Default

The default is none.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis spbm (on a port)

---

Enable the Shortest Path Bridging MAC (SPBM) instance on the Intermediate-System-to-Intermediate-System (IS-IS) interfaces.

## Syntax

- **default isis spbm <1-100> interface-type**
- **default isis spbm <1-100> l1-metric**
- **isis spbm <1-100>**
- **isis spbm <1-100> interface-type { broadcast | pt-pt }**
- **isis spbm <1-100> l1-metric <1-16777215>**
- **no isis spbm <1-100>**
- **no isis spbm <1-100> interface-type**
- **no isis spbm <1-100> l1-metric**

## Command Parameters

**<1-100>**

Specifies the Shortest Path Bridging MAC (SPBM) instance ID.

**interface-type { broadcast | pt-pt }**

Configures the Shortest Path Bridging MAC (SPBM) instance interface type.

**l1-metric <1-16777215>**

Configures the cost for the Shortest Path Bridging MAC (SPBM) instance.



## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## lACP aggregation enable

Configures the port as aggregatable. Use the no operator to remove this configuration.

## Syntax

- **default lACP aggregation enable**
- **lACP aggregation enable**
- **no lACP aggregation enable**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## lACP aggr-wait-time

Configure the aggregation wait time (in milliseconds) for the port.

## Syntax

- **lACP aggr-wait-time <200-2000>**

## Command Parameters

**<200-2000>**

Specifies the Aggregation time in milliseconds. The default is 2000.

## Default

The default value is 2000.

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp enable (for a port)

---

Enable LACP for the port.

### Syntax

- **default lacp**
- **default lacp enable**
- **lacp enable**
- **no lacp**
- **no lacp enable**

### Default

The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## lacp fast-periodic-time

---

Configure the fast-periodic time (in milliseconds) for the port.

### Syntax

- **default lacp fast-periodic-time**
- **lacp fast-periodic-time <200-20000>**

### Command Parameters

<200-20000>

Specifies the Fast periodic time value in milliseconds. The default is 20000 ms.

### Default

The default is 20000 ms.

### Command Mode

GigabitEthernet Interface Configuration

---

## lacp key

---

Configure the aggregation key for the port.

## Syntax

- **default lacp key**
- **lacp key <1-512,defVal>**

## Command Parameters

<1-512,defVal>

Specifies the aggregation key for this port.

## Default

The default is 0.

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp mode

Configure the Link Aggregation Control Protocol (LACP) mode to be active or passive.

## Syntax

- **default lacp mode**
- **lacp mode active**
- **lacp mode passive**

## Command Parameters

**active**

Specifies the Link Aggregation Control Protocol (LACP) mode to be active.

**passive**

Specifies the Link Aggregation Control Protocol (LACP) mode to be passive.

## Default

The default is passive.

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp partner-key

Configure the partner administrative key.

## Syntax

- **default lacp partner-key**
- **lacp partner-key <0-65535>**

## Command Parameters

<0-65535>

Specifies the partner administrative key.

## Default

The default is 0.

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp partner-port

Configure the partner administrative port value.

## Syntax

- **default lacp partner-port**
- **lacp partner-port <0-65535>**

## Command Parameters

<0-65535>

Specifies the partner administrative port value.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp partner-port-priority

Configure the partner administrative port priority value.

## Syntax

- **default lacp partner-port-priority**

- **lacp partner-port-priority <0-65535>**

## Command Parameters

<0-65535>

Specifies the partner administrative port priority value.

## Default

The default is 0.

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp partner-state

Configure the partner administrative state bitmask. Specify the partner administrative state bitmap in the range 0x0-0xff. The bit to state mapping is Exp, Def, Dis, Col, Syn, Agg, Time, and Act.

For example, to set the two partner-state parameters Act = true Agg = true specify a value of 0x05 (bitmap = 00000101).

## Syntax

- **default lacp partner-state**
- **lacp partner-state <0-255 | 0x0-0xff>**

## Command Parameters

<0-255 | 0x0-0xff>

Specifies the partner administrative state bitmask.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp partner-system-id

Configure the partner administrative system ID.

## Syntax

- **default lACP partner-system-id**
- **lACP partner-system-id <0x00:0x00:0x00:0x00:0x00:0x00>**

## Command Parameters

<0x00:0x00:0x00:0x00:0x00:0x00>

Specifies the partner administration system ID.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## lACP partner-system-priority

Configure the partner administrative system priority value.

## Syntax

- **default lACP partner-system-priority**
- **lACP partner-system-priority <0-65535>**

## Command Parameters

<0-65535>

Specifies the partner administrative system priority value.

## Default

The default value is 32768.

## Command Mode

GigabitEthernet Interface Configuration

---

## lACP priority

Configure the port priority.

## Syntax

- **default lACP priority**

- **lacp priority <0-65535>**

## Command Parameters

<0-65535>

Specifies the port priority.

## Default

The default value is 32768.

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp slow-periodic-time

Configure the slow periodic time.

## Syntax

- **default lacp slow-periodic-time**
- **lacp slow-periodic-time <10000-30000>**

## Command Parameters

<10000-30000>

Specifies the slow periodic time for this port.

## Default

The default value is 1000 ms.

## Command Mode

GigabitEthernet Interface Configuration

---

## lacp system-priority

Configure the LACP system priority.

## Syntax

- **default lacp system-priority**
- **lacp system-priority <0-65535>**

## Command Parameters

<0-65535>

Specifies the system priority for this port.

## Default

The default value is 32768.

## Command Mode

GigabitEthernet Interface Configuration

---

## lACP timeout-scale

Configure the timeout scale.

## Syntax

- **default lACP timeout-scale**
- **lACP timeout-scale <2-10>**

## Command Parameters

<2-10>

Specifies the timeout scale for this port.

## Default

The default is 3.

## Command Mode

GigabitEthernet Interface Configuration

---

## lACP timeout-time

Configure the timeout to either long or short.

## Syntax

- **default lACP timeout-time**
- **lACP timeout-time long**
- **lACP timeout-time short**



## Command Parameters

{long | short}

Specifies the timeout.

## Default

The default is long.

## Command Mode

GigabitEthernet Interface Configuration

---

## link-debounce

Configure Link Debounce time for all ports.

## Syntax

- **default link-debounce**
- **link-debounce <0-300000>**
- **no link-debounce**

## Command Parameters

<0-300000>

Specifies the Link Debounce time threshold in milliseconds.

## Default

The default status is disabled for all ports when not initially configured. If you run the **default link-debounce** command, the default configuration is enabled with a value of 1,000 milliseconds. To return to the initial disabled state, you must run the **no link-debounce** command or set the Link Debounce timer to 0.

## Command Mode

GigabitEthernet Configuration.

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## lldp cpd

Enables Cisco discovery protocol on the interface.

## Syntax

- `lldp cpd enable`
- `no lldp cpd enable`

## Command Parameters

`enable`

Enables Cisco discovery protocol on the selected port(s) to accept CDP packets only.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## lldp location-identification civic-address

---

Configures civic address location information of local Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) on specific ports.



### Note

If you try to configure a civic-address with a large number of arguments, 26 or more, the command fails and a software message informs you to split the command into multiple smaller commands.

## Syntax

- `default lldp location-identification civic-address`
- `lldp location-identification civic-address country-code WORD<2-2> (additional-code additional-information apartment block building city city-district county floor house-number house-number-suffix landmark leading-street-direction name place-type pobox postal community-name postal-zip-code room-number state street street suffix trailing-street-suffix) WORD<0-255>`
- `no lldp location-identification civic-address`

## Command Parameters

`additional-code WORD<0-255>`

Specifies the location information parameters.

`additional-information WORD<0-255>`

Example: South Wing

`apartment WORD<0-255>`

Example: Apt 42

**block WORD<0-255>**

Specifies a block, for example, 3

**building WORD<0-255>**

Example: Low Library.

**city WORD<0-255>**

Specifies a city, for example, Sunnyvale

**city-district WORD<0-255>**

Specifies a city district, for example, Santa Clara

**country-code WORD<2-2>**

Specifies a country using a 2 character string, example US (United States), CA (Canada).

**county WORD<0-255>**

Specifies a county, for example, Alameda

**floor WORD<0-255>**

Example: 8

**house-number WORD<0-255>**

Specifies a house number, for example, 123.

**house-number-suffix WORD<0-255>**

Specifies a house number suffix, for example, A, 1/2.

**landmark WORD<0-255>**

Specifies a landmark, for example, Columbia University.

**leading-street-direction WORD<0-255>**

Specifies a leading street direction, for example, N

**name WORD<0-255>**

Example: Joe's Barbershop

**place-type WORD<0-255>**

Example: office

**pobox WORD<0-255>**

Example: 12345

**postal-community-name WORD<0-255>**

Example: Leonia

**postal-zip-code WORD<0-255>**

Specifies a postal or zip code, for example, 95054

**room-number WORD<0-255>**

Example: 450F

**state WORD<0-255>**

Specifies a state, for example, NJ, FL

**street WORD<0-255>**

Specifies a street, for example, Great America Parkway

**street-suffix WORD<0-255>**

Specifies a street suffix, for example, Ave, Blvd

**trailing-street-suffix WORD<0-255>**

Specifies a trailing street suffix, for example, SW

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## lldp location-identification coordinate

---

Configures coordinate based location information of local LLDP-MED on specific ports.

## Syntax

- **default lldp location-identification coordinate**
- **lldp location-identification coordinate (altitude WORD<1-13> {floors | meters} datum {NAD83/MLLW | NAD83/NAVD88 | WGS84} latitude WORD<1-14> {NORTH | SOUTH} longitude WORD<1-14> {EAST | WEST})**
- **no lldp location-identification coordinate**

## Command Parameters

**{floors | meters}**

Specifies the value.

**altitude WORD<1-13>**

Specifies the value for altitude.

**datum {NAD83/MLLW | NAD83/NAVD88 | WGS84}**

Specifies the type of reference datum.

**latitude WORD<1-14>**

Specifies the latitude in degrees, and its relation to the equator from North or South.

**longitude WORD<1-14>**

Specifies the longitude in degrees, and its relation to the prime meridian from East or West.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## lldp location-identification ecs-elin

---

Configure emergency call service location of local LLDP-MED on specific ports.

### Syntax

- **default lldp location-identification ecs-elin**
- **lldp location-identification ecs-elin WORD<10-25>**
- **no lldp location-identification ecs-elin**

### Command Parameters

WORD<10-25>

Specifies the emergency line information number for emergency call service.

### Default

None

## Command Mode

GigabitEthernet Interface Configuration

## lldp med-network-policies

---

Configures LLDP-MED network policies on specific ports.

### Syntax

- **default lldp med-network-policies {guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling}**
- **lldp med-network-policies {guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling} [dscp <0-63>] [priority <0-7>] [tagging {tagged|untagged}] [vlan-id <0-4059>]**
- **no lldp med-network-policies {guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling}**

## Command Parameters

{guest-voice | guest-voice-signaling | softphone-voice | streaming-video | videoconferencing | video-signaling | voice | voice-signaling}

Specifies the type of LLDP-MED network policy.

**dscp** <0-63>

Specifies the Layer 3 DiffServ Code Point (DSCP) value, as defined in IETF RFC 2474 and RFC 2475.

**priority** <0-7>

Specifies the priority level, as defined in IEEE 802.1D.

**tagging** {tagged | untagged}

Specifies the type of VLAN tagging to apply on the selected ports.

**vlan-id** <0-4059>

Specifies the VLAN ID for the port, as defined in IEEE 802.1Q. If you configure priority tagged frames, the system recognizes only the 802.1D priority level and uses a value of 0 for the VLAN ID of the ingress port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## lldp port

---

Configures LLDP on a port or ports.

## Syntax

- **lldp port** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...] } **cdp**
- **lldp port** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...] } **status** <txAndrx>

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...] }

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**cpd**

Enables Cisco discovery protocol on the selected port(s) to accept CDP packets only.

The default is disabled.

**status <txAndrx>**

Specifies LLDP frames to transmit and receive on the selected port(s).

The default is enabled.

## Default

The default is none.

## Command Mode

GigabitEthernet Interface Configuration

## lldp status

---

Configures LLDP status on the interface.

## Syntax

- **lldp status {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**  
**<txAndrx>**

## Command Parameters

**{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**status <txAndrx>**

Specifies LLDP frames to transmit and receive on the selected port(s).

The default is enabled.

## Default

The default is none.

## Command Mode

GigabitEthernet Interface Configuration

---

## lldp tx-tlv dot3

---

Configures dot3 Link Layer Discovery Protocol (LLDP) TLV.

### Syntax

- `lldp tx-tlv dot3 {mac-phy-config-status}`
- `no lldp tx-tlv dot3 {mac-phy-config-status}`
- `default lldp tx-tlv dot3 {mac-phy-config-status}`

### Default

The default is disabled.

### Command Parameters

`mac-phy-config-status`

Specifies the status of the MAC Physical Config Status TLV. The default is disabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## lldp tx-tlv local-mgmt-addr

---

Configures the local management address TLV.

### Syntax

- `lldp tx-tlv local-mgmt-addr`
- `no lldp tx-tlv local-mgmt-addr`
- `default lldp tx-tlv local-mgmt-addr`

### Default

The default is enabled.

### Command Mode

GigabitEthernet Interface Configuration

---

## lldp tx-tlv med

---

Configure organization-specific TLVs for Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED).



## Syntax

- `lldp tx-tlv med {extendedPSE | inventory | location | med-capabilities | network-policy}`
- `no lldp tx-tlv med {extendedPSE | inventory | location | med-capabilities | network-policy}`
- `default lldp tx-tlv med {extendedPSE | inventory | location | med-capabilities | network-policy}`

## Command Parameters

### extendedPSE

Enables advanced power management between an LLDP-MED network connectivity and endpoint devices. The TLV enables the advertisement of fine grained power requirement details, endpoint power priority, and power status for network connectivity and endpoint devices.

The default is enabled for devices that support PoE.

### inventory

Specifies tracking and identification of inventory-related attributes for endpoint devices.

The default is enabled.

### location

Enables the network connectivity devices to advertise location information, including emergency call service location for communication endpoint devices.

The default is enabled.

### med-capabilities

Enables a network element to determine if connected devices support LLDP-MED

The default is enabled.

### network-policy

Enables network connectivity and endpoint devices advertise VLAN information, Layer 2, and Layer 3 priorities associated with a specific set of applications on a port. An LLDP-MED endpoint advertises this TLV for supported application types to enable the discovery of specific policy information and the diagnosis of network policy configuration mismatch issues.

The default is enabled.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

### lldp tx-tlv port-desc

---

Configures the port description transmission TLV.

#### Syntax

- **lldp tx-tlv port-desc**
- **no lldp tx-tlv port-desc**
- **default lldp tx-tlv port-desc**

#### Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

### lldp tx-tlv sys-cap

---

Configures the system capabilities transmission TLV.

#### Syntax

- **lldp tx-tlv sys-cap**
- **no lldp tx-tlv sys-cap**
- **default lldp tx-tlv sys-cap**

#### Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

### lldp tx-tlv sys-desc

---

Configures the system description transmission TLV.

#### Syntax

- **lldp tx-tlv sys-desc**

- **no lldp tx-tlv sys-desc**
- **default lldp tx-tlv sys-desc**

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## lldp tx-tlv sys-name

Configures the system name transmission TLV.

## Syntax

- **lldp tx-tlv sys-name**
- **no lldp tx-tlv sys-name**
- **default lldp tx-tlv sys-name**

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## lock

Lock a port to prevent other users from changing port parameters or modifying port action.

## Syntax

- **default lock**
- **default lock enable**
- **default lock port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **lock**
- **lock enable**
- **no lock**
- **no lock enable**

## Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## macsec actor-priority

Specifies priority for key-server election.

## Syntax

- **macsec actor-priority** <0x00-0xff>
- **default macsec actor-priority**

## Command Parameters

<0x00-0xff>

Specifies a hexadecimal priority value for key server election. Lower values have higher priorities.

## Default

The default is 10.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## macsec cipher-suite

---

Configures the MACsec cipher suite on a switch port for enhanced traffic security. MACsec supports two cipher suites, the GCM-AES-128 with a maximum key length of 128 bits and the GCM-AES-256 with a maximum key length of 256 bits.

Configuring a MACsec cipher suite is optional and is not supported on all hardware platforms.

### Syntax

- **default macsec cipher-suite**
- **macsec cipher-suite gcm-aes-128**
- **macsec cipher-suite gcm-aes-256**

### Command Parameters

{gcm-aes-128 | gcm-aes-256}

Specifies the MACsec encryption cipher suite.

### Default

The default is the 128-bit cipher suite.

### Command Mode

GigabitEthernet Interface Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## macsec confidentiality-offset

---

Encrypts the data following the Ethernet header based on the provided offset.

### Syntax

- **macsec confidentiality-offset <30-50>**
- **no macsec confidentiality-offset**

### Command Parameters

<30-50>

Enter the value of confidentiality offset to be achieved. Only 30 and 50 are valid values.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## macsec connectivity-association (to a port)

Associate a port with a connectivity-association (CA).

## Syntax

- **macsec connectivity-association WORD<5-15>**
- **no macsec connectivity-association WORD<5-15>**

## Command Parameters

WORD<5-15>

Specifies an existing connectivity-association name. It is a 5 to 15 character alphanumeric string.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## macsec enable

Enable MACsec on the specified port.

## Syntax

- **macsec enable**

- **no macsec enable**

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## macsec encryption

Enable encryption for the frames transmitted on MACsec enabled port.

## Syntax

- **macsec encryption**
- **no macsec encryption**

## Command Parameters

**encryption**

Enables encryption for the frames transmitted on MACsec enabled port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## macsec mka enable

Enable MKA on a port.

## Syntax

- **macsec mka enable**
- **no macsec mka enable**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## macsec mka profile

---

Apply a MACsec Key Agreement (MKA) profile to a port.

## Syntax

- **macsec mka profile WORD<1-16>**
- **no macsec mka profile WORD<1-16>**

## Command Parameters

**WORD<1-16>**

Specifies the MKA profile name. An MKA profile name can consist only of alphanumeric characters (0-9, A-Z, and a-z). The profile name is case sensitive.

## Command Mode

GigabitEthernet Interface Configuration

The following example applies an MKA profile to a port.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch:1(config)#interface gigabitethernet 1/3
Switch:1(config-if)#macsec mka profile test030519
```

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



## mac-security limit-learning

Limit MAC address learning to limit the number of forwarding database entries to protect the FDB.

### Syntax

- **default mac-security limit-learning enable**
- **default mac-security limit-learning max-addr**
- **default mac-security limit-learning port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **default mac-security port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} limit-learning enable**
- **default mac-security port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} limit-learning port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **default mac-security port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} limit-learning port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} max-addr**
- **mac-security limit-learning enable**
- **mac-security limit-learning max-addr <max-addr>**
- **mac-security port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} limit-learning enable**
- **mac-security port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} limit-learning max-addr <max-addr>**
- **no mac-security limit-learning**
- **no mac-security limit-learning enable**
- **no mac-security port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} limit-learning**
- **no mac-security port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} limit-learning enable**

### Command Parameters

#### enable

Limits the MAC learning for the port.

#### limit-learning max-addr <max-addr>

Specifies the maximum number of MAC addresses to learn. The default is 1024.

#### port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## mef-uni enable (for a port)

---

Enable mef-union port (s).

## Syntax

- **default mef-uni enable**
- **mef-uni enable**
- **no mef-uni enable**

## Default

The default is enabled

## Command Mode

GigabitEthernet Interface Configuration

## name (for a port)

---

Specify the name of the port that needs to be changed and have same settings for all the ports.

## Syntax

- **default name**
- **default name port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **name port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**  
**WORD<0-42>**
- **name WORD<0-42>**
- **no name**
- **no name port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**WORD <0-42>**

Specifies the new port name.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## poe poe-limit

---

Configure port power limit.

## Syntax

- **default poe-limit**
- **poe poe-limit <power\_limit>**
- **poe poe-limit port {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]} <power\_limit>**

## Command Parameters

{*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<*power\_limit*>

Specifies the configurable power limit, in watts on a particular port. To see the available range for the switch, use the CLI Help.

## Default

The default is the maximum power limit supported on the hardware platform.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

The power limit varies for different hardware platforms. For more information, see [VOSS User Guide](#).

## poe poe-priority

---

Configure PoE port priority.

## Syntax

- **default poe poe-priority**
- **default poe poe-priority {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} {critical|high|low}**
- **poe poe-priority <critical|high|low>**
- **poe poe-priority port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} {critical|high|low}**

## Command Parameters

**{critical|high|low}**

Configures the port priority.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is low.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## poe poe-shutdown

---

Disable power on the port.

### Syntax

- **default poe poe-shutdown**
- **default poe poe-shutdown port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **poe poe-shutdown**
- **poe poe-shutdown port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

The default is false.

### Command Mode

GigabitEthernet Interface Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## poe fast-poe-enable

---

Enable Fast PoE on a specific copper port.

### Syntax

- **poe fast-poe-enable [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **default poe fast-poe-enable [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no fast-poe-enable [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

```
port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## poe perpetual-poe-enable

---

Enable Perpetual PoE on a specific copper port.

## Syntax

- **poe perpetual-poe-enable** [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]
- **default poe perpetual-poe-enable** [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]
- **no perpetual-poe-enable** [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]

## Command Parameters

```
port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## policy-vlan-precedence

---

Use this command to indicate whether source MAC or IP subnet VLAN classification takes precedence.

## Syntax

- **default policy-vlan-precedence**
- **default policy-vlan-precedence port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **policy-vlan-precedence port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} source-mac**
- **policy-vlan-precedence port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} subnet**
- **policy-vlan-precedence source-mac**
- **policy-vlan-precedence subnet**

## Command Parameters

**{source-mac|subnet}**

Indicates that the source MAC-based or subnet-based VLAN classification takes precedence.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## private-vlan

---

Sets the Private VLAN port type.

## Syntax

- **default private-vlan**
- **no private-vlan**
- **private-vlan <isolated|promiscuous|trunk>**

## Command Parameters

<isolated|promiscuous|trunk>

Sets Private VLAN port type to isolated, promiscuous, or trunk.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## protocol-vlan

---

Enable protocol-based VLAN on the port.

## Syntax

- **default protocol-vlan**
- **default protocol-vlan enable**
- **default protocol-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no protocol-vlan**
- **no protocol-vlan enable**
- **no protocol-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **protocol-vlan**
- **protocol-vlan enable**
- **protocol-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**enable**

Enables or disables protocol-based VLAN for the port.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/



port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## qos 802.1p-override

Configure a port as untrusted to determine the Layer 2 Quality of Service (QoS) actions the switch performs. An untrusted port (override enabled) overrides 802.1p bit markings.

## Syntax

- **default qos 802.1p-override**
- **default qos 802.1p-override enable**
- **no qos 802.1p-override**
- **no qos 802.1p-override enable**
- **qos 802.1p-override**
- **qos 802.1p-override enable**

## Command Parameters

**enable**

If you configure this variable, it overrides incoming 802.1p bits; if you do not configure this variable, it honors and handles incoming 802.1p bits. The default is disable (Layer 2 trusted).

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## qos if-policer

Configures ingress policer or ingress rate-limit on ports.

## Syntax

- **default qos if-policer**
- **default qos if-policer port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **no qos if-policer**
- **no qos if-policer port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **qos if-policer peak-rate** <64-10000000> **svc-rate** <64-10000000>
- **qos if-policer port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} **peak-rate** <64-10000000> **svc-rate** <64-10000000>

## Command Parameters

**peak-rate** <64-10000000>

Specifies the peak rate limit in Kbps. The range is 64-10000000.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**svc-rate** <64-10000000>

Specifies the service rate limit in Kbps. The range is 64-10000000.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## qos if-rate-limiting

Configures ingress port rate limiting in kbps.

## Syntax

- **default qos if-rate-limiting** [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]

- **no qos if-rate-limiting** [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]}
- **qos if-rate-limiting** [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]} **rate** <1000-40000000>

## Command Parameters

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**rate** <1000-40000000>

Specifies the ingress rate limit in Kbps. The range is 1000–40000000.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## qos if-shaper

---

Configure port-based shaping to rate-limit all outgoing traffic to a specific rate.

## Syntax

- **default qos if-shaper**
- **default qos if-shaper** port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **no qos if-shaper**
- **no qos if-shaper** port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **qos if-shaper** port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} **shape-rate** <shape-rate>
- **qos if-shaper** **shape-rate** <shape-rate>

## Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**shape-rate** <*shape-rate*>

Specifies the shaping rate in Kb/s. Different hardware platforms support different egress rate limits, depending on the port with the highest speed available on the platform. If you try to configure a limit that is too high for the port speed, the switch displays the following message: `Error: port slot/port, The QOS Egress shaper rate can not exceed the port capability.`

The default is 0, which means shaping is disabled on the port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## qos level

---

Configure the default port QoS level to assign a default QoS level for all traffic (providing the packet does not match an ACL that remarks the packet).

## Syntax

- **default qos level**
- **default qos level port {slot/port[/sub-port]}**
- **qos level <0-6>**
- **qos level port {slot/port[/sub-port]} <0-6>**

## Command Parameters

<0-6>

Specifies the default Quality of Service (QoS) level for the port traffic. QoS level 7 is reserved for network control traffic.

**port** {*slot/port[/sub-port]*}

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default value is 1.

## Command Mode

GigabitEthernet Interface Configuration

## rate-limit

Configure broadcast and multicast bandwidth limiting to limit the amount of ingress broadcast and multicast traffic on a port. The switch drops traffic that violates the bandwidth limit.

## Syntax

- **default rate-limit broadcast**
- **default rate-limit multicast**
- **default rate-limit port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} broadcast**
- **default rate-limit port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} multicast**
- **no rate-limit broadcast**
- **no rate-limit multicast**
- **no rate-limit port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} broadcast**
- **no rate-limit port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} multicast**
- **rate-limit broadcast {<1-65535> | <50-65000000>}**
- **rate-limit broadcast <1-65535>**
- **rate-limit multicast {<1-65535> | <50-65000000>}**
- **rate-limit multicast <1-65535>**
- **rate-limit port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} broadcast {<1-65535> | <50-65000000>}**
- **rate-limit port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} multicast {<1-65535> | <50-65000000>}**

## Command Parameters

**<1-65535>**

Specifies the bandwidth limit for broadcast and multicast traffic from 1-65535 packets per second.

**broadcast {<1-65535> | <50-65000000>}**

Rate limit for broadcast. Range depends on hardware platform.

**multicast {<1-65535> | <50-65000000>}**

Rate limit for multicast. Range depends on hardware platform.

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled (no rate limit).

## Command Mode

GigabitEthernet Interface Configuration

---

## rmon (for a port)

Configure Remote Network Monitoring (RMON) on a particular port.

## Syntax

- **default rmon**
- **no rmon**
- **rmon**

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## sflow counter-interval

Configure the counter sampling interval values at port level to determine how often the sFlow agent polls and exports counters for a configured interface.

## Syntax

- **default sflow counter-interval**
- **no sflow counter-interval**
- **sflow counter-interval <1-3600>**

## Command Parameters

<1-3600>

Specifies the polling interval for a slot.

## Default

The default is 0 (disabled).

## Command Mode

GigabitEthernet Interface Configuration

---

## sflow max-header-size

Specifies the maximum number of bytes to be copied from the sampled packet.

## Syntax

- **default sflow max-header-size**
- **sflow max-header-size <64-256>**

## Command Parameters

<64-256>

Identifies the maximum number of bytes to be copied from the sampled packet.

## Default

The default is 128.

## Command Mode

GigabitEthernet Interface Configuration

---

## sflow sampling-rate

Configures the packet sampling rate on a port.

## Syntax

- **default sflow sampling-rate**
- **no sflow sampling-rate**
- **sflow sampling-rate <1024-1000000>**

## Command Parameters

<1024-1000000>

Configures the packet sampling rate on a port.

## Default

The default is 0, which means sFlow is disabled on the port.

## Command Mode

GigabitEthernet Interface Configuration

## shutdown

---

Disable an Ethernet module before you remove it from the chassis to minimize traffic loss. Traffic does not flow on a disabled module.

## Syntax

- **default shutdown**
- **default shutdown port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no shutdown**
- **no shutdown port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **shutdown**
- **shutdown port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**port** <{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}>

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration



## slpp (for a port)

Enable Simple Loop Prevention Protocol (SLPP) by port to detect a loop and automatically stop it.

### Syntax

- **default slpp**
- **default slpp packet-rx**
- **default slpp packet-rx-threshold**
- **default slpp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **default slpp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} packet-rx**
- **default slpp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} packet-rx-threshold**
- **no slpp**
- **no slpp packet-rx**
- **no slpp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no slpp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} packet-rx**
- **slpp packet-rx**
- **slpp packet-rx-threshold <1-500>**
- **slpp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} packet-rx**
- **slpp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} packet-rx-threshold <1-500>**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### **packet-rx**

Enables or disables SLPP packet reception on the port. The default is disabled.

**packet-rx-threshold <1-500>**

Specifies the SLPP reception threshold on the ports, expressed as an integer. The packet reception threshold specifies the number of SLPP packets the port receives before it is administratively disabled.



#### Caution

Configure the rx-threshold above 50 ms only on lightly loaded switches. If you configure the rx-threshold to a value greater than 50 ms on a heavily loaded switch and a loop occurs, the system can experience high CPU utilization. The default is 1.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## slpp-guard (for a port)

Configures SLPP Guard for switch ports.

## Syntax

- `default slpp-guard`
- `default slpp-guard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable`
- `default slpp-guard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} timeout`
- `default slpp-guard timeout`
- `no slpp-guard`
- `no slpp-guard enable`
- `no slpp-guard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable`
- `no slpp-guard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} timeout`
- `no slpp-guard timeout`
- `slpp-guard enable`
- `slpp-guard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable`
- `slpp-guard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} timeout`
- `slpp-guard timeout <0 | 10-65535>`

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### enable

Enables SLPP Guard on a port. The default is disabled.

### timeout <0 | 10-65535>

Specifies the time period, in seconds, for which SLPP Guard disables the port. After the timeout period expires, the switch reenables the port. The timeout value can be 0 or a value ranging from 10 to 65535. With a value of 0, the port remains disabled until it is manually re-enabled. The default timeout value is 60 seconds.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## snmp trap link-status

---

Enable link trap on the port.

## Syntax

- **default snmp trap link-status**
- **default snmp trap link-status port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no snmp trap link-status**
- **no snmp trap link-status port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **snmp trap link-status**
- **snmp trap link-status enable**
- **snmp trap link-status port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **snmp trap link-status port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

## Command Parameters

enable

Enables or disables link-trap status for the port.

```
port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

## source-mac-vlan

---

Enable source MAC-based VLAN on the port.

## Syntax

- **default source-mac-vlan**
- **default source-mac-vlan enable**
- **default source-mac-vlan port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}
- **no source-mac-vlan**
- **no source-mac-vlan enable**
- **no source-mac-vlan port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}
- **source-mac-vlan**
- **source-mac-vlan enable**
- **source-mac-vlan port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

## Command Parameters

**enable**

Enables or disables source MAC-based VLAN for the port.

```
port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

## spanning-tree bpduguard

---

Configures spanning-tree BPDU Guard configuration.

## Syntax

- **spanning-tree bpduguard enable**
- **spanning-tree bpduguard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **spanning-tree bpduguard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} timeout <0-65535>**
- **spanning-tree bpduguard timeout <0-65535>**

## Command Parameters

### enable

Enables BPDU Guard on the port. The default is disabled.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### timeout <0-65535>

Specifies the value to use for port-state recovery. After a BPDU Guard disables a port, the port remains in the disabled state until this timer expires. You can configure a value from 10 to 65535. The default is 120 seconds.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## spanning-tree mstp cost

---

Configure the contribution of this port to the path cost value for the link.

## Syntax

- `default spanning-tree mstp cost`
- `spanning-tree mstp cost <1-200000000>`

## Command Parameters

<1-200000000>

Specifies the cost value. The default is 2000000.

## Default

The default is 2000000.

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree mstp edge-port

Configure the port as an edge port.

## Syntax

- `default spanning-tree mstp edge-port`
- `spanning-tree mstp edge-port { false | true }`

## Command Parameters

<false|true>

Enables or disables the port as an edge port.

## Default

The default is disabled (false).

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree mstp force-port-state

Enable the force-port-state flag.

## Syntax

- **default spanning-tree mstp force-port-state**
- **no spanning-tree mstp force-port-state**
- **no spanning-tree mstp force-port-state enable**
- **spanning-tree mstp force-port-state enable**

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree mstp hello-time (on a port)

Configure the hello-time delay for the port.

## Syntax

- **default spanning-tree mstp hello-time**
- **spanning-tree mstp hello-time <100-1000>**

## Command Parameters

<100-1000>

Configures the hello-time for a port in one hundredths of a second. The default is 2.

## Default

The default is 2.

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree mstp msti (on a port)

Configure Multiple Spanning Tree Protocol (MSTP) to set the MSTP configuration version.

## Syntax

- **default spanning-tree mstp msti <1-63> cost**
- **default spanning-tree mstp msti <1-63> force-port-state enable**

- `default spanning-tree mstp msti <1-63> port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} cost`
- `default spanning-tree mstp msti <1-63> port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} force-port-state enable`
- `default spanning-tree mstp msti <1-63> port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} priority`
- `default spanning-tree mstp msti <1-63> priority`
- `no spanning-tree mstp msti <1-63> force-port-state enable`
- `no spanning-tree mstp msti <1-63> port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} force-port-state enable`
- `spanning-tree mstp msti <1-63> cost <1-200000000>`
- `spanning-tree mstp msti <1-63> force-port-state enable`
- `spanning-tree mstp msti <1-63> port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} cost <1-200000000>`
- `spanning-tree mstp msti <1-63> port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} force-port-state enable`
- `spanning-tree mstp msti <1-63> port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} priority <0-240>`
- `spanning-tree mstp msti <1-63> priority <0-240>`

## Command Parameters

**<1-63>**

Specifies the instance parameter.

**cost <1-200000000>**

Configures the path cost for the port

**force-port-state enable**

Enables MSTI learning for the port.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**priority <0-65535>**

Configures the MSTP bridge priority. Allowed values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.

## Default

None



## Command Mode

GigabitEthernet Interface Configuration

### spanning-tree mstp p2p

---

Specify the point-to-point status of the LAN segment attached to this port.

#### Syntax

- **default spanning-tree mstp p2p**
- **spanning-tree mstp p2p auto**
- **spanning-tree mstp p2p force-false**
- **spanning-tree mstp p2p force-true**

#### Command Parameters

<auto|force-false|force-true>

A value of force-true indicates that this port is treated as if it connects to a point-to-point link.

A value of force-false indicates that this port is treated as having a shared media connection.

A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotiation or by management means.

The default is auto.

#### Default

The default is auto.

## Command Mode

GigabitEthernet Interface Configuration

### spanning-tree mstp port

---

Configure all Multiple Spanning Tree Protocol (MSTP) parameters for a port.

#### Syntax

- **default spanning-tree mstp**
- **default spanning-tree mstp port {slot/port[/sub-port]}**
- **default spanning-tree mstp port {slot/port[/sub-port]} cost**
- **default spanning-tree mstp port {slot/port[/sub-port]} edge-port**
- **default spanning-tree mstp port {slot/port[/sub-port]} force-port-state**

- `default spanning-tree mstp port {slot/port[/sub-port]} hello-time`
- `default spanning-tree mstp port {slot/port[/sub-port]} p2p`
- `default spanning-tree mstp port {slot/port[/sub-port]} priority`
- `default spanning-tree mstp port {slot/port[/sub-port]} protocol-migration`
- `no spanning-tree mstp`
- `no spanning-tree mstp port {slot/port[/sub-port]}`
- `spanning-tree mstp port {slot/port[/sub-port]} cost <1-200000000>`
- `spanning-tree mstp port {slot/port[/sub-port]} edge-port { false | true }`
- `spanning-tree mstp port {slot/port[/sub-port]} force-port-state enable`
- `spanning-tree mstp port {slot/port[/sub-port]} hello-time <100-1000>`
- `spanning-tree mstp port {slot/port[/sub-port]} p2p auto`
- `spanning-tree mstp port {slot/port[/sub-port]} p2p force-false`
- `spanning-tree mstp port {slot/port[/sub-port]} p2p force-true`
- `spanning-tree mstp port {slot/port[/sub-port]} priority <0-240>`
- `spanning-tree mstp port {slot/port[/sub-port]} protocol-migration false`
- `spanning-tree mstp port {slot/port[/sub-port]} protocol-migration true`

## Command Parameters

### <0-240>

Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16.

### <100-1000>

Configures the hello-time for a port in one hundredths of a second.

### <1-200000000>

Specifies the cost value.

### <auto|force-false|false-true>

A value of force-true indicates that this port is treated as if it connects to a point-to-point link.

A value of force-false indicates that this port is treated as having a shared media connection.

A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotiation or by management means.

### edge-port <false|true>

Enables or disables the port as an edge port. The default is disabled (false).

### port {slot/port[/sub-port]}

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**protocol-migration <false|true>**

Configures the protocol migration state of this port. The default is false.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree mstp priority (on a port)

Specify the four most significant bits of the port identifier for a given spanning tree instance that can be modified independently for each spanning tree instance supported by the bridge.

## Syntax

- **default spanning-tree mstp priority**
- **spanning-tree mstp priority <0-240>**

## Command Parameters

**<0-240>**

Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16.

## Default

The default is 128.

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree mstp protocol-migration

Initiates or terminates protocol migration for the port. If enabled, the port transmits BPDUs without instance information.

## Syntax

- **default spanning-tree mstp protocol-migration**
- **spanning-tree mstp protocol-migration false**
- **spanning-tree mstp protocol-migration true**

## Command Parameters

<false|true>

Configures the protocol migration state of this port.

## Default

The default is false.

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree rstp cost

Configure the contribution of this port to the path cost value for the link.

## Syntax

- **default spanning-tree rstp cost**
- **spanning-tree rstp cost <1-200000000>**

## Command Parameters

<1-200000000>

Specifies the cost value.

## Default

The default is 2000000.

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree rstp edge-port

Configure the port as an edge port.

## Syntax

- **default spanning-tree rstp edge-port**
- **spanning-tree rstp edge-port { false | true }**

## Command Parameters

<false|true>

Enables or disables the port as an edge port.

## Default

The default is disabled (false).

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree rstp p2p

Specify the point-to-point status of the LAN segment attached to this port.

## Syntax

- **default spanning-tree rstp p2p**
- **spanning-tree rstp p2p auto**
- **spanning-tree rstp p2p force-false**
- **spanning-tree rstp p2p force-true**

## Command Parameters

<auto|force-false|force-true>

A value of force-true indicates that this port is treated as if it connects to a point-to-point link.

A value of force-false indicates that this port is treated as having a shared media connection.

A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotiation or by management means.

## Default

The default is auto.

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree rstp port

Configure all Rapid Spanning Tree Protocol (RSTP) parameters for a port.

## Syntax

- `default spanning-tree rstp`
- `default spanning-tree rstp`
- `default spanning-tree rstp port {slot/port[/sub-port]}`
- `no spanning-tree rstp`
- `no spanning-tree rstp port {slot/port[/sub-port]}`
- `spanning-tree rstp port {slot/port[/sub-port]} cost <1-200000000>`
- `spanning-tree rstp port {slot/port[/sub-port]} edge-port { false | true }`
- `spanning-tree rstp port {slot/port[/sub-port]} p2p auto`
- `spanning-tree rstp port {slot/port[/sub-port]} p2p force-false`
- `spanning-tree rstp port {slot/port[/sub-port]} p2p force-true`
- `spanning-tree rstp port {slot/port[/sub-port]} priority <0-240>`
- `spanning-tree rstp port {slot/port[/sub-port]} protocol-migration false`
- `spanning-tree rstp port {slot/port[/sub-port]} protocol-migration true`
- `spanning-tree rstp port {slot/port[/sub-port]} stp enable`

## Command Parameters

`cost <1-200000000>`

Specifies the cost value. The default is 2000000.

`edge-port <false|true>`

Enables or disables the port as an edge port. The default is disabled (false).

`p2p <auto|force-false|false-true>`

A value of force-true indicates that this port is treated as if it connects to a point-to-point link.

A value of force-false indicates that this port is treated as having a shared media connection.

A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotiation or by management means.

The default is auto.

`port {slot/port[/sub-port]}`

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

`priority <0-240>`

Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16. The default is 128.

`protocol-migration <false|true>`

Configures the protocol migration state of this port. The default is false.

**stp enable**

Enables STP for the port. The default is disabled.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## spanning-tree rstp priority (on a port)

---

Specify the four most significant bits of the port identifier for a given spanning tree instance that can be modified independently for each spanning tree instance supported by the bridge.

## Syntax

- **default spanning-tree rstp priority**
- **spanning-tree rstp priority <0-240>**

## Command Parameters

<0-240>

Specifies the four most significant bits of the port identifier. Assigns RSTP bridge priority in a range of 0-240. The values configured for port priority must be in steps of 16.

## Default

The default is 128.

## Command Mode

GigabitEthernet Interface Configuration

## spanning-tree rstp protocol-migration

---

Initiate or terminate protocol migration for the port. If enabled, the port transmits BPDUs without instance information.

## Syntax

- **default spanning-tree rstp protocol-migration**
- **spanning-tree rstp protocol-migration false**
- **spanning-tree rstp protocol-migration true**

## Command Parameters

<false|true>

Configures the protocol migration state of this port.

## Default

The default is false.

## Command Mode

GigabitEthernet Interface Configuration

---

## spanning-tree rstp stp

Enable STP on the port.

## Syntax

- **default spanning-tree rstp stp**
- **no spanning-tree rstp stp enable**
- **spanning-tree rstp stp enable**

## Default

The default value is enabled.

## Command Mode

GigabitEthernet Interface Configuration

---

## speed

Configure the speed of the port on the Ethernet modules.



### Note

Not all parameters appear on all hardware platforms.

## Syntax

- **default speed**
- **default speed port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **speed 10**
- **speed 100**
- **speed 1000**
- **speed 10000**



- **speed 2500**
- **speed 25000**
- **speed 5000**
- **speed port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 10**
- **speed port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 100**
- **speed port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 1000**
- **speed port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 10000**
- **speed port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 2500**
- **speed port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 25000**
- **speed port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 5000**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**<10|100|1000|10000|2500|25000|5000>**

Specifies the port speed.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

If Auto-Negotiation is disabled and you manually configure the speed on a port that results in a configuration mismatch in speed between two ports, VSP 4450 Series and VSP 4900 Series switches may show an incorrect operational status of "up" for the mismatched ports.

## subnet-vlan

Enable subnet-based VLAN on the port.



### Note

This command does not appear on all hardware platforms.

## Syntax

- **default subnet-vlan**
- **default subnet-vlan enable**
- **default subnet-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no subnet-vlan**
- **no subnet-vlan enable**
- **no subnet-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **subnet-vlan**
- **subnet-vlan enable**
- **subnet-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

### enable

Enables or disables subnet-based VLAN for the port.

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is enabled.

## Command Mode

GigabitEthernet Interface Configuration

## spoof-detect

---

Configure the spoof detection to prevent an IP spoofing.

## Syntax

- **default spoof-detect**
- **default spoof-detect enable**
- **default spoof-detect port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no spoof-detect**
- **no spoof-detect enable**

- **no spoof-detect port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no spoof-detect port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **spoof-detect**
- **spoof-detect enable**
- **spoof-detect port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

### enable

Enables spoof detection on the port.

**port** {*slot/port[/sub-port] [-slot/port[/sub-port]] [,...]*}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## tagged-frames-discard

Discards tagged frames on the port.

## Syntax

- **default tagged-frames-discard**
- **default tagged-frames-discard enable**
- **default tagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **default tagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **no tagged-frames-discard**
- **no tagged-frames-discard enable**
- **no tagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no tagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

- **tagged-frames-discard**
- **tagged-frames-discard enable**
- **tagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **tagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

## Command Parameters

### enable

Discards tagged frames on the port.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## tx-flow-control

Enable TX flow control for TX to transmit the MAC control PAUSE frames to indicate congestion on the receive side of the port interface. Flow control can only be enabled on 1 Gbit/s and 10 Gbit/s ports. Flow control cannot be enabled for ports that run at less than 1 Gbit/s.

## Syntax

- **default tx-flow-control**
- **default tx-flow-control enable**
- **default tx-flow-control port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **default tx-flow-control port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **no tx-flow-control**
- **no tx-flow-control enable**
- **no tx-flow-control port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

- **no tx-flow-control port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**
- **tx-flow-control**
- **tx-flow-control enable**
- **tx-flow-control port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **tx-flow-control port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable**

## Command Parameters

### enable

Enables the TX flow control on the module.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

**tx-flow-control** is enabled by default on XA1400 Series.

## Command Mode

GigabitEthernet Interface Configuration

## untagged-frames-discard

---

Configure a tagged port to discard all untagged packets so that the frame is not classified into the default VLAN for the port.

## Syntax

- **default untagged-frames-discard**
- **default untagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no untagged-frames-discard**
- **no untagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

- **untagged-frames-discard**
- **untagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## untag-port-default-vlan

---

Untag the default VLAN on the port.

## Syntax

- **default untag-port-default-vlan**
- **default untag-port-default-vlan enable**
- **default untag-port-default-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no untagged-frames-discard**
- **no untagged-frames-discard port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no untag-port-default-vlan**
- **no untag-port-default-vlan enable**
- **no untag-port-default-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **untag-port-default-vlan**
- **untag-port-default-vlan enable**
- **untag-port-default-vlan port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

### **enable**

Untags the default VLAN for the port.

**port** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## vlacp

Configure Virtual Link Aggregation Control Protocol (VLACP) on a port to ensure that there is end-to-end reachability.

## Syntax

- **default vlapc**
- **default vlapc enable**
- **default vlapc etherstype**
- **default vlapc fast-periodic-time**
- **default vlapc flap-frequency**
- **default vlapc flap-interval**
- **default vlapc funcmac-addr**
- **default vlapc slow-periodic-time**
- **default vlapc timeout**
- **default vlapc timeout-scale**
- **no vlapc**
- **no vlapc enable**
- **vlacp enable**
- **vlacp etherstype <1536-65535 | 0x600-0xffff>**
- **vlacp flap-frequency <3-30>**
- **vlacp flap-interval <10-600>**
- **vlacp fast-periodic-time <100-20000>**
- **vlacp funcmac-addr 0x00:0x00:0x00:0x00:0x00:0x00**

- **vlacp slow-periodic-time <10000-30000>**
- **vlacp timeout long**
- **vlacp timeout short**
- **vlacp timeout-scale <2-10>**

## Command Parameters

### **enable**

Enables VLACP for this port.

### **ethertype <0X600-0Xfff>**

Configures the VLACP protocol identification for this port.

### **fast-periodic-time <100-20000>**

Configures the fast periodic time (in milliseconds) for this port.

### **flap-frequency <3-30>**

Configures the frequency of VLACP flaps allowed in a specific time interval for the VLACP Flap Detect and Damping feature. The default value is 3.

### **flap-interval <10-600>**

Configures the time interval (in seconds) to record the VLACP flaps on ports. The default value is 60 seconds.

### **funcmac-addr <0x00:0x00:0x00:0x00:0x00:0x00>**

Configures the multicast MAC address used for the VLACPDU. Specify a MAC address in the format 0x00:0x00:0x00:0x00:0x00:0x00. The default is 01:80:c2:00:11:00.

### **slow-periodic-time <10000-30000>**

Configures the slow periodic time (in milliseconds) for a specific port type.

### **timeout {long|short}**

Configures the port to use the long or short timeout:

- Long configures the port to use the timeout-scale value multiplied by the slow-periodic-time.
- Short configures the port to use the timeout-scale value multiplied by the fast-periodic-time.

For example, if you specify a short timeout, configure the timeout-scale value to 3, and the fast-periodic-time to 400 ms, the timer will expire within 1000 to 1200 ms. To configure this option to the default value, use the default operator with the command.

### **timeout-scale <2-10>**

Configures a timeout scale for this port used to calculate the timeout. The default value is 3. To configure this option to the default value, use the default operator with the command.

## Default

None



## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

Use the following information to prevent flooding VLACP packets across a defaulted switch:

- Use the default MAC address, 01:80:c2:00:11:00, for end-to-end connections that traverse an intermediate network.
- Use the reserved multicast MAC address 01-80-c2-00-00-0f for directly-connected, peer-to-peer links.

## vlacp flap-detect enable

---

Enables the VLACP Flap Detect and Damping feature on the port.

## Syntax

- **default vlapc flap-detect enable**
- **no vlapc flap-detect enable**
- **vlacp flap-detect enable**

## Default

The default configuration is disabled.

## Command Mode

GigabitEthernet Interface Configuration

## Usage Guidelines

- Do not enable VLACP Flap Detect and Damping on Link Aggregation Control Protocol (LACP) enabled ports.
- Do not enable VLACP Flap Detect and Damping interswitch Trunking (IST).

## vrf (for a port)

---

Associate a port to a Virtual Router Forwarding (VRF) so that the port becomes a member of the VRF instance.

## Syntax

- **no vrf**
- **vrf WORD<1-16>**

## Command Parameters

vrf WORD<1-16>

Specifies the VRF name.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration



# Global Configuration

---

The following topics document commands available in Global Configuration mode of the command line interface (CLI).

## access-policy

---

Configure an access policy to control access to the switch. You can define network stations that are explicitly allowed to access the switch or network stations that are explicitly forbidden to access the switch.

For each service, you can also specify the level of access; for example, read-only or read/write/all. Use the command without parameters to globally enable access policies.

### Syntax

- **access-policy**
- **access-policy <1-65535>**
- **default access-policy**
- **default access-policy <1-65535>**
- **no access-policy**
- **no access-policy <1-65535>**

### Command Parameters

**<1-65535>**

Specifies the policy ID.

### Default

None

### Command Mode

Global Configuration

## access-policy <1-65535> accesslevel

---

Restrain access to criteria specified in the access policy. If true, the system accepts only the currently configured access level. If false, the system accepts access up to the configured access level.

## Syntax

- **access-policy <1-65535> accesslevel { ro | rwa | rw }**
- **default access-policy <1-65535> accesslevel**

## Command Parameters

{ ro | rwa | rw }

Specifies the access level.

<1-65535>

Specifies the policy ID.

## Default

The default value is ro.

## Command Mode

Global Configuration

## access-policy <1-65535> access-strict

---

Specify the level of access if you configure the policy to allow access. The access-strict command ties to the accesslevel command. If you enable access-strict, the access policy looks at the accesslevel value, and only applies to that access level. If you disable access-strict (false), the policy looks at the value for accesslevel, and then the system applies the policy to anyone with equivalent rights or higher.

## Syntax

- **access-policy <1-65535> access-strict**
- **default access-policy <1-65535> access-strict**
- **no access-policy <1-65535> access-strict**

## Command Parameters

<1-65535>

Specifies the policy ID.

## Default

The default value is disabled (false).

## Command Mode

Global Configuration

---

## access-policy <1-65535> enable

---

Activate the access policy.

### Syntax

- **access-policy <1-65535> enable**
- **default access-policy <1-65535> enable**
- **no access-policy <1-65535> enable**

### Command Parameters

<1-65535>

Specifies the policy ID.

### Default

The default is disabled (off).

### Command Mode

Global Configuration

---

## access-policy <1-65535> ftp

---

Activate or disable FTP for the specified policy. Because FTP derives its login and password from the CLI management filters, FTP works for read-write-all (rwa) and readwrite (rw) access but not for the read-only (ro) access.

### Syntax

- **access-policy <1-65535> ftp**
- **default access-policy <1-65535> ftp**
- **no access-policy <1-65535> ftp**

### Command Parameters

<1-65535>

Specifies the policy ID.

### Default

The default is disabled.

## Command Mode

Global Configuration

### access-policy <1-65535> host

---

Specify the trusted host address as an IP address for remote login access.

#### Syntax

- **access-policy <1-65535> host WORD<0-46>**
- **default access-policy <1-65535> host**
- **no access-policy <1-65535> host**

#### Command Parameters

<1-65535>

Specifies the policy ID.

WORD<0-46>

Specifies the IPv4 or IPv6 address.

#### Default

None

## Command Mode

Global Configuration

### access-policy <1-65535> http

---

Activate the HTTP for this access policy.

#### Syntax

- **access-policy <1-65535> http**
- **default access-policy <1-65535> http**
- **no access-policy <1-65535> http**

#### Command Parameters

<1-65535>

Specifies the policy ID.

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## access-policy <1-65535> mode

Specify whether the designated network address is allowed access to the system through the specified access service.

## Syntax

- **access-policy <1-65535> mode { allow | deny }**
- **default access-policy <1-65535> mode**

## Command Parameters

{ allow | deny }

Allows or denies access to the designated network address.

<1-65535>

Specifies the policy ID.

## Default

The default is allow.

## Command Mode

Global Configuration

---

## access-policy <1-65535> name

Specify a name expressed as a string.

## Syntax

- **access-policy <1-65535> name WORD<0-15>**
- **default access-policy <1-65535> name**

## Command Parameters

<1-65535>

Specifies the policy ID.

## Default

None

## Command Mode

Global Configuration

## access-policy <1-65535> network

---

Specify the IP address and subnet mask that can access the system through the specified access service.

## Syntax

- **access-policy <1-65535> network WORD<1-46> <0-128>**
- **default access-policy <1-65535> network**
- **no access-policy <1-65535> network**

## Command Parameters

<1-65535>

Specifies the policy ID.

WORD<1-46> <0-128>

Specifies the IP address and subnet mask

## Default

None

## Command Mode

Global Configuration

## access-policy <1-65535> precedence

---

Specify a precedence value for a policy, expressed as a number from 1-128. The precedence value determines which policy the system uses if multiple policies apply. Lower numbers take higher precedence.

## Syntax

- **access-policy <1-65535> precedence <1-128>**
- **default access-policy <1-65535> precedence**



## Command Parameters

<1-128>

Specifies a precedence value for a policy.

<1-65535>

Specifies the policy ID.

## Default

The default is 10.

## Command Mode

Global Configuration

---

## access-policy <1-65535> rlogin

Activate remote logon for the access policy.

## Syntax

- **access-policy <1-65535> rlogin**
- **default access-policy <1-65535> rlogin**
- **no access-policy <1-65535> rlogin**

## Command Parameters

<1-65535>

Specifies the policy ID.

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

---

## access-policy <1-65535> snmp-group

Add a Simple Network Management Protocol version 3 (SNMP-v3) group under the access policy.

## Syntax

- **access-policy <1-65535> snmp-group WORD<1-32> { snmpv1 | snmpv2c | usm }**
- **no access-policy <1-65535> snmp-group WORD<1-32> { snmpv1 | snmpv2c | usm }**

## Command Parameters

{ snmpv1 | snmpv2c | usm }

Configures the security model.

<1-65535>

Specifies the policy ID.

WORD<1-32>

Specifies the name of the group.

## Default

None

## Command Mode

Global Configuration

## access-policy <1-65535> snmpv3

---

Activate Simple Network Management Protocol (SNMP) version 3 for the access policy.

## Syntax

- **access-policy <1-65535> snmpv3**
- **default access-policy <1-65535> snmpv3**
- **no access-policy <1-65535> snmpv3**

## Command Parameters

<1-65535>

Specifies the policy ID.

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## access-policy <1-65535> ssh

---

Activate Secure Shell (SSH) for the access policy.

### Syntax

- **access-policy <1-65535> ssh**
- **default access-policy <1-65535> ssh**
- **no access-policy <1-65535> ssh**

### Command Parameters

<1-65535>

Specifies the policy ID.

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## access-policy <1-65535> telnet

---

Activate Telnet for the access policy.

### Syntax

- **access-policy <1-65535> telnet**
- **default access-policy <1-65535> telnet**
- **no access-policy <1-65535> telnet**

### Command Parameters

<1-65535>

Specifies the policy ID.

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## access-policy <1-65535> tftp

---

Activate the Trivial File Transfer Protocol (TFTP) for this access policy.

### Syntax

- **access-policy <1-65535> tftp**
- **default access-policy <1-65535> tftp**
- **no access-policy <1-65535> tftp**

### Command Parameters

**<1-65535>**

Specifies the policy ID.

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## access-policy <1-65535> username

---

Specify the trusted host user name for remote login access.

### Syntax

- **access-policy <1-65535> username WORD<0-30>**
- **default access-policy <1-65535> username**

### Command Parameters

**<1-65535>**

Specifies the policy ID.

**WORD<0-30>**

Specifies the username.

### Default

None

### Command Mode

Global Configuration

---

## access-policy by-mac

---

Configure access-policies by MAC address to allow or deny local MAC addresses on the network management port after an access policy is activated. If the source MAC does not match a configured entry, then the default action is taken.

### Syntax

- **access-policy by-mac 0x00:0x00:0x00:0x00:0x00:0x00 { allow | deny }**
- **access-policy by-mac action { allow | deny }**
- **default access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00>**
- **default access-policy by-mac action**
- **no access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00>**

### Command Parameters

**<0x00:0x00:0x00:0x00:0x00:0x00> <allow|deny>**

Adds a MAC address to the policy. Enter the MAC address in hexadecimal format. Specify the action to take for the MAC address.

**action <allow|deny>**

Specifies the action for a MAC address that does not match the policy.

### Default

The default action is allow.

### Command Mode

Global Configuration

---

## application

---

Enter Application mode.

### Syntax

- **application**

### Default

None

### Command Mode

Global Configuration

---

## app-telemetry enable

---

Enables Application Telemetry.

### Syntax

- **no app-telemetry enable**

### Default

The default value is disable.

### Command Mode

Global Configuration

---

## auto-recover-delay

---

Set the time delay for the automatic recovery of ports.

### Syntax

- **auto-recover-delay <5-3600>**
- **default auto-recover-delay**
- **no auto-recover-delay <5-3600>**

### Command Parameters

**<5-3600>**

Specifies the range to be set for the auto-recovery of ports in seconds. The range varies between 5 to 3600 seconds.

### Default

The default is 30.

### Command Mode

Global Configuration

---

## autotopology

---

Configure the SynOptics Network Management Protocol (SONMP) to allow a network management station (NMS) formulate a map that shows the interconnections between Layer 2 devices in a network.

## Syntax

- **autotopology**
- **default autotopology**
- **no autotopology**

## Default

The default status is enabled.

## Command Mode

Global Configuration

## auto-sense access-diffserv

---

Configures the ports operating in Auto-sense mode to determine the Layer 3 QoS actions the switch performs. The Auto-sense access ports override the Differentiated Services Code Point (DSCP) markings.

## Syntax

- **auto-sense access-diffserv [enable]**
- **default auto-sense access-diffserv [enable]**
- **no auto-sense access-diffserv [enable]**

## Command Parameters

**enable**

Specifies access ports that are operating in Auto-sense mode.

## Default

The default is enabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense data (globally)

---

Configures Auto-sense data traffic information.

## Syntax

- **auto-sense data i-sid <1-16777215>**
- **no auto-sense data i-sid**

## Command Parameters

i-sid <1-16777215>

Specifies the service interface identifier (I-SID).

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## auto-sense dhcp-detection

Configures the dhcp server detection in Auto-sense mode.

## Syntax

- **auto-sense dhcp-detection**
- **no auto-sense dhcp-detection**
- **default auto-sense dhcp-detection**

## Default

The default is enabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



---

## auto-sense eapol voice lldp-auth

---

Configures Link Layer Discovery Protocol (LLDP) authentication for IP phones on ports that are operating in Auto-sense mode.

### Syntax

- **auto-sense eapol voice lldp-auth**
- **default auto-sense eapol voice lldp-auth**
- **no auto-sense eapol voice lldp-auth**

### Default

The default is disabled.

### Command Mode

Global Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## auto-sense fa authentication-key

---

Configures Fabric Attach authentication key for ports that operate in Auto-sense mode.

### Syntax

- **auto-sense fa authentication-key WORD<0-32>**
- **default auto-sense fa authentication-key**

### Command Parameters

**WORD<0-32>**

Specifies the authentication key value.

### Default

None.

### Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense fa camera eapol status {authorized | auto}

---

Configures EAPoL authentication requirements for auto-sensed cameras.

### Syntax

- **auto-sense fa camera eapol status {authorized | auto}**
- **default auto-sense fa camera eapol status**
- **no auto-sense fa camera eapol status**

### Command Parameters

#### authorized

Specifies to skip EAPoL authentication and authorize the connection.

#### auto

Specifies that authorization depends on the result of EAPoL authentication.

### Default

The default is auto.

### Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense fa camera i-sid <1-16777215>

---

Configures an I-SID for auto-sensed cameras.

### Syntax

- **auto-sense fa camera i-sid <1-16777215>**
- **no auto-sense fa camera i-sid**

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense fa message-authentication

---

Configures Fabric Attach message authentication for ports that are operating in Auto-sense mode.

## Syntax

- **auto-sense fa message-authentication**
- **default auto-sense fa message-authentication**
- **no auto-sense fa message-authentication**

## Default

Message authentication is enabled by default.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense fa proxy management i-sid <1-16777215> c-vid <1-4094>

---

Configures a specific I-SID and customer VLAN ID to use as the management I-SID when a port is in the Auto-sense FA PROXY state.

## Syntax

- **auto-sense fa proxy management i-sid <1-16777215> c-vid <1-4094>**
- **no auto-sense fa proxy management i-sid**

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## auto-sense fa proxy-no-auth i-sid <1-16777215>

Configures an I-SID for auto-sensed client switches that do not use Fabric Attach (FA) message authentication, like EXOS.

## Syntax

- **auto-sense fa proxy-no-auth i-sid <1-16777215>**
- **no auto-sense fa proxy-no-auth i-sid**

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## auto-sense fa ovs eapol status {authorized | auto}

Configures EAPoL authentication requirements for auto-sensed virtual switches.

## Syntax

- **auto-sense fa ovs eapol status {authorized | auto}**
- **default auto-sense fa ovs eapol status**
- **no auto-sense fa ovs eapol status**

## Command Parameters

### authorized

Specifies to skip EAPoL authentication and authorize the connection.

### auto

Specifies that authorization depends on the result of EAPoL authentication.

## Default

The default is auto.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## auto-sense fa ovs i-sid <1-16777215>

Configures an I-SID for auto-sensed virtual switches.

## Syntax

- **auto-sense fa ovs i-sid <1-16777215>**
- **no auto-sense fa ovs i-sid**

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## auto-sense fa wap-type1 eapol status {authorized | auto}

Configures EAPoL authentication requirements for auto-sensed wireless access points (WAP).

## Syntax

- **auto-sense fa wap-type1 eapol status {authorized | auto}**
- **default auto-sense fa wap-type1 eapol status**
- **no auto-sense fa wap-type1 eapol status**

## Command Parameters

### authorized

Specifies to skip EAPoL authentication and authorize the connection.

### auto

Specifies that authorization depends on the result of EAPoL authentication.

## Default

The default is auto.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## auto-sense fa wap-type1 i-sid <1-16777215>

Configures an I-SID for auto-sensed wireless access points (WAP).

## Syntax

- **auto-sense fa wap-type1 i-sid <1-16777215>**
- **no auto-sense fa wap-type1 i-sid**

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense isis hello-auth type hmac-md5

---

Configures HMAC-MD5 authentication type for IS-IS hello packets on ports that are operating in Auto-sense mode. MD5 authentication creates an encoded checksum in the transmitted packet. The receiving router uses an authentication key (password) to verify the MD5 checksum of the packet.

## Syntax

- **auto-sense isis hello-auth type hmac-md5**
- **auto-sense isis hello-auth type hmac-md5 [key WORD<1-16>]**
- **auto-sense isis hello-auth type hmac-md5 key WORD<1-16> [key-id <1-255>]**
- **no auto-sense isis hello-auth**

## Command Parameters

**key WORD<1-16>**

Specifies the authentication key (password) that the receiving router uses to verify the packet.

**key-id <1-255>**

Specifies the key ID.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense isis hello-auth type hmac-sha-256

---

Configures HMAC-SHA256 authentication type for IS-IS hello packets on ports that are operating in Auto-sense mode. With SHA-256 authentication, the switch adds an HMAC-SHA256 digest to each Hello packet. The switch that receives the Hello packet computes the digest of the packet and compares it with the received digest. If the digests match, the receiving switch accepts the packet. If the digests do not match, the receiving switch discards the packet.

## Syntax

- **auto-sense isis hello-auth type hmac-sha-256**
- **auto-sense isis hello-auth type hmac-sha-256 [key WORD<1-16>]**
- **auto-sense isis hello-auth type hmac-sha-256 key WORD<1-16> [key-id <1-255>]**
- **no auto-sense isis hello-auth**

## Command Parameters

**key WORD<1-16>**

Specifies the authentication key (password) that the receiving router uses to verify the packets.

**key-id <1-255>**

Specifies the key ID.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense isis hello-auth type simple

---

Configures simple password authentication for IS-IS hello packets on ports that are operating in Auto-sense mode. Simple password authentication uses a text password in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet.

## Syntax

- **auto-sense isis hello-auth type simple**
- **auto-sense isis hello-auth type simple [key WORD<1-16>]**
- **auto-sense isis hello-auth type simple key WORD<1-16> [key-id <1-255>]**
- **no auto-sense isis hello-auth**

## Command Parameters

**key WORD<1-16>**

Specifies the authentication key (password) that the receiving router uses to verify the packet.



**key-id <1-255>**

Specifies the key ID.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense isis hello-auth type none

---

Configures the authentication type as none, for IS-IS hello packets on ports that are operating in Auto-sense mode.

## Syntax

- **auto-sense isis hello-auth type none**
- **auto-sense isis hello-auth type none [key WORD<1-16>]**
- **auto-sense isis hello-auth type none key WORD<1-16> [key-id <1-255>]**
- **no auto-sense isis hello-auth**

## Command Parameters

**key WORD<1-16>**

Specifies the authentication key (password) that the receiving router uses to verify the packet.

**key-id <1-255>**

Specifies the key ID.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense onboarding

---

Configures the Auto-sense onboarding traffic information.

### Syntax

- **auto-sense onboarding i-sid <1-16777215>**
- **no auto-sense onboarding i-sid**

### Command Parameters

**i-sid <1-16777215>**

Specifies the service instance identifier (I-SID).

### Default

The default onboarding I-SID value is 15999999.

### Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense qos 802.1p-override

---

Overrides incoming 802.1p bits on ports that are operating in Auto-sense mode.

### Syntax

- **auto-sense qos 802.1p-override**
- **no auto-sense qos 802.1p-override**
- **default auto-sense qos 802.1p-override**

### Default

802.1p Override is enabled by default.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense voice i-sid <1-16777215>

---

Configures Auto-sense voice information on IP phones.

## Syntax

- **auto-sense voice i-sid <1-16777215> c-vid<c-vid>**
- **auto-sense voice i-sid <1-16777215> untagged**
- **no auto-sense voice**

## Command Parameters

### <c-vid>

Specifies the customer VLAN ID that maps to the specified port or ports. Different hardware platforms support different customer VLAN ID ranges. Use the CLI Help to see the available range for the switch.

### untagged

Specifies the VLAN tagging type as untagged.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## auto-sense wait-interval

---

Configures the time, in seconds, for Auto-sense to wait for a Link Layer Discovery Protocol (LLDP) neighbor to be detected in the Auto-sense wait state before transitioning to the Auto-sense onboarding state.

## Syntax

- **auto-sense wait-interval <10-120>**
- **default auto-sense wait-interval**

## Command Parameters

<10-120>

Specifies the time interval, in seconds.

## Default

The default value is 35.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## banner

---

Configure the CLI logon banner to display a warning message to users before authentication.

## Syntax

- **banner custom**
- **banner displaymotd**
- **banner motd WORD<1-1516>**
- **banner static**
- **banner WORD<1-80>**
- **default banner**
- **default banner displaymotd**
- **default banner motd**
- **no banner**
- **no banner displaymotd**
- **no banner motd**

## Command Parameters

custom

Activates the custom banner.

**displaymotd**

Activates or disables the message of the day.

**motd WORD<1-1516>**

Creates a message of the day to display with the logon banner. To provide a string with spaces, include the text in quotation marks ("").

**static**

Activates static banner.

**WORD<1-80>**

Adds lines of text to the CLI logon banner.

## Default

The default configuration uses the default banner with no message of the day.

## Command Mode

Global Configuration

## boot config choice

---

Change the boot source order to change the order in which the system accesses the configuration files. If you change the primary source, the system uses your configuration first, and then accesses the default locations. If the default locations do not contain a configuration or backup configuration file, the system loads the default configuration.

## Syntax

- **boot config choice primary backup-config-file WORD<0-255>**
- **boot config choice primary config-file WORD<0-255>**
- **default boot config choice primary**
- **default boot config choice primary backup-config-file**

## Command Parameters

{backup-config-file |config-file}

Specifies that the boot source uses either the configuration file or a backup configuration file.

**WORD<0-255>**

Identifies the configuration file. WORD<0-255> is the device and file name, up to 255 characters including the path, in one of the following formats: a.b.c.d:<file>, or /intflash/<file>.

## Default

By default, the primary source is the internal flash.

## Command Mode

Global Configuration

### boot config flags advanced-feature-bandwidth-reservation

---

Enables the switch to support advanced features such as SPB, SMLT, and vIST by reserving ports as loopback ports.

#### Syntax

- **boot config flags advanced-feature-bandwidth-reservation high**
- **boot config flags advanced-feature-bandwidth-reservation low**
- **boot config flags advanced-feature-bandwidth-reservation vim**
- **default boot config flags advanced-feature-bandwidth-reservation**
- **no boot config flags advanced-feature-bandwidth-reservation**

#### Command Parameters

##### high

Reserves the maximum bandwidth for the advanced features. Depending on the hardware platform, the number of reserved ports is different.

##### low

Reserves less bandwidth to support minimum functionality for advanced features. Depending on the hardware platform, the number of reserved ports is different.

##### vim

Reserves the internal Versatile Interface Module (VIM) ports as loopback ports.

#### Default

The default for XA1400 and 5420 series is enabled with low level which means the switch operates in Full Feature mode but with less bandwidth to support minimum functionality for advanced features. The default for 5520 series is enabled with vim level if VIM is not installed in the switch, else low level is enabled.

## Command Mode

Global Configuration

#### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

If your switch does not support this boot configuration flag, it is because the hardware reserves the bandwidth automatically with no user interaction.

You must save the configuration and restart the switch for a configuration change to take effect.

You must ensure your configuration does not include reserved ports before you enable this feature. If the configuration includes reserved ports after you enable this feature and restart the switch, the switch aborts loading the configuration.

The vim parameter is only supported on the 5520 Series.

## boot config flags block-snmp

---

Activate or disable Simple Network Management Protocol (SNMP) management.

### Syntax

- **boot config flags block-snmp**
- **default boot config flags block-snmp**
- **no boot config flags block-snmp**

### Default

The default is disabled.

### Command Mode

Global Configuration

## boot config flags debug-config

---

Activate or disable run-time debugging of the configuration file.

### Syntax

- **boot config flags debug-config**
- **boot config flags debug-config console**
- **boot config flags debug-config file**
- **default boot config flags debug-config**
- **no boot config flags debug-config**

### Command Parameters

#### console

Displays the line-by-line configuration file processing and result of the execution on the console while the device loads the configuration file.

#### file

Logs the line-by-line configuration file processing and result of the execution to the debug file while the device loads the configuration file.

The system logs the debug config output to `/intflash/debugconfig_primary.txt` for the primary configuration file. The system logs the debug config output to `/intflash/debugconfig_backup.txt` for the backup configuration, if the backup configuration file loads.

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

After you enable debug-config and save the configuration, the debug output either displays on the console or logs to an output file the next time the switch reboots. You do not have to restart the switch after you enable debug-config unless you want to immediately debug the configuration.

## boot config flags debugmode

---

Control whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the trace commands. If you enable this flag, the switch does not restart following a fatal error.



### Important

Do not change this flag unless directed by support.

## Syntax

- `boot config flags debugmode`
- `default boot config flags debugmode`
- `no boot config flags debugmode`

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

You must save the configuration and reboot the switch for a configuration change to take effect.



---

## boot config flags dvr-leaf-mode

---

Enables an SPB node to be configured as a DvR Leaf.

### Syntax

- **boot config flags dvr-leaf-mode**
- **default boot config flags dvr-leaf-mode**
- **no boot config flags dvr-leaf-mode**

### Default

The default is disabled.

### Command Mode

Global Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## boot config flags enhancedsecure-mode

---

Enable enhanced secure mode. If you enable enhanced secure mode the switch provides role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.

### Syntax

- **boot config flags enhancedsecure-mode jitc**
- **boot config flags enhancedsecure-mode non-jitc**
- **default boot config flags enhancedsecure-mode**
- **no boot config flags enhancedsecure-mode**

### Command Parameters

{jitc | non-jitc}

Enables either the JITC or non-JITC enhanced secure mode.

### Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

You must save the configuration and reboot the switch for a configuration change to take effect.



### Note

When you migrate your switch from enhanced secure mode enabled to disabled, or from disabled to enabled, you must build a new configuration.

Do not use a configuration created in either enhanced secure mode disabled or enabled and expect it to transfer over to the new mode.

The configuration file cannot be guaranteed if you transfer between enhanced secure mode enabled to disabled, or from enhanced secure mode disabled to enabled.

---

## boot config flags factorydefaults

Specify whether the switch uses the factory default settings at startup.

## Syntax

- **boot config flags factorydefaults**
- **no boot config flags factorydefaults**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This flag resets to the default setting after the CPU restarts. If you change this flag, you must restart the switch.

---

## boot config flags flow-control-mode

Activate or disable flow control globally. When disabled, the system does not generate nor configure the transmission of flow control messages.

## Syntax

- **boot config flags flow-control-mode**
- **default boot config flags flow-control-mode**

- `no boot config flags flow-control-mode`

## Default

The default is disabled.

## Command Mode

Global Configuration

## boot config flags ftpd

---

Activate or disable the FTP server on the switch. To enable FTP, ensure that the tftpd flags is disabled.

## Syntax

- `boot config flags ftpd`
- `default boot config flags ftpd`
- `no boot config flags ftpd`

## Default

The default is disabled.

## Command Mode

Global Configuration

## boot config flags ha-cpu

---

Enable High Availability-CPU.

## Syntax

- `boot config flags ha-cpu`
- `default boot config flags ha-cpu`
- `no boot config flags ha-cpu`

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## boot config flags hsecure

Activate or disable High Secure mode. The hsecure command provides the following password behavior: 10 character enforcement, aging time, failed login attempt limitation, and designated IP address filtration.

### Syntax

- **boot config flags hsecure**
- **default boot config flags hsecure**
- **no boot config flags hsecure**

### Default

The default is disabled.

### Command Mode

Global Configuration

## Usage Guidelines

If you enable High Secure mode, you must restart the switch to enforce secure passwords. If you operate the switch in High Secure mode, the switch prompts a password change if you enter invalid-length passwords.

---

## boot config flags ipv6-egress-filter

Enables IPv6 egress filters.

### Syntax

- **boot config flags ipv6-egress-filter**
- **default boot config flags ipv6-egress-filter**
- **no boot config flags ipv6-egress-filter**

### Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

You must save the configuration and reboot the switch for a configuration change to take effect.

## boot config flags ipv6-mode

---

Activate or disable IPv6 mode.

## Syntax

- **boot config flags ipv6-mode**
- **default boot config flags ipv6-mode**
- **no boot config flags ipv6-mode**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## boot config flags linerate-directed-broadcast

---

Enables or disables datapath support for IP Directed Broadcast using port 1/46.

## Syntax

- **boot config flags linerate-directed-broadcast**
- **default boot config flags linerate-directed-broadcast**
- **no boot config flags linerate-directed-broadcast**

## Command Parameters

**false**

Disables datapath support for IP Directed Broadcast on port 1/46.

**true**

Enables datapath support for IP Directed Broadcast on port 1/46.

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

You must save the configuration and reboot the switch for a configuration change to take effect.



### Note

After setting this flag and saving the configuration, the software cannot be upgraded or downgraded to a software release that does not contain this directed broadcast hardware assist functionality.

---

## boot config flags logging

---

The system names log files according to the following:

- File names appear in 8.3 (xxxxxxx.sss) format.
- The first 6 characters of the file name contain the last three bytes of the chassis base MAC address.
- The next two characters in the file name specify the slot number of the CPU that generated the logs.
- The last three characters in the file name are the sequence number of the log file.

The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.

## Syntax

- **boot config flags logging**
- **default boot config flags logging**
- **no boot config flags logging**

## Default

The default is enabled.

## Command Mode

Global Configuration

## boot config flags macsec

---

Configure the boot flag to enable Media Access Control Security (MACsec) on all the ports.

### Syntax

- **default boot config flags macsec**
- **boot config flags macsec**
- **no boot config flags macsec**

### Default

None

### Command Mode

Global Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## boot config flags nni-mstp

---

Activate or disable MSTP and allow non SPBM B-VLAN configuration on SPBM NNI ports.

### Syntax

- **boot config flags nni-mstp**
- **default boot config flags nni-mstp**
- **no boot config flags nni-mstp**

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## boot config flags reboot

---

Activate or disable automatic reboot on a fatal error. The reboot command is equivalent to the debugmode command.



### Important

Do not change this parameter unless directed to do so by Technical Support.

### Syntax

- `boot config flags reboot`
- `default boot config flags reboot`
- `no boot config flags reboot`

### Default

The default is enabled.

### Command Mode

Global Configuration

### Usage Guidelines

You must save the configuration and reboot the switch for a configuration change to take effect.

---

## boot config flags rlogind

---

Activate or disable the remote login (rlogin) and remote shell (rsh) server.

### Syntax

- `boot config flags rlogind`
- `default boot config flags rlogind`
- `no boot config flags rlogind`

### Default

The default is disabled.

### Command Mode

Global Configuration



## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## boot config flags spanning-tree-mode

---

Specify the Multiple Spanning Tree Protocol (MSTP) or Rapid Spanning Tree Protocol (RSTP) mode. If you do not specify a protocol, the switch uses the default mode.

### Syntax

- **boot config flags spanning-tree-mode mstp**
- **boot config flags spanning-tree-mode rstp**
- **default boot config flags spanning-tree-mode**
- **no boot config flags spanning-tree-mode**

### Default

The default is MSTP.

### Command Mode

Global Configuration

## Usage Guidelines

You must save the configuration and reboot the switch for a configuration change to take effect.

## boot config flags spbm-config-mode

---

Enable SPBM configuration mode.

### Syntax

- **boot config flags spbm-config-mode**
- **default boot config flags spbm-config-mode**
- **no boot config flags spbm-config-mode**

### Default

The default value is enabled.

### Command Mode

Global Configuration

---

## boot config flags sshd

---

Activate or disable the Secure Shell (SSH) server service.

### Syntax

- `boot config flags sshd`
- `default boot config flags sshd`
- `no boot config flags sshd`

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## boot config flags syslog-rfc5424-format

---

Enables syslog and logging to use the RFC 5424 formatting. With this formatting, the syslog header has a timestamp conforming to RFC 3339, which helps identify the syslog generation time by indicating the year, milliseconds, and timezone, as well as the hostname from which the message is generated.

### Syntax

- `boot config flags syslog-rfc5424-format`
- `default boot config flags syslog-rfc5424-format`
- `no boot config flags syslog-rfc5424-format`

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## boot config flags telnetd

---

Activate or disable the Telnet server service.

### Syntax

- `boot config flags telnetd`
- `default boot config flags telnetd`

- `no boot config flags telnetd`

## Default

The default is disabled.

## Command Mode

Global Configuration

## boot config flags tftpd

---

Activate or disable Trivial File Transfer Protocol (TFTP) server service.

## Syntax

- `boot config flags tftpd`
- `default boot config flags tftpd`
- `no boot config flags tftpd`

## Default

The default is disabled.

## Command Mode

Global Configuration

## boot config flags trace-logging

---

Activate or disable the creation of trace logs.



### Important

Do not change this parameter unless directed to do so by Technical Support.

## Syntax

- `boot config flags trace-logging`
- `default boot config flags trace-logging`
- `no boot config flags trace-logging`

## Default

The default is disabled.

## Command Mode

Global Configuration

### boot config flags urpf-mode

---

Enable the urpf-mode boot flag.

#### Syntax

- **boot config flags urpf-mode**
- **default boot config flags urpf-mode**
- **no boot config flags urpf-mode**

#### Default

The default is disabled.

## Command Mode

Global Configuration

#### Usage Guidelines

You must save the configuration and reboot the switch for a configuration change to take effect.

### boot config flags verify-config

---

Activates syntax checking of the configuration file.

When you enable the verify-config flags, the primary configuration file is pre-checked for syntax errors. If the system finds an error, the system loads the backup configuration file.

If you disable the verify-config flags, the system ignores any lines with errors during loading of the primary configuration file.

If the primary configuration file is not present or cannot be found, the system tries to load the backup file. The system does not check the backup file for syntax errors. The system ignores any lines with errors during the loading of the backup configuration file.

If no backup file exists, the system defaults to factory defaults.

#### Syntax

- **boot config flags verify-config**
- **default boot config flags verify-config**
- **no boot config flags verify-config**

## Default

The default is enabled.

## Command Mode

Global Configuration

---

## boot config flags vrf-scaling

Increases the maximum number of VRFs and Layer 3 VSNs that the switch supports.

## Syntax

- **boot config flags vrf-scaling**
- **default boot config flags vrf-scaling**
- **no boot config flags vrf-scaling**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

Platforms that do not support this boot configuration flag automatically support the maximum number of VRFs without additional VLAN reservation.

---

## boot config flags vxlan-gw-full-interworking-mode

Activate or disable VXLAN Gateway in Full Interworking Mode, which supports SPB, SMLT, and vIST.

## Syntax

- **boot config flags vxlan-gw-full-interworking-mode**
- **default boot config flags vxlan-gw-full-interworking-mode**
- **no boot config flags vxlan-gw-full-interworking-mode**

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## boot config host

---

Configure the remote host logon to modify parameters for FTP and TFTP access. Use the default parameters for TFTP transfers. If you want to use FTP as transfer mechanism, you must change the password to a valid value.

## Syntax

- `boot config host ftp-debug`
- `boot config host password WORD<0-16>`
- `boot config host tftp-debug`
- `boot config host tftp-hash`
- `boot config host tftp-rexmit <1-120>`
- `boot config host tftp-timeout <1-120>`
- `boot config host user WORD<0-16>`
- `default boot config host ftp-debug`
- `default boot config host tftp-debug`
- `default boot config host tftp-hash`
- `default boot config host tftp-rexmit`
- `default boot config host tftp-timeout`
- `default boot config host user`
- `no boot config host ftp-debug`
- `no boot config host tftp-debug`
- `no boot config host tftp-hash`

## Command Parameters

### ftp-debug

Enables or disables the debug mode on FTP. If you enable the debug mode, debug messages appear on the management console screen. The default is disabled.

### password WORD<0-16>

Configures the password to enable FTP transfers. WORD<0-16> is the password, up to 16 characters. After you configure this password, you can use only FTP for remote host logon.

**Important**

This password must match the password for the FTP server or the FTP operation fails. Also, if you configure the password to a valid value, then all copying to and from the network uses FTP instead of TFTP.

If the user name or password is incorrect, copying over the network fails.

**tftp-debug**

Enables or disables debug mode on TFTP or TFTPd. If you enable the debug mode, debug messages appear on the management console screen. The default is disabled.

**Important**

tftp-debug should be used exclusively to transfer small files less than 1MB in size. Using it for larger files might cause unwanted behavior, such as transfer failure.

**tftp-hash**

Enables or disables the TFTP hash bucket display. The default is disabled.

**tftp-rexmit <1-120>**

Configures the TFTP retransmission timeout in seconds. The default is 2.

**tftp-timeout <1-120>**

Configures the TFTP timeout in seconds. The default is 6.

**user WORD<0-16>**

Configures the remote user logon. WORD<0-16> is the user logon name (up to 16 characters). The default is target.

## Default

None

## Command Mode

Global Configuration

## boot config loadconfigtime

---

Set the timeout for loading the configuration file.

## Syntax

- **boot config loadconfigtime <0-300>**
- **default boot config loadconfigtime**

## Command Parameters

<0-300>

Specifies the timeout for loading the configuration file in seconds.

## Default

The default is 60 seconds.

## Command Mode

Global Configuration

---

## boot config logfile

Configure logfile parameters.

- The log file is named using an 8.3 (xxxxxxx.sss) format.
- The first six characters of the file name contain the last three bytes of the chassis base MAC address.
- The next two characters specify the slot number of the CP that generated the logs.
- The last three characters denote the sequence number of the log file.

Multiple sequence numbers are generated for the same chassis and same slot, if the maximum log file size is reached.

## Syntax

- **boot config logfile <64-500> <500-16384> <10-90>**
- **default boot config logfile**

## Command Parameters

<10-90>

Specifies the maximum percentage, from 10-90%, of space on the external storage device the log file can use. The switch does not support this parameter.

<500-16384>

Specifies the maximum size of the log file from 500-16384 KB.

<64-500>

Specifies the minimum free memory space on the external storage device from 64-500 KB. The switch does not support this parameter.

## Default

None



## Command Mode

Global Configuration

### boot config multicast

---

Configure multicast parameters.

#### Syntax

- **boot config multicast**
- **default boot config multicast**

#### Default

None

## Command Mode

Global Configuration

### boot config sio console baud

---

Configure the serial port devices to define connection settings for the console port.

#### Syntax

- **boot config sio console baud <9600 - 115200> {<1-8> | SF1 | SF2 | SF3}**
- **default boot config sio console baud**

#### Command Parameters

**<9600-115200> {<1-8> | SF1 | SF2 | SF3}**

Configures the baud rate for the port.

#### Default

The default value differs depending on the platform:

- 5420 Series — 115200
- 5520 Series — 115200
- VSP 4450 Series — 9600
- VSP 4900 Series — 115200
- VSP 7200 Series — 9600
- VSP 7400 Series — 115200
- VSP 8200 Series — 9600
- VSP 8400 Series — 9600

- VSP 8600 Series — 115200
- XA1400 Series — 115200

## Command Mode

Global Configuration

## certificate ca

Configures the certificate authority (CA) and perform related actions. You can configure only one CA in a device at a time.

## Syntax

- **certificate ca WORD<1-45> [action caauth | action enroll validity-days <7-1185> | action get-crl | action install | action noop | action remove | action renew validity-days <7-1185> | ca-url WORD<0-1000> | common-name WORD<0-64> | install-file root-ca-filename WORD<1-80> | key-name<0-64> | sha256-fingerprint WORD<64-64> | use-post <true|false>]**
- **default certificate ca**
- **no certificate ca WORD<1-45> [action | ca-url | common-name | key-name | sha256-fingerprint | use-post]**

## Command Parameters

### action caauth

Authenticates the trustpoint CA by getting the certificate of the CA and stores the CA certificate locally.

### action enroll [validity-days <7-1185>]

Generates certificate signing request to obtain identity certificate from configured trustpoint CA, gets the digital certificate, and stores it locally, associating with the trustpoint CA. The validity-days specifies the number of days for which the certificate remains valid. The default value is 365 days.

### action get-crl

Gets the Certificate Revocation List from the CDP and stores into a file.

### action install

Installs the subject certificate obtained from the given trustpoint CA.

### action noop

Specifies that no operation should be performed after configuring trustpoint.

### action remove

Releases the locally stored certificate associated with the trustpoint CA post revocation.

### action renew [challengepassword WORD<0-128>]

This password is provided offline by the CA during the end entity registration. The length of the password is from 0 to 128.

**action renew [validity-days <7-1185>]**

Generates certificate renewal request for given trustpoint CA, gets the digital certificate, and stores it locally by replacing the old certificate with the new one. The validity-days specifies the number of days for which the certificate remains valid. The default value is 365 days.

**ca-url WORD<0-1000>**

Specifies the trusted CA url.

**common-name WORD<0-64>**

Specifies the name of the owner of the device or user.

**install-file [rootca-filename WORD<1-80>]**

Installs the Root CA file obtained offline from the CA.

**key-name WORD<0-45>**

Specifies the key pair generated by the command that was first associated with the CA trustpoint.

**sha256-fingerprint WORD<64-64>**

Specifies an encrypted fingerprint of the expected certificate to match.

**use-post <true|false>**

Specify the HTTP request style. The default value is True.

**WORD<1-45>**

Specifies the name of the certificate authority. It should be alphanumeric and case-sensitive with maximum length is 45 characters.

## Default

None

## Command Mode

Global Configuration

## certificate generate-csr

---

Generate a certificate signing request (CSR) and store it in a file.

## Syntax

- **certificate generate-csr**
- **certificate generate-csr relaxed**

## Command Parameters

relaxed

Uses relaxed-mode CSR generation for less restrictive consistency checks and subject alternative name inclusion in the CSR.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

To use relaxed mode, you must configure at least one certificate subject common name on the switch.

---

## certificate generate-keypair

Generate the private and public key pair for the specific cryptography type.

## Syntax

- **certificate generate-keypair type rsa size <2048>**
- **default certificate generate-keypair**
- **no certificate generate-keypair**

## Command Parameters

**size 2048**

Specifies the size or modulus of key-pair to be generated. The value should be 2048.

**type rsa**

Specifies type of cryptography algorithm used to generate the key-pair.

## Default

None

## Command Mode

Global Configuration

---

## certificate install-file

Install certification authority (CA), root CA, or subject certificates, or a Certificate Revocation List (CRL) file obtained offline from the CA.

## Syntax

- `certificate install-file offline-ca-filename WORD<1-80>`
- `certificate install-file offline-crl-filename WORD<1-80>`
- `certificate install-file offline-root-ca-filename WORD<1-80>`
- `certificate install-file offline-subject-filename WORD<1-80>`
- `certificate install-file offline-subject-filename WORD<1-80> relaxed`
- `certificate install-file offline-subject-filename WORD<1-80> relaxed pkcs12-password WORD<1-128>`
- `no certificate install-file offline-ca-filename WORD<1-80>`
- `no certificate install-file offline-crl-filename WORD<1-80>`
- `no certificate install-file offline-root-ca-filename WORD<1-80>`
- `no certificate install-file offline-subject-filename WORD<1-80>`

## Command Parameters

`offline-ca-filename WORD<1-80>`

Specifies the CA file name obtained from the CA.

`offline-crl-filename WORD<1-80>`

Specifies the CRL file obtained from the CA.

`offline-root-ca-filename WORD<1-80>`

Specifies the root CA file name obtained from the CA.

`offline-subject-filename WORD<1-80>`

Specifies the subject certificate file name obtained from the CA.

`relaxed pkcs12-password WORD<1-128>`

Uses the relaxed mode for offline subject certificate installation for less restrictive consistency checks.

You can also install a PKCS12 format certificate and secret key in relaxed mode. *WORD<1-128>* is the password to extract the PKCS12 container. If you do not include this parameter, the supported format is Distinguished Encoding Rules (DER).

## Default

None

## Command Mode

Global Configuration

## certificate subject

---

Configure the device subject parameters to identify the device, such as the name, Email ID, company, department, location, and subject name.

### Syntax

- `certificate subject common-name WORD<0-64>`
- `certificate subject country WORD<0-128>`
- `certificate subject e-mail WORD<0-254>`
- `certificate subject locality WORD<0-128>`
- `certificate subject organization WORD<0-64>`
- `certificate subject province WORD<0-128>`
- `certificate subject-name WORD <1-45>`
- `certificate subject unit WORD<0-64>`
- `default certificate subject`
- `no certificate subject`
- `no certificate subject common-name`
- `no certificate subject country`
- `no certificate subject e-mail`
- `no certificate subject locality`
- `no certificate subject organization`
- `no certificate subject province`
- `no certificate subject unit`
- `no certificate subject-name`

### Command Parameters

**common-name WORD<0-64>**

Specifies the name of the subject sending the Certificate Signing Request to the Certificate Authority.

**country WORD<2-2>**

Specifies the country of the subject sending the Certificate Signing Request to the Certificate Authority.

**e-mail WORD<0-254>**

Specifies the Email address of the subject sending the Certificate Signing Request to the Certificate Authority.

**locality WORD<0-128>**

Specifies the locality of the subject sending the Certificate Signing Request to the Certificate Authority.

**organization WORD<0-64>**

Specifies the organization of the subject sending the Certificate Signing Request to the Certificate Authority.

**province WORD<0-128>**

Specifies the province of the subject sending the Certificate Signing Request to the Certificate Authority.

**subject-name WORD<0-45>**

Specifies the subject Distinguished Name (DN) of the subject to be used in local digital certificate request. You can configure up to 10 subject DN identities. If a subject name is not specified, the switch generates one.

**unit WORD<0-64>**

Specifies the organizational unit of the subject sending the Certificate Signing Request to the Certificate Authority.

## Default

None

## Command Mode

Global Configuration

## certificate subject-alternative-name

---

Use a subject alternative name to associate values, such as an email address, an IP address, a fully qualified domain name (FQDN), or a subject name with a security certificate.

## Syntax

- **certificate subject-alternative-name dns WORD<1-255>**
- **certificate subject-alternative-name e-mail WORD<1-255>**
- **certificate subject-alternative-name ip WORD<1-255>**
- **certificate subject-alternative-name subject-name WORD<1-45>**
- **default certificate subject-alternative-name**
- **no certificate subject-alternative-name**
- **no certificate subject-alternative-name dns WORD<1-255>**
- **no certificate subject-alternative-name e-mail WORD<1-255>**
- **no certificate subject-alternative-name ip WORD<1-255>**
- **no certificate subject-alternative-name subject-name WORD<1-45>**

## Command Parameters

**dns WORD<1-255>**

Specifies the FQDN to add as a subject alternative name.

**e-mail WORD<1-255>**

Specifies the e-mail address to add as a subject alternative name.

**ip WORD<1-255>**

Specifies the IP address to add as a subject alternative name.

**subject-name WORD<1-45>**

Specifies the subject alternative name of the subject used in local digital certificate request.

## Default

By default, subject alternative names are not configured.

## Command Mode

Global Configuration

## cfm cmac enable

---

Enables CFM for C-VLANs, which creates the MD, MA, and MEP, and then associate the MEP and MIP level to C-VLANs.

## Syntax

- **cfm cmac enable**
- **no cfm cmac enable**

## Default

The default is disabled

## Command Mode

Global Configuration

## cfm cmac level <0-7>

---

Configures the maintenance level for the MEP and MIP associated with C-VLANs.

## Syntax

- **cfm cmac level <0-7>**
- **default cfm cmac level**

## Command Parameters

<0-7>



Specifies the global C-MAC CFM maintenance level for the chassis within the range of 0 to 7.

## Default

The default is 4.

## Command Mode

Global Configuration

## cfm cmac mepid <1-8191>

---

Assigns a global MEP ID for all CFM CMAC MEPs.

## Syntax

- **cfm cmac mepid <1-8191>**
- **default cfm cmac mepid**

## Command Parameters

**<1-8191>**

Specifies the global MEP ID within the range of 1 to 8191.

## Default

The default is 1.

## Command Mode

Global Configuration

## cfm maintenance-association

---

Create the Connectivity Fault Management (CFM) Maintenance-Association (MA).

## Syntax

- **cfm maintenance-association WORD<1-22> WORD<1-22>**
- **cfm maintenance-association WORD<1-22> WORD<1-22> index <1-2147483647>**
- **no cfm maintenance-association WORD<1-22> WORD<1-22>**

## Command Parameters

**index <1-2147483647>**

Specifies a Maintenance-Association (MA) entry index.

**WORD<1-22>**

Creates the Connectivity Fault Management (CFM) Maintenance-Association (MA).

## Default

The default is disabled.

## Command Mode

Global Configuration

## cfm maintenance-domain

---

Create the Connectivity Fault Management (CFM) Maintenance-Domain (MD).

## Syntax

- **cfm maintenance-domain WORD<1-22>**
- **cfm maintenance-domain WORD<1-22> index <1-2147483647>**
- **cfm maintenance-domain WORD<1-22> index <1-2147483647> maintenance-level <0-7>**
- **cfm maintenance-domain WORD<1-22> level <0-7>**
- **cfm maintenance-domain WORD<1-22> maintenance-level <0-7>**
- **cfm maintenance-domain WORD<1-22> maintenance-level <0-7> index <1-2147483647>**
- **no cfm maintenance-domain WORD<1-22>**

## Command Parameters

**index <1-2147483647>**

Specifies a Maintenance-Domain (MD) entry index.

**level <0-7>**

Specifies the Maintenance-Domain (MD) level for an existing Maintenance-Domain (MD).

**maintenance-level <0-7>**

Specifies the Maintenance-Domain (MD) maintenance level when creating the Maintenance-Domain (MD).

**WORD<0-22>**

Specifies the Maintenance-Domain (MD) name.

**WORD<0-22>**

Specifies the Maintenance-Association (MA) name.

## Default

None

## Command Mode

Global Configuration

# cfm maintenance-endpoint

---

Create the Connectivity Fault Management (CFM) Maintenance-Endpoint (MEP).

## Syntax

- **cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191>**
- **cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191> enable**
- **cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191> state enable**
- **no cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191>**
- **no cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191> enable**

## Command Parameters

**<1-8191>**

Specifies the Maintenance Endpoint (MEP) ID.

**enable**

Enables an existing Maintenance Endpoint (MEP). Use this parameter with the no option to disable an existing MEP.

**state enable**

Enables the Maintenance Endpoint (MEP) when creating the MEP. Use the no option to disable the Maintenance Endpoint.

**WORD<1-22>**

Specifies the Maintenance-Domain (MD) name.

**WORD<1-22>**

Specifies the Maintenance-Association (MA) name.

## Default

None

## Command Mode

Global Configuration

---

## cfm spbm enable

---

Enables CFM for B-VLANs, which creates the MD, MA, and MEP, and then associate the MEP and MIP level to B-VLANs.

### Syntax

- **cfm spbm enable**
- **no cfm spbm enable**

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## cfm spbm level

---

Configures the maintenance level for every CFM SPBM MEP and MIP level on all SPBM VLANs.

### Syntax

- **cfm spbm level <0-7>**
- **default cfm spbm level**

### Command Parameters

<0-7>

Specifies the maintenance level for every CFM SPBM MEP and MIP level on all SPBM VLANs. The default is 4.

### Default

The default is 4.

### Command Mode

Global Configuration

---

## cfm spbm mepid

---

Assigns a global MEP ID for all CFM SPBM MEPs.

## Syntax

- **cfm spbm mepid <1-8191>**
- **default cfm spbm mepid**

## Command Parameters

<1-8191>

Specifies the global MEP ID for all CFM SPBM MEPs. The default is 1.

## Default

The default is 1.

## Command Mode

Global Configuration

## cli password

---

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive the switch, use default passwords to initially access CLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

## Syntax

- **cli password WORD<1-20> layer1**
- **cli password WORD<1-20> layer2**
- **cli password WORD<1-20> layer3**
- **cli password WORD<1-20> read-only**
- **cli password WORD<1-20> read-write**
- **cli password WORD<1-20> read-write-all**

## Command Parameters

<layer1|layer2|layer3|read-only|read-write|read-write-all>

Changes the password for the specific access level.

- The read-only default logon is ro and the default password is ro.
- The Layer 1 read/write logon is l1 and the default password is l1.
- The Layer 2 read/write logon is l2 and the default password is l2.
- The Layer 3 read/write logon is l3 and the default password is l3.
- The read/write logon is rw and the default password is rw.
- The read/write/all logon is rwa and the default password is rwa.

WORD<1-20>

Specifies the user login name.

## Default

None

## Command Mode

Global Configuration

## cli timeout

---

Configure the idle timeout period before automatic logoff for CLI and Telnet sessions.

### Syntax

- **cli timeout <30-65535>**
- **default cli timeout**

### Command Parameters

**<30-65535>**

Configures the timeout value, in seconds, to wait for a Telnet or CLI login session before terminating the connection.

### Default

The default is 900 seconds.

### Command Mode

Global Configuration

## clilog

---

Use CLI logging to track all CLI commands executed and for fault management purposes. CLI commands are logged to the system log file as CLILog module.

### Syntax

- **clilog enable**
- **clilog maxfilesize <64-256000>**
- **clilog syslog-host enable**
- **default clilog**
- **default clilog enable**
- **default clilog maxfilesize**

- **default clilog syslog-host enable**
- **no clilog enable**
- **no clilog syslog-host enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

## clock time-zone

---

Configure the time zone to use an internal system clock to maintain accurate time. The time zone data in Linux includes daylight changes for all time zones from 1901 to 2038. You do not need to configure daylight saving time.

## Syntax

- **clock time-zone**
- **clock time-zone WORD<1-10> [WORD<1-20>] [WORD<1-20> ]**
- **default clock time-zone**
- **no clock time-zone**

## Command Parameters

### WORD<1-10>

Specifies a directory name or a time zone name in `/usr/share/zoneinfo`, for example, Africa, Australia, Antarctica, or US. To see a list of options, enter `clock time-zone` at the command prompt without variables.

### WORD<1-20> WORD<1-20>

The first instance of `WORD<1-20>` is the area within the timezone. The value represents a time zone data file in `/usr/share/zoneinfo/WORD<1-10>/`, for example, Shanghai in Asia.

The second instance of `WORD<1-20>` is the subarea. The value represents a time zone data file in `/usr/share/zoneinfo/WORD<1-10>/WORD<1-20>/`, for example, Vevay in America/Indiana.

To see a list of options, enter `clock time-zone` at the command prompt without variables.

## Default

The default is Coordinated Universal Time (UTC).

## Command Mode

Global Configuration

## debug ip pim

---

Configures debug commands for pim messages globally.

### Syntax

- `debug ip pim assert`
- `debug ip pim bstrap`
- `debug ip pim group {A.B.C.D}`
- `debug ip pim hello`
- `debug ip pim join-prune`
- `debug ip pim pimdbglog`
- `debug ip pim pimdbgtrace`
- `debug ip pim rcv-dbg-trace`
- `debug ip pim register`
- `debug ip pim regstop`
- `debug ip pim rp-adv`
- `debug ip pim send-dbg-trace`
- `debug ip pim source {A.B.C.D}`

### Command Parameters

#### assert

Set assert debug trace to true.

#### bstrap

Set bstrap trace to true.

#### group {A.B.C.D}

Set group value to specific multicast group value.

#### hello

Set hello debug trace to true.

#### join-prune

Set joinprune debug trace to true.

#### pimdbglog

Set pim debug log to true.

#### pimdbgtrace

Set pim debug trace to true.

#### rcv-dbg-trace

Set rcv debug trace to true.

#### register

Set register debug trace to true.



**regstop**

Set register stop debug trace to true.

**rp-adv**

Set rp-adv debug trace to true.

**send-dbg-trace**

Set send trace to true.

**source {A.B.C.D}**

Set source value to specific source ip-addr.

## Default

None

## Command Mode

Global Configuration

## dvr controller

---

Configures a switch as the DvR Controller of a DvR domain, whose domain ID you specify. Configuring a switch as the Controller enables DvR globally on the node.

## Syntax

- **default dvr controller inject-default-route-disable**
- **dvr controller <1-255>**
- **dvr controller inject-default-route-disable**
- **no dvr controller**
- **no dvr controller inject-default-route-disable**

## Command Parameters

<1-255>

Configures a switch as the DvR Controller of a DvR domain, whose domain ID you specify. Configuring a switch as the Controller enables DvR globally on the node.

## Default

none

## Command Mode

Global Configuration

---

## dvr controller <1-255> inject-default-route-disable

---

Disables injection of default routes for the GRT on the DvR Controller.

### Syntax

- **default dvr controller <1-255> inject-default-route-disable**
- **dvr controller <1-255> inject-default-route-disable**

### Default

The default is enable

### Command Mode

Global Configuration

---

## dvr leaf

---

Configures a switch as the DvR Leaf in a DvR domain, whose domain ID you specify. Configuring a switch as the DvR Leaf enables DvR globally on the node.

### Syntax

- **dvr leaf <1-255>**
- **no dvr leaf**

### Command Parameters

<1-255>

Configures a switch as the DvR Leaf in a DvR domain, whose domain ID you specify. Configuring a switch as the DvR Leaf enables DvR globally on the node.

### Default

none

### Command Mode

Global Configuration

---

## dvr leaf <1-255> virtual-ist {A.B.C.D/X} {A.B.C.D} peer-ip {A.B.C.D} cluster-id <1-1000>

---

Configures vIST on a DvR Leaf node pair. When you configure vIST on a DvR Leaf node pair, the switch generates an I-SID from the configured cluster ID. This I-SID is unique across the SPB network as long as the cluster ID is unique across the SPB network, for the vIST pair.

You can configure only one instance of vIST on the Leaf node pair. To configure vIST, both nodes must be Leaf nodes. You cannot configure vIST, for example, on a Controller-Leaf node pair. Also both the nodes must belong to the same DvR domain.

vIST configuration over Leaf nodes in different domains is not supported.

## Syntax

- **dvr leaf <1-255> virtual-ist {A.B.C.D/X} {A.B.C.D} peer-ip {A.B.C.D} cluster-id <1-1000>**

## Command Parameters

**none**

Configures vIST on a DvR Leaf node pair

## Default

none

## Command Mode

Global Configuration

## **dvr leaf <1-255> virtual-ist {A.B.C.D} {A.B.C.D} peer-ip {A.B.C.D} cluster-id <1-1000>**

Configures vIST on a DvR Leaf node pair. When you configure vIST on a DvR Leaf node pair, the switch generates an I-SID from the configured cluster ID. This I-SID is unique across the SPB network as long as the cluster ID is unique across the SPB network, for the vIST pair.

You can configure only one instance of vIST on the Leaf node pair. To configure vIST, both nodes must be Leaf nodes. You cannot configure vIST, for example, on a Controller-Leaf node pair. Also both the nodes must belong to the same DvR domain.

vIST configuration over Leaf nodes in different domains is not supported.

## Syntax

- **dvr leaf <1-255> virtual-ist {A.B.C.D} {A.B.C.D} peer-ip {A.B.C.D} cluster-id <1-1000>**

## Command Parameters

**none**

Configures vIST on a DvR Leaf node pair

## Default

none

## Command Mode

Global Configuration

## dvr redistribute direct

---

Enables route redistribution of direct routes on the GRT. The route type is internal.

## Syntax

- **dvr redistribute direct enable**
- **dvr redistribute direct metric <0-65535>**
- **dvr redistribute direct route-map**

## Command Parameters

**enable**

Enables route redistribution of direct routes on the GRT. The route type is internal.

**metric <0-65535>**

Configures the route redistribution metric for direct routes on the GRT.

**route-map**

Configures the route policy for route redistribution of direct routes, on the GRT.

## Default

The default is disable

## Command Mode

Global Configuration

## dvr redistribute static

---

Enables route redistribution of static routes on the GRT. The route type is internal.

## Syntax

- **dvr redistribute static enable**
- **dvr redistribute static metric <0-65535>**
- **dvr redistribute static route-map**

## Command Parameters

### **enable**

Enables route redistribution of static routes on the GRT. The route type is external.

### **metric <0-65535>**

Configures the route redistribution metric for static routes on the GRT.

### **route-map**

Configures the route policy for route redistribution of static routes, on the GRT.

## Default

The default is disable

## Command Mode

Global Configuration

## eapol auto-isid-offset

---

Configure an I-SID offset value, and globally enable I-SID offset for the Extensible Authentication Protocol (EAPoL) feature. The I-SID offset value is used to calculate an I-SID value for a Switched UNI if no I-SID value is provided by the RADIUS server. In that case, the I-SID value is calculated as follows: I-SID = VLAN ID + configured I-SID offset value.

## Syntax

- **default eapol auto-isid-offset**
- **eapol auto-isid-offset <0-15995903>**
- **eapol auto-isid-offset enable**
- **no eapol auto-isid-offset enable**

## Command Parameters

### **<0-15995903>**

Specifies the I-SID offset value used to calculate an I-SID value if no I-SID value is provided by the RADIUS server.

### **enable**

Enables I-SID offset globally on the switch.

## Default

The default status is disabled, and the default I-SID offset value is 15990000.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

Configure the I-SID offset value first, and then enable I-SID offset globally on the switch.

## eapol enable

---

Configure Extensible Authentication Protocol (EAPoL) on the switch.

## Syntax

- **default eapol enable**
- **eapol enable**
- **no eapol enable**

## Default

None

## Command Mode

Global Configuration

## eapol multihost non-eap-pwd-fmt

---

Configure the RADIUS password format for non-eap authentication for a radius server.

## Syntax

- **default eapol multihost non-eap-pwd-fmt**
- **eapol multihost non-eap-pwd-fmt**
- **eapol multihost non-eap-pwd-fmt ip-addr**
- **eapol multihost non-eap-pwd-fmt keystring**
- **eapol multihost non-eap-pwd-fmt mac-addr**
- **eapol multihost non-eap-pwd-fmt padding**
- **eapol multihost non-eap-pwd-fmt port-number**

## Command Parameters

ip-addr

Management ip-address of the switch.

**key WORD<1-32>**

Key string used in password format.

**mac-addr**

MAC address of the client.

**padding**

A dot(.) is used as delimiter.

**port-number**

Index of the port on which MAC is received.

## Default

None

## Command Mode

Global Configuration

## end

---

Use this command to return to the Privileged EXEC mode from Global Configuration mode or higher.

## Syntax

- **end**

## Default

None

## Command Mode

Global Configuration

## endpoint-tracking auto-isid-offset

---

Configure an I-SID offset value, and globally enable I-SID offset for the Endpoint Tracking feature. The I-SID offset value is used to calculate an I-SID value for a Switched UNI if no I-SID value is provided by the RADIUS server. In that case, the I-SID value is calculated as follows: I-SID = VLAN ID + configured I-SID offset value.

## Syntax

- **default endpoint-tracking auto-isid-offset**
- **endpoint-tracking auto-isid-offset <0-15995903>**

- **endpoint-tracking auto-isid-offset enable**
- **no endpoint-tracking auto-isid-offset enable**

## Command Parameters

<0-15995903>

Specifies the I-SID offset value used to calculate an I-SID value if no I-SID value is provided by the RADIUS server.

**enable**

Enables I-SID offset globally on the switch.

## Default

The default status is disabled, and the default I-SID offset value is 15990000.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

Configure the I-SID offset value first, and then enable I-SID offset globally on the switch.

If you have previously enabled Endpoint Tracking globally and want to change the currently configured I-SID offset value, you must disable Endpoint Tracking globally, change the I-SID value, and then re-enable Endpoint Tracking globally.

## endpoint-tracking enable (global)

---

Enable or disable Endpoint Tracking globally on a switch.

## Syntax

- **endpoint-tracking enable**
- **no endpoint-tracking enable**

## Default

Disabled

## Command Mode

Global Configuration



## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## endpoint-tracking visibility-mode

---

Enable or disable visibility mode for Endpoint Tracking.

### Syntax

- **default endpoint-tracking visibility-mode**
- **endpoint-tracking visibility-mode**
- **no endpoint-tracking visibility-mode**

### Default

The default is disabled.

### Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## energy-saver (global)

---

Configures the Energy Saver feature on the switch.

### Syntax

- **default energy-saver efficiency-mode**
- **default energy-saver enable**
- **default energy-saver poe-power-saving**
- **energy-saver efficiency-mode**
- **energy-saver enable**
- **energy-saver poe-power-saving**
- **no energy-saver efficiency-mode**
- **no energy-saver enable**
- **no energy-saver poe-power-saving**

## Command Parameters

### efficiency-mode

Enables efficiency mode on the switch.

- Efficiency mode enables Energy Saver globally and on all ports; it also enables PoE power saving.
- Efficiency mode creates a weekday schedule that starts at 6:00 p.m. and ends at 7:30 a.m.
- During the weekend Energy Saver is always activated.

### enable

Enables Energy Saver on the switch.

### poe-power-saving

Enables PoE power savings on the switch.

## Default

Disabled

## Command Mode

Global Configuration

## energy-saver schedule

Configures a scheduled time interval during which the switch will operate in low power state.

## Syntax

- **default energy-saver schedule {friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekday | weekend} <hhmm>**
- **energy-saver schedule {friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekday | weekend} <hhmm> activate**
- **energy-saver schedule {friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekday | weekend} <hhmm> deactivate**
- **no energy-saver schedule {friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekday | weekend} <hhmm>**

## Command Parameters

{friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekday | weekend}

Specifies the day(s) to enable Energy Saver feature on the switch.

<hhmm>

Specifies the hour and minutes to enable Energy Saver feature on the switch.

activate

Activates the scheduled event.

**deactivate**

Deactivates the scheduled event.

**Default**

Disabled

**Command Mode**

Global Configuration

---

**fa assignment-timeout**

---

Configure the Fabric Attach (FA) assignment time-out in seconds.

**Syntax**

- **default fa assignment-timeout**
- **fa assignment-timeout <30-480>**

**Command Parameters**

<30-480>

Specifies the FA assignment timeout in seconds. The default value is 240 seconds.

**Default**

None

**Command Mode**

Global Configuration

---

**fa discovery-timeout**

---

Configure the FA discovery time-out in seconds.

**Syntax**

- **default fa fa discovery-timeout**
- **fa discovery-timeout <30-480>**

**Command Parameters**

<30-480>

Specifies the FA discovery timeout in seconds. The default value is 240 seconds.

## Default

None

## Command Mode

Global Configuration

---

## fa enable

Enable FA globally.

## Syntax

- **fa enable**
- **no fa enable**

## Default

None

## Command Mode

Global Configuration

---

## fa zero-touch-client

Configure FA zero touch for client.

## Syntax

- **fa zero-touch-client standard <camera|ona-sdn|ona-spb-over-ip|phone|router|security-device|srvr-endpt|switch|video|virtual-switch|wap-type1|wap-type2> i-sid <1-15999999>**
- **fa zero-touch-client standard camera i-sid <1-15999999>**
- **fa zero-touch-client standard ona-sdn i-sid <1-15999999>**
- **fa zero-touch-client standard ona-spb-over-ip i-sid <1-15999999>**
- **fa zero-touch-client standard phone i-sid <1-15999999>**
- **fa zero-touch-client standard router i-sid <1-15999999>**
- **fa zero-touch-client standard security-device i-sid <1-15999999>**
- **fa zero-touch-client standard srvr-endpt i-sid <1-15999999>**
- **fa zero-touch-client standard switch i-sid <1-15999999>**
- **fa zero-touch-client standard video i-sid <1-15999999>**
- **fa zero-touch-client standard virtual-switch i-sid <1-15999999>**
- **fa zero-touch-client standard wap-type1 i-sid <1-15999999>**

- **fa zero-touch-client standard wap-type2 i-sid <1-15999999>**
- **no fa zero-touch-client standard camera i-sid <1-15999999>**
- **no fa zero-touch-client standard ona-sdn i-sid <1-15999999>**
- **no fa zero-touch-client standard ona-spb-over-ip i-sid <1-15999999>**
- **no fa zero-touch-client standard phone i-sid <1-15999999>**
- **no fa zero-touch-client standard router i-sid <1-15999999>**
- **no fa zero-touch-client standard security-device i-sid <1-15999999>**
- **no fa zero-touch-client standard srvr-endpt i-sid <1-15999999>**
- **no fa zero-touch-client standard switch i-sid <1-15999999>**
- **no fa zero-touch-client standard video i-sid <1-15999999>**
- **no fa zero-touch-client standard virtual-switch i-sid <1-15999999>**
- **no fa zero-touch-client standard wap-type1 i-sid <1-15999999>**
- **no fa zero-touch-client standard wap-type2 i-sid <1-15999999>**

## Command Parameters

### camera

Specifies the client type as IP Camera.

### i-sid <1-15999999>

Specifies the Client I-SID for I-SID/VLAN binding generation.

### ona-sdn

Specifies the client type as ONA (SDN).

### ona-spb-over-ip

Specifies the client type as ONA (SpbOlp).

### phone

Specifies the client type as IP Phone.

### router

Specifies the client type as Router.

### security-device

Specifies the client type as Security Device.

### srvr-endpt

Specifies the client type as Server Endpoint.

### standard

Specifies the Standard (pre-defined) client type.

### switch

Specifies the client type as Switch.

### video

Specifies the client type as IP Video.

### virtual-switch

Specifies the client type as Virtual Switch.

#### wap-type1

Specifies the client type as Wireless AP (Type 1).

#### wap-type2

Specifies the client type as Wireless AP (Type 2).

## Default

The default value is enable.

## Command Mode

Global Configuration

## filter acl

Use an access control list (ACL) to specify an ordered list of ACEs, or filter rules.

## Syntax

- **default filter acl <acl-id>**
- **default filter acl <acl-id> enable**
- **default filter acl <acl-id> name**
- **filter acl <acl-id> enable**
- **filter acl <acl-id> name WORD<0-32>**
- **filter acl <acl-id> type <inVlan | inPort | outPort | inVsn>**
- **filter acl <acl-id> type <inVlan | inPort | outPort | inVsn> name WORD<0-32>**
- **filter acl <acl-id> type <inVlan | inPort | outPort | inVsn> pktType ipv6**
- **filter acl <acl-id> type inVsn matchType <both | terminatingNNIOnly | uniOnly>**
- **filter acl <acl-id> type inVsn matchType <both | terminatingNNIOnly | uniOnly> pktType ipv6**
- **no filter acl <acl-id>**
- **no filter acl <acl-id> enable**

## Command Parameters

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

**matchType <both | terminatingNNIOnly | uniOnly>**

For inVsn ACL types, specifies the type of port to associate with the ACL.

The default value is <both>.

**name WORD<0-32>**

Specifies an optional descriptive name for the ACL.

**pktType ipv6**

Specifies the packet type as IPv6.

**type <inVlan|inPort|outPort|inVsn>**

Specifies the access control list (ACL) type. The values inVlan, inPort, and inVsn are ingress ACLs, and outPort is an egress ACL.

## Default

None

## Command Mode

Global Configuration

## filter acl ace

---

Use an access control entry (ACE) to define a packet pattern and the desired behavior for packets that carry the pattern.

## Syntax

- **default filter acl ace <acl-id> <ace-id>**
- **default filter acl ace <acl-id> <ace-id> enable**
- **default filter acl ace <acl-id> <ace-id> name**
- **filter acl ace <acl-id> <ace-id>**
- **filter acl ace <acl-id> <ace-id> enable**
- **filter acl ace <acl-id> <ace-id> name WORD<1-32>**
- **no filter acl ace <acl-id> <ace-id>**
- **no filter acl ace <acl-id> <ace-id> enable**

## Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

**enable**

Enables an access control entry (ACE) within an access control list (ACL). After you enable an ACE, to make changes, first disable it.

#### name WORD<1-32>

Specifies an optional descriptive name for the access control entry (ACE) that uses 1-32 characters.

## Default

None

## Command Mode

Global Configuration

## filter acl ace action

Configure the access control entry (ACE) action mode as deny or permit.

## Syntax

- **default filter acl ace action <acl-id> <ace-id> { permit | deny } internal-qos**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt count**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt count redirect-next-hop**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt redirect-next-hop**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt redirect-next-hop unreachable**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-ports**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } redirect-next-hop**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } remark-dot1p**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } remark-dscp**
- **default filter acl ace action <acl-id> <ace-id> { permit | deny } count**
- **filter acl ace action <acl-id> <ace-id> { permit | deny }**



- `filter acl ace action <acl-id> <ace-id> { permit | deny } count`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } internal-qos <0-7>`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt <1-512>`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-ports {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } redirect-next-hop WORD<1-45>`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } remark-dot1p <0-7>`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } remark-dscp <0-256 | 0-256>`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } redirect-next-hop WORD<1-45> [count | unreachable | vrf {WORD <1-16>}]`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } redirect-next-hop WORD<1-45> unreachable { permit | deny }`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } redirect-next-hop WORD<1-45> unreachable { permit | deny } count`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } redirect-next-hop WORD<1-45> vrf WORD <1-16> unreachable { permit | deny }`
- `filter acl ace action <acl-id> <ace-id> { permit | deny } redirect-next-hop WORD<1-45> vrf WORD <1-16> unreachable { permit | deny } count`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny }`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } count`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } internal-qos`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt count`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt count [log [redirect-next-hop]]`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt count redirect-next-hop`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt log`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt log redirect-next-hop`
- `no filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-mlt redirect-next-hop`

- **no filter acl ace action <acl-id> <ace-id> { permit | deny } monitor-dst-ports**
- **no filter acl ace action <acl-id> <ace-id> { permit | deny } remark-dscp**
- **no filter acl ace action <acl-id> <ace-id> { permit | deny } redirect-next-hop**
- **no filter acl ace action <acl-id> <ace-id> { permit | deny } remark-dot1p**

## Command Parameters

**<ace-id>**

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

**<acl-id>**

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

**<permit|deny>**

Configures the action mode for security access control entries (ACEs). Each ACE has a mode of permit or deny the matched traffic. You can use filters to configure metering of permitted traffic.



### Note

For each Security ACE, you must define one or more actions as well as the associated action mode (permit or deny). Otherwise, the security ACE cannot be enabled. There is no default configuration for Security ACEs.

With QoS ACEs, the action mode is not configurable. QoS ACEs are always set to action mode permit.

**count**

Enables the ability to count matching packets. Use this parameter with either a security or QoS access control entry (ACE). The default is disabled.

**internal-qos**

Configures the Quality of Service (QoS) level. The default value is 1.

**monitor-dst-mlt <1-512>**

Configures mirroring to a destination MLT group. This action is a security action.

**monitor-dst-ports {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Configures mirroring to a destination port or ports. This action is a security action.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**redirect-next-hop WORD<1-15>**

Specifies the next-hop IP address for redirect mode (a.b.c.d). This action is a security action.

**vrf WORD<1-16>**

Applies a VRF name to the redirect next hop IP address.

**remark-dot1p <0-7>**

Specifies the new 802.1 priority bit for matching packets: zero, one, two, three, four, five, six, or seven. This action is a QoS action.

**remark-dscp <0-63>**

Specifies the new Per-Hop Behavior (PHB) for matching packets:

- phbcs0
- phbcs1
- phbaf11
- phbaf12
- phbaf13
- phbcs2
- phbaf21
- phbaf22
- phbaf23
- phbcs3
- phbaf31
- phbaf32
- phbaf33
- phbcs4
- phbaf41
- phbaf42
- phbaf43
- phbcs5
- phbef
- phbcs6
- phbcs7

This action is a QoS action.

## Default

The default to configure ACE actions to meter flows after a packet matches an ACE is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Policy Based Routing (Redirect Next Hop) per VRF is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are

for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## filter acl ace arp

---

Use access control entry (ACE) ARP entries so that the filter looks for ARP requests or responses.

### Syntax

- **default filter acl ace arp <acl-id> <ace-id>**
- **filter acl ace arp <acl-id> <ace-id> operation eq arprequest**
- **filter acl ace arp <acl-id> <ace-id> operation eq arpreponse**
- **no filter acl ace arp <acl-id> <ace-id>**
- **no filter acl ace arp <acl-id> <ace-id> operation**

### Command Parameters

<ace-id>

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

<acl-id>

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

**operation eq <arprequest|arpreponse>**

Specifies an ARP operation type of arpRequest or arpResponse. For ARP, only one operator and attribute exist (eq and operation).

### Default

None

### Command Mode

Global Configuration

## filter acl ace ethernet

---

Use Ethernet access control entries (ACEs) to filter on Ethernet parameters.

### Syntax

- **default filter acl ace ethernet <acl-id> <ace-id>**
- **filter acl ace ethernet <acl-id> <ace-id> dst-mac eq WORD<1-1024>**
- **filter acl ace ethernet <acl-id> <ace-id> dst-mac mask WORD<1-1024> WORD<1-1024>**

- **filter acl ace ethernet <acl-id> <ace-id> ether-type eq WORD<1-200>**
- **filter acl ace ethernet <acl-id> <ace-id> port eq {slot/port[/sub-port]}**
- **filter acl ace ethernet <acl-id> <ace-id> src-mac eq WORD<1-1024>**
- **filter acl ace ethernet <acl-id> <ace-id> src-mac mask WORD<1-1024> WORD<1-1024>**
- **filter acl ace ethernet <acl-id> <ace-id> vlan-id eq <1-4059>**
- **filter acl ace ethernet <acl-id> <ace-id> vlan-id mask <1-4059> <0-0xFFF | 0x0-0x0>**
- **filter acl ace ethernet <acl-id> <ace-id> vlan-tag-prio eq <0-7>**
- **filter acl ace ethernet <acl-id> <ace-id> vlan-tag-prio mask <0-7> <0-0x7 | 0x0-0x0>**
- **no filter acl ace ethernet <acl-id> <ace-id>**
- **no filter acl ace ethernet <acl-id> <ace-id> dst-mac**
- **no filter acl ace ethernet <acl-id> <ace-id> ether-type**
- **no filter acl ace ethernet <acl-id> <ace-id> port**
- **no filter acl ace ethernet <acl-id> <ace-id> src-mac**
- **no filter acl ace ethernet <acl-id> <ace-id> vlan-id**
- **no filter acl ace ethernet <acl-id> <ace-id> vlan-tag-prio**

## Command Parameters

**<ace-id>**

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

**<acl-id>**

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

**dst-mac <eq|mask> WORD<1-1024>**

The <eq|mask> parameter specifies an operator for a field match condition.

The WORD<1-1024> parameter specifies a list of destination MAC addresses separated by a comma or a range of MAC addresses specified from low to high; for example, [AA:BB:CC:DD:EE:FF].

**ether-type <eq> WORD<1-200>**

The <eq> parameter specifies an operator for a field match condition: equal to. The WORD<1-200> parameter specifies an ether-type name:

- ip
- arp
- ipx802dot3
- ipx802dot2
- ipxSnap

- ipxEthernet2
- appleTalk
- AppleTalk-Arp
- sna802dot2
- snaEthernet2
- netBios
- xns
- vines
- rarp
- PPPoE-discovery
- PPPoE-session

**port eq** {*slot/port* [/sub-port]}

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**src-mac** <eq|mask> WORD<1-1024>

The <eq|mask> parameter specifies an operator for a field match condition: equal to.

The WORD<1-1024> parameter specifies a list of source MAC addresses separated by separated by a comma, or a range of MAC addresses specified from low to high; for example, [AA:BB:CC:DD:EE:FF].

**vlan-id** <eq|mask> <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vlan-tag-prio** <eq|mask> <0-7>

The <eq|mask> parameter specifies an operator for a field match condition. The <0-7> parameter specifies a VLAN tag priority from 0-7 or undefined.

## Default

None

## Command Mode

Global Configuration

## filter acl ace ip

Use IP access control entries (ACEs) to filter on the source IP address, destination IP address, DiffServ Code Point (DSCP), protocol, IP options, IP fragmentation parameters, and routed packets.

## Syntax

- `default filter acl ace ip <acl-id> <ace-id>`
- `filter acl ace ip <acl-id> <ace-id> dscp eq <0-63 | 0-63>`
- `filter acl ace ip <acl-id> <ace-id> dst-ip eq {A.B.C.D}`
- `filter acl ace ip <acl-id> <ace-id> dst-ip mask {A.B.C.D} <0-32>`
- `filter acl ace ip <acl-id> <ace-id> dst-ip mask {A.B.C.D} {A.B.C.D}`
- `filter acl ace ip <acl-id> <ace-id> dst-ip range {A.B.C.D} {A.B.C.D}`
- `filter acl ace ip <acl-id> <ace-id> ip-frag-flag eq { noFragment | anyFragment }`
- `filter acl ace ip <acl-id> <ace-id> ip-options any`
- `filter acl ace ip <acl-id> <ace-id> ip-protocol-type eq WORD<1-256>`
- `filter acl ace ip <acl-id> <ace-id> src-ip eq {A.B.C.D}`
- `filter acl ace ip <acl-id> <ace-id> src-ip mask {A.B.C.D} <0-32>`
- `filter acl ace ip <acl-id> <ace-id> src-ip mask {A.B.C.D} {A.B.C.D}`
- `filter acl ace ip <acl-id> <ace-id> dscp mask <0-63 | 0-63> <0-0x40 | 0x0-0x0>`
- `filter acl ace ip <acl-id> <ace-id> dst-ip eq WORD <1-1024>`
- `filter acl ace ip <acl-id> <ace-id> routed-only`
- `no filter acl ace ip <acl-id> <ace-id> dscp`
- `no filter acl ace ip <acl-id> <ace-id> dst-ip`
- `no filter acl ace ip <acl-id> <ace-id> ip-frag-flag`
- `no filter acl ace ip <acl-id> <ace-id> ip-options`
- `no filter acl ace ip <acl-id> <ace-id> ip-protocol-type`
- `no filter acl ace ip <acl-id> <ace-id> src-ip`
- `no filter acl ace ip <acl-id> <ace-id> routed-only`
- `no filter acl ace ip <acl-id> <ace-id>`

## Command Parameters

`<ace-id>`

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

`<acl-id>`

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

`dscp <eq|mask> WORD <0-256>`

The `<eq|mask>` parameter specifies an operator for a field match condition. The equals to parameter specifies the PHB name or DSCP value {0 to 256, where 256 => disable}, or:

- `phbc0`
- `phbc1`

- phbaf11
- phbaf12
- phbaf13
- phbcs2
- phbaf21
- phbaf22
- phbaf23
- phbcs3
- phbaf31
- phbaf32
- phbaf33
- phbcs4
- phbaf41
- phbaf42
- phbaf43
- phbcs5
- phbcs6
- phbef
- phbcs7

**dst-ip <eq|mask> WORD <1-1024>**

The <eq|mask> parameter specifies an operator for a field match condition.

The WORD<1-1024> parameter specifies the destination IP address list in one of the following formats:

- a.b.c.d
- [w.x.y.z-p.q.r.s]
- [l.m.n.o/mask]
- [a.b.c.d/len]

**ip-frag-flag eq <noFragment|anyFragment>**

The eq parameter specifies an operator for a field match condition: equal to.

The ip-frag-flag parameter specifies a match option for IP fragments: noFragment or anyFragment.

**ip-options any**

Matches to an IP option. Any is the only option.

**ip-protocol-type <eq> WORD <1-256>**

The <eq> parameter specifies an operator for a field match condition: equal to.

The WORD<1-256> parameter specifies one or more IP protocol types:

- (1-256)
- icmp
- tcp
- udp



- ipsecesp
- ipsecah
- ospf
- vrrp
- undefined

#### src-ip <eq|mask> WORD <1-1024>

The <eq|mask> parameter specifies an operator for a field match condition: equal to, not equal to, less than or equal to, greater than or equal to.

The WORD<1-1024> parameter specifies a source IP address list in one of the following formats:

- a.b.c.d
- [w.x.y.z-p.q.r.s]
- [l.m.n.o/mask]
- [a.b.c.d/len]

#### routed-only

Specifies a field match condition for IPv4 routed packets only. The default is disabled.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

The **routed-only** parameter is not supported on VSP 8600 Series or XA1400 Series.

The **routed-only** parameter is not supported for Multicast packets.

## filter acl ace ipv6

Use access control entry (ACE) IPv6 entries to filter on IPv6 parameters.

## Syntax

- **filter acl ace ipv6 <acl-id> <ace-id> dst-ipv6 {eq | mask} WORD<0-255> [WORD<0-255>]**
- **filter acl ace ipv6 <acl-id> <ace-id> nxt-hdr eq {fragment | hop-by-hop | icmpv6 | ipsecah | ipsecesp | noHdr | routing | tcp | udp | undefined}**
- **filter acl ace ipv6 <acl-id> <ace-id> src-ipv6 {eq | mask} WORD<0-255> [WORD<0-255>]**
- **filter acl ace ipv6 <acl-id> <ace-id> traffic-class eq <0-255>**

- **filter acl ace ipv6 <acl-id> <ace-id> routed-only**
- **no filter acl ace ipv6 <acl-id> <ace-id>**
- **no filter acl ace ipv6 <acl-id> <ace-id> dst-ipv6**
- **no filter acl ace ipv6 <acl-id> <ace-id> nxt-hdr**
- **no filter acl ace ipv6 <acl-id> <ace-id> src-ipv6**
- **no filter acl ace ipv6 <acl-id> <ace-id> traffic-class**
- **no filter acl ace ipv6 <acl-id> <ace-id> routed-only**

## Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

**dst-ipv6 {eq | mask} WORD<0-255>**

The *<eq|mask>* parameter specifies an operator for a field match condition.

The *WORD<0-255>* parameter specifies a list of destination IPv6 addresses separated by a comma, or a range of IPv6 addresses specified from low to high; for example, [AA:BB:CC:DD:EE:FF].

**nxt-hdr eq <fragment | hop-by-hop | icmpv6 | ipsecah | ipsecesp | noHdr | routing | tcp | udp | undefined>**

Specify next header of IP header.

**src-ipv6 {eq | mask} WORD<0-255>**

The *<eq|mask>* parameter specifies an operator for a field match condition: equal to.

The *WORD<0-255>* parameter specifies a list of source IPv6 addresses separated by a comma, or a range of IPv6 addresses specified from low to high; for example, [AA:BB:CC:DD:EE:FF].

**traffic-class eq <0-255>**

Specify traffic class attribute of IPv6 header.

**routed-only**

Specifies a field match condition for IPv6 routed packets only. The default is disabled.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

The **routed-only** parameter is not supported on VSP 8600 Series or XA1400 Series.

## filter acl ace policer

---

Use the policer filter to limit the service and peak rate traffic at the ingress.

## Syntax

- **default filter acl ace policer <acl-id> <ace-id>**
- **filter acl ace policer <acl-id> <ace-id> svc-rate <0-4000000000> peak-rate <8-4000000000>**
- **no filter acl ace policer <acl-id> <ace-id>**

## Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

### **policer**

Specifies the policer parameters for an ACE.

**svc-rate <0-4000000000>**

Specifies the rate of transfer of traffic which has to be delivered.

**peak-rate <8-4000000000>**

Specifies the maximum rate of transfer of traffic above which the packets are dropped at ingress.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## filter acl ace protocol

Use protocol access control entries (ACEs) to filter on the TCP source port, UDP source port, TCP destination port, UDP destination port, ICMP message type, and TCP flags.

### Syntax

- **default filter acl ace protocol <acl-id> <ace-id>**
- **filter acl ace protocol <acl-id> <ace-id> dst-port eq WORD<1-60>**
- **filter acl ace protocol <acl-id> <ace-id> dst-port mask WORD<1-60> <0x0-0xFFFF>**
- **filter acl ace protocol <acl-id> <ace-id> icmp-msg-type eq WORD<1-200>**
- **filter acl ace protocol <acl-id> <ace-id> icmpv6-msg-type eq WORD<1-200>**
- **filter acl ace protocol <acl-id> <ace-id> src-port eq <0-65535>**
- **filter acl ace protocol <acl-id> <ace-id> tcp-flags eq WORD<1-50>**
- **filter acl ace protocol <acl-id> <ace-id> tcp-flags mask WORD<1-50> <0-0x3F | 0x0-0x0>**
- **filter acl ace protocol <acl-id> <ace-id> routing-type eq <0-2>**
- **filter acl ace protocol <acl-id> <ace-id> src-port mask <0-65535> <0x0-0xFFFF>**
- **no filter acl ace protocol <acl-id> <ace-id>**
- **no filter acl ace protocol <acl-id> <ace-id> dst-port**
- **no filter acl ace protocol <acl-id> <ace-id> icmp-msg-type**
- **no filter acl ace protocol <acl-id> <ace-id> src-port**
- **no filter acl ace protocol <acl-id> <ace-id> tcp-flags**
- **no filter acl ace protocol <acl-id> <ace-id> routing-type**

### Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

**dst-port <eq|mask> WORD<1-60>**

The <eq|mask> parameter specifies an operator for a field match condition: equal to.

The WORD<1-60> parameter specifies the destination port for the TCP protocol: (0-65535), or {echo| ftpdata| ftpcontrol| ssh| telnet| dns| http|bgp| hdot323| bootpServer| boorpClient| tftp| rip| rtp| rctp| undefined}.

**icmp-msg-type <eq> WORD <1-200>**

Specifies the Internet Control Message Protocol (ICMP) message type attribute of the protocol.

The <eq> parameter specifies an operator for a field match condition: equal to.

The WORD<1-200> parameter specifies one or more IP protocol types (0-255), or {echoreply| destunreach| sourcequench| redirect| echo-request| routeradv|routerselect| time-exceeded| param-problem| timestamp-request|timestamp-reply| addressmask-request| addressmask-reply| traceroute}.

#### **icmpv6-msg-type <eq> WORD <1-200>**

Specifies the ICMPv6 message type attribute of the protocol.

The <eq> parameter specifies an operator for a field match condition: equal to.

The WORD<1-200> parameter specifies one or more Icmpmsg type {0-255} or {destUnreach | pktTooBig | timeExceeded | paramProblem | echoRequest | echoReply | mcastListenReq | mcastListenRpt | mcastListenDone | routerSolicit | routerAdvert | neighborSolicit | neighborAdvert | redirectMsg | nodeInfoReq | nodeInfoRsp | v2McastListenRpt}.

#### **routing-type eq <0-2>**

This parameter represents the routing type attribute.

#### **src-port <eq|mask> WORD<1-65535>**

The <eq|mask> parameter specifies an operator for a field match condition.

The WORD <1-65535> parameter specifies the destination port for the TCP protocol {0-65535}.

#### **tcp-flags <eq|mask> WORD<1-50>**

Specifies TCP-flags attribute of the protocol.

The <eq|mask> parameter specifies an operator for a field match condition.

The WORD <1-50> parameter specifies one or more TCP flags: {none| fin| syn| rst| push| ack| urg| undefined}. The tcp-flags and icmp-msg-type command options support lists.

## Default

None

## Command Mode

Global Configuration

## filter acl i-sid

---

For inVsn ACL filters, specify the I-SID associated with the customer VLAN (Layer 2 VSN) or the customer VRF (Layer 3 VSN).

## Syntax

- **filter acl i-sid <acl-id> <0-15999999>**

## Command Parameters

<0-15999999>

Specifies the I-SID associated with the customer VLAN (Layer 2 VSN), the customer VRF (Layer 3 VSN), or the IP Shortcut. The I-SID must already be configured on the fabric node.

<acl-id>

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information, see [VOSS User Guide](#).

## filter acl port

---

Associate ports with, or remove ports from, an ACL so that filters do or do not apply to port traffic, respectively.

## Syntax

- **default filter acl port** <acl-id> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **filter acl port** <acl-id> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **no filter acl port** <acl-id> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<acl-id>

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Global Configuration

## filter acl set

Configure an access control list (ACL) filter.

## Syntax

- `default filter acl set <acl-id> default-action`
- `default filter acl set <acl-id> global-action`
- `default filter acl set <acl-id> global-action monitor-dst-mlt`
- `default filter acl set <acl-id> global-action monitor-dst-ports`
- `filter acl set <acl-id> default-action deny`
- `filter acl set <acl-id> default-action deny control-packet-action deny`
- `filter acl set <acl-id> default-action deny control-packet-action permit`
- `filter acl set <acl-id> default-action permit`
- `filter acl set <acl-id> default-action permit policer svc-rate <0-4000000000> peak-rate <8-4000000000>`
- `filter acl set <acl-id> global-action monitor-dst-mlt <1-512>`
- `filter acl set <acl-id> global-action monitor-dst-ports{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `no filter acl set <acl-id> global-action monitor-dst-mlt`
- `no filter acl set <acl-id> global-action monitor-dst-ports`
- `no filter acl set <acl-id> policer`

## Command Parameters

`{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

`<acl-id>`

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

`default-action <permit|deny>`

Specifies the action to be taken when none of the access control entries (ACEs) match. The options are deny or permit.



#### Note

To configure the ACL default policer, you must specify the permit option.

#### policer

Specifies the default action to be taken to permit or deny the policer. By attaching a policer to an ACL ACE entry, you can limit the bandwidth of an ingress flow for that ACE.

#### svc-rate <0-4000000000>

Specifies the rate of transfer of traffic which has to be delivered.

#### peak-rate <8-4000000000>

Specifies the maximum rate of transfer of traffic above which the packets are dropped at ingress.

#### global-action {monitor-dst-mlt<1-512>|monitor-dst-ports}

Specifies the action to be taken for all access control entry (ACE) matches. The options are:  
monitor-dst-mlt <1-512>|

monitor-dst-ports {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}.

## Default

The default action is deny.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## filter acl vlan

Associate VLANs with, or remove VLANs from, an access control list (ACL) so that filters do or do not apply to VLAN traffic, respectively.

## Syntax

- **default filter acl vlan <acl-id> <1-4059>**
- **filter acl vlan <acl-id> <1-4059>**
- **no filter acl vlan <acl-id> <1-4059>**

## Command Parameters

<1-4059>



Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

<acl-id>

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Global Configuration

## ike policy WORD<1-32> auth-method

---

Specifies the authentication method.

## Syntax

- **default ike policy WORD<1-32> < auth-method | revocation-check-method>**
- **ike policy WORD<1-32> auth-method digital-certificate peer-name WORD <1-64>**
- **ike policy WORD<1-32> auth-method digital-certificate revocation-check-method <cr1 | none | ocsp>**
- **ike policy WORD<1-32> auth-method pre-shared-key**
- **no ike policy WORD<1-32> [auth-method]**

## Command Parameters

### digital-certificate

Configures the authentication method as digital-certificate.

### peer-name WORD <1-64>

Specifies peer identity name for IKE phase 1.

### pre-shared-key

Configures the authentication method to use a pre-shared-key.

### revocation-method <cr1|none|ocsp>

Specifies the revocation check method.

### WORD<1-32>

Specifies the name of the IKE Phase 1 policy.

## Default

The default is pre-shared key.

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Secure AAA server communication is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## ike policy WORD<1-32> dpd-timeout

---

Configure the Dead-Peer Detection timeout in seconds for the IKE Phase 1 policy.

## Syntax

- **default ike policy WORD<1-32> dpd-timeout**
- **ike policy WORD<1-32> dpd-timeout <0-4294967295>**

## Command Parameters

<0-4294967295>

Configure the Dead-Peer Detection timeout in seconds.

WORD<1-32>

Specifies the name of the IKE Phase 1 policy.

## Default

The default is 300 seconds.

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Secure AAA server communication is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

---

## ike policy WORD<1-32> enable

---

Enables the admin state of IKE Phase 1 policy.

### Syntax

- **default ike policy WORD<1-32> enable**
- **ike policy WORD<1-32> enable**
- **no ike policy WORD<1-32> [enable]**

### Command Parameters

**WORD<1-32>**

Specifies the name of the IKE Phase 1 policy.

### Default

None

### Command Mode

Global Configuration

### Usage Guidelines

DEMO FEATURE - Secure AAA server communication is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

---

## ike policy WORD<1-32> laddr

---

Use this command to specify the local and remote IP address.

### Syntax

- **ike policy WORD<1-32> laddr WORD<1-256> raddr WORD<1-256>**

### Command Parameters

**laddr WORD<1-256>**

Specifies the local IPv4 or IPv6 address.

**raddr WORD<1-256>**

Specifies the remote IPv4 or IPv6 address.

**WORD<1-32>**

Specifies the name of the IKE Phase 1 policy.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Secure AAA server communication is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## ike policy WORD<1-32> p2-pfs

---

Enables the Phase 2 perfect forward secrecy.

## Syntax

- **default ike policy WORD<1-32> p2-pfs [dh-group] [use-ike-group]**
- **ike policy WORD<1-32> p2-pfs <disable | enable> [dh-group <modp768 | modp1024 | modp2048 | any>] [use-ike-group <disable | enable>]**
- **no ike policy WORD<1-32> [p2-pfs]**

## Command Parameters

**dh-group <modp768|modp1024|modp2048|any>**

Configures the Diffie-Hellman (DH) group to be used for Phase 2 perfect forward secrecy (PFS). The default value is modp2048.

**use-ike-group <enable|disable>**

Specifies whether to use the IKE Phase 1 DH group for Phase 2 PFS. The default is enable.

**WORD<1-32>**

Specifies the name of the IKE Phase 1 policy.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Secure AAA server communication is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## ike policy WORD<1-32> pre-shared-key

---

Configures the pre-shared-key.

### Syntax

- **ike policy WORD<1-32> pre-shared-key WORD<0-32>**

### Command Parameters

#### WORD<0-32>

Configures the pre-shared-key. For Federal Information Processing Standards (FIPS) compliance, the minimum length is 14 characters.

#### WORD<1-32>

Specifies the name of the IKE Phase 1 policy.

### Default

None

### Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Secure AAA server communication is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## ike profile

---

Use this command to configure an IKE Phase 1 profile.

### Syntax

- **default ike profile WORD<1-32> [dh-group] [encrypt-algo] [encrypt-key-len] [hash-algo] [lifetime-sec]**
- **ike profile WORD<1-32>**

- `ike profile WORD<1-32> dh-group <modp768 | modp1024 | modp2048 | any>`
- `ike profile WORD<1-32> encrypt-algo <desCbc | 3DesCbc | aesCbc | any>`
- `ike profile WORD<1-32> encrypt-key-len <128 | 192 | 256>`
- `ike profile WORD<1-32> hash-algo <MD5 | SHA | SHA256 | any>`
- `ike profile WORD<1-32> lifetime-sec <0-4294967295>`
- `no ike profile WORD<1-32>`

## Command Parameters

`dh-group <modp768|modp1024|modp2048|any>`

Specifies the Diffie-Hellman (DH) group. DH groups categorize the key used in the key exchange process, by its strength. The key from a higher group number is more secure. The default value is modp2048.

`encrypt-algo <desCbc|3DesCbc|aesCbc|any>`

Specifies the type of encryption algorithm. The default value is aesCbc.

`encrypt-key-len <128|192|256>`

Specifies the length of the encryption key. The default is 256.

`hash-algo <md5|sha|sha256|any>`

Specifies the type of hash algorithm. The default value is sha256.

`lifetime-sec <0-4294967295>`

Specifies the lifetime value in seconds. The lifetime ensures that the peers renegotiate the SAs just before the expiry of the lifetime value, to ensure that Security Associations are not compromised. The default value is 86400 seconds.

`WORD<1-32>`

Specifies the IKE profile name.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Secure AAA server communication is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## ike v2-profile

Use this command to configure an IKE Phase 2 profile.

## Syntax

- `default ike v2-profile WORD<1-32> dh-group`
- `default ike v2-profile WORD<1-32> encrypt-algo`
- `default ike v2-profile WORD<1-32> encrypt-key-len`
- `default ike v2-profile WORD<1-32> hash-algo`
- `default ike v2-profile WORD<1-32> integrity-algo`
- `default ike v2-profile WORD<1-32> lifetime-sec`
- `ike v2-profile WORD<1-32>`
- `ike v2-profile WORD<1-32> dh-group <any>`
- `ike v2-profile WORD<1-32> dh-group <modp1024>`
- `ike v2-profile WORD<1-32> dh-group <modp2048>`
- `ike v2-profile WORD<1-32> dh-group <modp768>`
- `ike v2-profile WORD<1-32> encrypt-algo <3DesCbc>`
- `ike v2-profile WORD<1-32> encrypt-algo <aesCbc>`
- `ike v2-profile WORD<1-32> encrypt-algo <any>`
- `ike v2-profile WORD<1-32> encrypt-algo <desCbc>`
- `ike v2-profile WORD<1-32> encrypt-key-len <128|192|256>`
- `ike v2-profile WORD<1-32> hash-algo <any>`
- `ike v2-profile WORD<1-32> hash-algo <md5>`
- `ike v2-profile WORD<1-32> hash-algo <sha>`
- `ike v2-profile WORD<1-32> hash-algo <sha256>`
- `ike v2-profile WORD<1-32> integrity-algo <aes-xcbc>`
- `ike v2-profile WORD<1-32> integrity-algo <any>`
- `ike v2-profile WORD<1-32> integrity-algo <hmac-md5>`
- `ike v2-profile WORD<1-32> integrity-algo <hmac-sha>`
- `ike v2-profile WORD<1-32> integrity-algo <hmac-sha256>`
- `ike v2-profile WORD<1-32> lifetime-sec <0-4294967295>`
- `no ike v2-profile WORD<1-32>`

## Command Parameters

`dh-group <modp768|modp1024|modp2048|any>`

Specifies the Diffie-Hellman (DH) group. DH groups categorize the key used in the key exchange process, by its strength. The key from a higher group number is more secure. The default value is modp2048.

`encrypt-algo <desCbc|3DesCbc|aesCbc|any>`

Specifies the type of encryption algorithm. The default value is aesCbc.

`encrypt-key-len <128|192|256>`

Specifies the length of the encryption key. The default is 256.

**hash-algo <md5|sha|sha256|any>**

Specifies the type of hash algorithm. The default value is sha256.

**integrity-algo <hmac-md5|hmac-sha|hmacsha256|aes-xcbc|any>**

Specifies the type of integrity algorithm. The default is sha256.

**lifetime-sec <0-4294967295>**

Specifies the lifetime value in seconds. The lifetime ensures that the peers renegotiate the SAs just before the expiry of the lifetime value, to ensure that Security Associations are not compromised. The default value is 86400 seconds.

**WORD<1-32>**

Specifies the IKE v2-profile name.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Secure AAA server communication is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## interface GigabitEthernet

---

Use this command to enter Interface Configuration mode for a GigabitEthernet slot and port.

## Syntax

- interface GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



## Default

None

## Command Mode

Global Configuration

## interface Loopback

---

Use this command to enter Interface Configuration mode for a loopback interface.

## Syntax

- **interface Loopback <1-256>**

## Command Parameters

<1-256>

Specifies the loopback ID.

## Default

None

## Command Mode

Global Configuration

## interface mgmtEthernet

---

Use this command to enter Interface Configuration mode for a management interface. This mode only applies to hardware with a dedicated, physical management interface.

## Syntax

- **interface mgmtEthernet mgmt**

## Default

None

## Command Mode

Global Configuration

---

## interface mlt

---

Use this command to enter Interface Configuration mode for an MLT.

### Syntax

- **interface mlt <1-512>**

### Command Parameters

<1-512>

Specifies the MLT ID.

### Default

None

### Command Mode

Global Configuration

---

## interface vlan

---

Use this command to enter Interface Configuration mode for a VLAN.

### Syntax

- **interface Vlan <1-4059>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

Global Configuration

## ip alternative-route (globally)

---

Enable the alternative route feature globally.

### Syntax

- **default ip alternative-route**
- **ip alternative-route**
- **no ip alternative-route**

### Command Parameters

#### alternative-route

Enables or disables the Alternative Route feature. The default value is enabled.

If the alternative-route parameter is disabled, all existing alternative routes are removed. When the parameter is enabled, all alternative routes are re-added.

### Default

The default is enabled.

### Command Mode

Global Configuration

## ip arp

---

Configure ARP static entries to modify the ARP parameters on the device. The only way to change a static ARP is to delete the static ARP entry and create a new entry with new information.

### Syntax

- **default ip arp {A.B.C.D}**
- **default ip arp request-threshold**
- **default ip arp timeout**
- **ip arp {A.B.C.D} 0x00:0x00:0x00:0x00:0x00:0x00 {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} vid <1-4059>**
- **ip arp {A.B.C.D} 0x00:0x00:0x00:0x00:0x00:0x00 {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **ip arp request-threshold <50-1000>**
- **ip arp timeout <1-32767>**
- **no ip arp {A.B.C.D}**

## Command Parameters

**{A.B.C.D}**

Specifies the IP address.

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC address in hexadecimal format. The MAC address parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive).

**timeout <1-32767>**

Configures the timeout value.

**vid <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Global Configuration

## ip arp multicast-mac-flooding

---

Determine whether ARP entries for multicast MAC addresses are associated with the VLAN or the port interface on which they were learned. Links the ARP entry for the Network Load Balancer (NLB) cluster to the multicast group ID (MGID) of the VLAN.

## Syntax

- **default ip arp multicast-mac-flooding**
- **default ip arp multicast-mac-flooding enable**
- **ip arp multicast-mac-flooding**
- **ip arp multicast-mac-flooding enable**
- **no ip arp multicast-mac-flooding**
- **no ip arp multicast-mac-flooding enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

## ip arp static-mcast

---

Configure Layer 3 multicast MAC filtering to route an IP frame to a unicast IP address and flood it with a destination multicast MAC address. You must manually define a static ARP entry that associates an IP address with a multicast MAC address, flooding ports, and a multilink trunk.

## Syntax

- **default ip arp static-mcast {A.B.C.D}**
- **ip arp static-mcast {A.B.C.D} <0x00:0x00:0x00:0x00:0x00:0x00> vid <1-4059> [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] [WORD<1-16>]**
- **no ip arp static-mcast {A.B.C.D}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Specifies the port that receives the multicast flooding.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**<0x00:0x00:0x00:0x00:0x00:0x00>**

Specifies the MAC address in hexadecimal format. The MAC address parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive).

**A.B.C.D**

Specifies the IP address.

**vid <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**WORD<1-16>**

Specifies the multilink trunk ID.

## Default

None

## Command Mode

Global Configuration

## ip as-list

---

Use an asynchronous (AS) path list to restrict the routing information a router learns or advertises to and from a neighbor. The AS path list acts as a filter that Match AS paths.

## Syntax

- **ip as-list** <1-1024> **memberId** <0-65535> <permit|deny> **as-path** WORD<0-1536>

## Command Parameters

<permit|deny>

Permits or denies access for matching conditions.

as-list <1-1024>

Creates the specified AS-path list entry.

as-path WORD <0-1536>

Specifies an integer value between 0 and 1536 placed within quotation marks ""

memberId <0-65535>

Adds a regular expression entry to the specified AS-path list. It is an integer value between 0 and 65 535.

## Default

None

## Command Mode

Global Configuration

## ip community-list

---

Use community lists to specify permitted routes by using their BGP community. This list acts as a filter that Match communities or AS numbers

## Syntax

- **ip community-list** <1-1024> **memberId** <0-65535> <permit|deny> **community-string** WORD<0-256>
- **no ip community-list** <1-1024>
- **no ip community-list** <1-1024> **community-string** WORD<0-256>
- **no ip community-list** <1-1024> **memberid** <0-65535>

## Command Parameters

**<permit|deny>**

Sets the access mode, which permits or denies access for matching conditions.

**community-list** <1-1024>

Creates the specified community list entry. <1-1024> specifies the list id.

**community-string** WORD<0-256>

Specifies an alphanumeric string value with a string length of 0 to 1536 characters. This string value is either an AS num: community-value or a well-known community string. Well known communities include: internet no-export no-advertise local-as (known as NO\_EXPORT\_SUBCONFED).

**memberId** <0-65535>

Adds an entry to the community list. <0-65535> is an integer value that represents the member ID in the community list.

## Default

None

## Command Mode

Global Configuration

## ip dhcp-relay fwd-path

---

Create the forwarding path from the client to the server.

## Syntax

- **default ip dhcp-relay fwd-path** <A.B.C.D> <A.B.C.D>
- **ip dhcp-relay fwd-path** {A.B.C.D} {A.B.C.D}
- **no ip dhcp-relay fwd-path** <A.B.C.D> <A.B.C.D>

## Command Parameters

**fwd-path** <A.B.C.D> <A.B.C.D>

Configures the forwarding path from the client to the server. A.B.C.D is the IP address configured on an interface (a locally configured IP address) to forward or relay BootP or Dynamic Host Configuration Protocol (DHCP). The relay can also be a VRRP address.

A.B.C.D is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out from the interface.

## Default

None

## Command Mode

Global Configuration

## ip dhcp-relay fwd-path enable

---

Enable the forwarding path from the client to the server.

## Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}**
- **ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} disable**
- **ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} enable**
- **no ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} enable**

## Command Parameters

**disable**

Disables Dynamic Host Configuration Protocol (DHCP) relaying on the path from the IP address to the server.

**fwd-path <A.B.C.D> <A.B.C.D> enable**

Enables Dynamic Host Configuration Protocol (DHCP) relaying on the path from the IP address to the server.

The first <A.B.C.D> variable is the agent IP address configured on an interface (a locally configured IP address).

The second <A.B.C.D> variable is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out from the interface.

## Default

The ip dhcp-relay fwd-path default state is disabled.



## Command Mode

Global Configuration

## Usage Guidelines

If the agent IP address (the first `<A.B.C.D>` variable) is a VLAN or port IP address, you must enable DHCP Relay on that VLAN or port by running **ip dhcp-relay** within the VLAN context. However, if the first `<A.B.C.D>` variable is a VRRP address, you do not need to enable DHCP Relay on the VLAN or port in which the VRRP address resides.

## ip dhcp-relay fwd-path mode

---

Modify Dynamic Host Configuration Protocol (DHCP) mode to forward BootP messages only, DHCP messages only, or both.

### Syntax

- **default ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D> mode**
- **ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode bootp**
- **ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode bootp\_dhcp**
- **ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode dhcp**

### Command Parameters

**fwd-path <A.B.C.D> <A.B.C.D> mode <bootp|bootp-dhcp|dhcp>**

Modifies the Dynamic Host Configuration Protocol (DHCP) mode to forward BootP messages only, DHCP messages only, or both. The default is both.

mode is {bootp | bootp\_dhcp | dhcp}.

### Default

The default mode is both.

## Command Mode

Global Configuration

## ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} src-port-67 (globally)

---

Configure a forwarding path with source port 67 in a User Datagram Protocol (UDP) globally.

### Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} src-port-67**
- **ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} src-port-67**

- **no ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} src-port-67**

## Command Parameters

**src-port-67**

Specifies the UDP source port to 67 for BOOTP request. The default is 68.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip dhcp-snooping binding

---

Adds static binding entry to the DHCP binding table.

## Syntax

- **ip dhcp-snooping binding <1-4059> 0x00:0x00:0x00:0x00:0x00:0x00 ip {A.B.C.D} port {slot/port[sub-port]}**
- **ip dhcp-snooping binding <1-4059> 0x00:0x00:0x00:0x00:0x00:0x00 ip {A.B.C.D} port {slot/port[sub-port]} [expiry <0-2147483646>]**
- **no ip dhcp-snooping binding <1-4059> 0x00:0x00:0x00:0x00:0x00:0x00**

## Command Parameters

**<1-4059>**

Specifies the VLAN ID.

**0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC address of the DHCP client.

**expiry <0-2147483646>**

Specifies the expiry time (in seconds) for the DHCP client.

**ip {A.B.C.D}**

Specifies the IP address of the DHCP client.

**port {slot/port[sub-port]}**

Specifies the switch port to which the DHCP client connects.

## Default

None

## Command Mode

Global Configuration

# ip dhcp-snooping enable

---

Enables DHCP Snooping globally.

## Syntax

- **default ip dhcp-snooping enable**
- **ip dhcp-snooping enable**
- **no ip dhcp-snooping enable**

## Default

Disabled

## Command Mode

Global Configuration

# ip domain-name

---

Configure the Domain Name Service (DNS) to establish the mapping between a name and an IP address.

## Syntax

- **default ip domain-name**
- **ip domain-name WORD<0-255>**
- **no ip domain-name**

## Command Parameters

**WORD<0-255>**

Configures the default domain name.

## Default

None

## Command Mode

Global Configuration

## ip ecmp

Enable Equal Cost Multipath protocol (ECMP). If the ECMP parameter is disabled, all existing ECMP routes are removed. When ECMP is enabled, all ECMP routes are re-added.

## Syntax

- `default ip ecmp`
- `default ip ecmp`
- `default ip ecmp max-path`
- `ip ecmp`
- `ip ecmp max-path <ECMP-Paths>`
- `ip ecmp pathlist-1 WORD<0-64>`
- `ip ecmp pathlist-2 WORD<0-64>`
- `ip ecmp pathlist-3 WORD<0-64>`
- `ip ecmp pathlist-4 WORD<0-64>`
- `ip ecmp pathlist-5 WORD<0-64>`
- `ip ecmp pathlist-6 WORD<0-64>`
- `ip ecmp pathlist-7 WORD<0-64>`
- `ip ecmp pathlist-8 WORD<0-64>`
- `no ip ecmp`
- `no ip ecmp pathlist-1`
- `no ip ecmp pathlist-2`
- `no ip ecmp pathlist-3`
- `no ip ecmp pathlist-4`
- `no ip ecmp pathlist-5`
- `no ip ecmp pathlist-6`
- `no ip ecmp pathlist-7`
- `no ip ecmp pathlist-8`

## Command Parameters

`max-path <ECMP-Paths>`

Specifies the maximum number of ECMP paths. Different hardware platforms can support a different number of ECMP paths. For more information on the maximum number of ECMP paths supported on the switch, see the scaling information in [VSP 8600 Release Notes](#).

`pathlist-1 WORD<0-64>`

Configures one equal-cost path to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

**pathlist-2 WORD<0-64>**

Configures up to two equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

**pathlist-3 WORD<0-64>**

Configures up to three equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

**pathlist-4 WORD<0-64>**

Configures up to four equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

**pathlist-5 WORD<0-64>**

Configures up to five equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

**pathlist-6 WORD<0-64>**

Configures up to six equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

**pathlist-7 WORD<0-64>**

Configures up to seven equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

**pathlist-8 WORD<0-64>**

Configures up to eight equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

## Default

The default is disabled.

## Command Mode

Global Configuration

## ip forward-protocol udp

---

Configure UDP protocols to determine which UDP broadcasts are forwarded.

## Syntax

- **default ip forward-protocol udp**
- **default ip forward-protocol udp <1-65535>**
- **ip forward-protocol udp <1-65535> WORD<1-15>**
- **no ip forward-protocol udp <1-65535>**

## Command Parameters

<1-65535> WORD/1-15 <1-15>

Creates a new UDP protocol. <1-65535>WORD <1-15>is the UDP protocol name as a string.

## Default

None

## Command Mode

Global Configuration

---

## ip forward-protocol udp portfwd

Configure a UDP port forward entry to add or remove a port forward entry.

## Syntax

- **default ip forward-protocol udp portfwd <1-65535> {A.B.C.D}**
- **ip forward-protocol udp portfwd <1-65535> {A.B.C.D}**
- **no ip forward-protocol udp portfwd <1-65535> {A.B.C.D}**

## Command Parameters

<1-65535> <A.B.C.D>

Adds a UDP protocol port to the specified port forwarding list.

1-65535 is a UDP protocol port in the range of 1 to 65535.

A.B.C.D is an IP address in a.b.c.d format.

## Default

None

## Command Mode

Global Configuration

## ip forward-protocol udp portfwldlist

---

Configure the UDP port forwarding list.

### Syntax

- **default ip forward-protocol udp portfwldlist <1-1000>**
- **default ip forward-protocol udp portfwldlist <1-1000> <1-65535> {A.B.C.D}**
- **ip forward-protocol udp portfwldlist <1-1000>**
- **ip forward-protocol udp portfwldlist <1-1000> <1-65535> {A.B.C.D}**
- **ip forward-protocol udp portfwldlist <1-1000> name WORD<0-15>**
- **no ip forward-protocol udp portfwldlist <1-1000> <1-65535> {A.B.C.D}**
- **no ip forward-protocol udp portfwldlist <1-1000>**

### Command Parameters

{A.B.C.D}

A.B.C.D is an IP address in a.b.c.d format.

<1-1000>

Creates a UDP port forwarding list in the range of 1 to 1000.

name WORD<0-15>

Specifies a name for the forwarding list.

### Default

None

### Command Mode

Global Configuration

## ip gratuitous-arp

---

Enable Gratuitous Address Resolution Protocol (ARP) on a global level. When Gratuitous ARP is enabled, the switch allows all Gratuitous ARP requests. If you disable Gratuitous ARP, the switch only allows Gratuitous ARP packets associated with Routed Split Multi-Link Trunking (RSMLT) or Virtual Router Redundancy Protocol (VRRP), and the switch discards all other Gratuitous ARP request packets.

### Syntax

- **default ip gratuitous-arp**
- **ip gratuitous-arp**
- **no ip gratuitous-arp**

## Default

The default is enabled.

## Command Mode

Global Configuration

## ip icmp

---

Enable Fragmented ICMP packet filtering, redirect and unreachable messages.

## Syntax

- **default ip icmp**
- **default ip icmp unreachable**
- **default ip icmp drop-fragments**
- **ip icmp unreachable**
- **ip icmp drop-fragments**
- **no ip icmp**
- **no ip icmp unreachable**
- **no ip icmp drop-fragments**

## Command Parameters

### drop-fragments

Enables IPv4 Fragmented ICMP packet filtering. The default is disabled.

### unreachable

Enables the switch to send Internet Control Message Protocol (ICMP) unreachable messages. When enabled, generates Internet Control Message Protocol (ICMP) network unreachable messages if the destination network is not reachable from this router. These messages help determine if the routing switch is reachable over the network. The default is disabled.

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



---

## ip icmp echo-broadcast-request (globally)

---

Enables or disables the processing of IPv4 ICMP messages sent to a broadcast address globally.

### Syntax

- `default ip icmp echo-broadcast-request`
- `ip icmp echo-broadcast-request`
- `no ip icmp echo-broadcast-request`

### Command Parameters

`echo broadcast-request`

Enables or disables the processing of IPv4 ICMP messages sent to a broadcast address globally.  
The default value is enabled.

### Default

The default is enabled.

### Command Mode

Global Configuration

---

## ip igmp (globally)

---

Configure the Internet Group Management Protocol (IGMP) commands to establish and manage the multicast groups.

### Syntax

- `default ip igmp ssm-map {A.B.C.D} {A.B.C.D}`
- `default ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]`
- `ip igmp generate-log`
- `ip igmp generate-trap`
- `ip igmp immediate-leave-mode <multiple-user|one-user>`
- `ip igmp ssm [dynamic-learning] [group-range {A.B.C.D/X}]`
- `ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]`
- `ip igmp ssm-map all`
- `no ip igmp ssm-map {A.B.C.D} {A.B.C.D}`
- `no ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]`
- `ip igmp stream-timeout <10-432000>`
- `default ip igmp stream-timeout`

## Command Parameters

### **generate-log**

Sets the Internet Group Management Protocol (IGMP) log.

### **generate-trap**

Sets the Internet Group Management Protocol (IGMP) trap.

### **immediate-leave-mode <multiple-user|one-user>**

Enables immediate leave mode to users which is either a single user or multiple users.

### **ssm [dynamic-learning] [group-range {A.B.C.D/X}]**

Enables and sets the Source Specific Multicast (SSM) features.

The parameter `dynamic-learning` enables SSM dynamic learning.

The parameter `group-range {A.B.C.D/X}` configures the range group address and mask. The SSM range parameter extends the default SSM range of 232/8 to include an IP multicast address. You can configure existing applications without having to change their group configurations. This parameter specifies an IP multicast address within the range of 224.0.0.0 and 239.255.255.255. The default is 232.0.0.0. The address mask is the IP address mask of the multicast group. The default is 255.0.0.0.

### **ssm-map {A.B.C.D} {A.B.C.D} [enable]**

Enables the Source Specific Multicast (SSM) map table for a specific entry or creates a static entry for a specific group.

The parameter `{A.B.C.D} {A.B.C.D}` creates a static SSM channel table entry by specifying the group and source IP addresses. The first IP address is an IP multicast address within the SSM range. The second IP address is the source IP address and it is an IP host address that sends traffic to the group. The default for `{A.B.C.D}{A.B.C.D} enable` is `enable` for each entry. The default is `enable` for each entry.

### **ssm-map all**

Enables the Source Specific Multicast (SSM) map table for all static entries.

### **ssm-map {A.B.C.D} {A.B.C.D} [enable]**

Enables the Source Specific Multicast (SSM) map table for a specific entry or creates a static entry for a specific group.

The parameter `{A.B.C.D} {A.B.C.D}` creates a static SSM channel table entry by specifying the group and source IP addresses. The first IP address is an IP multicast address within the SSM range. The second IP address is the source IP address and it is an IP host address that sends traffic to the group. The default for `{A.B.C.D}{A.B.C.D} enable` is `enable` for each entry. The default is `enable` for each entry.

### **stream-timeout <10-432000>**

Specifies the activity timeout for IGMP snooping streams in seconds. The default is 300 seconds.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

Before you disable or delete an ssm-map, always send IGMPv1 or IGMPv2 leave messages from hosts that operate in IGMPv1 or IGMPv2. If you do not perform this action, receiving and processing reports in SSM range on an IGMP interface enabled with IGMPv1 or IGMPv2 can lead to unexpected behavior.

## ip igmp generate-log

---

Set igmp log.

### Syntax

- **ip igmp generate-log**

### Default

None

## Command Mode

Global Configuration

## ip ipfix aging-interval

---

Specifies (in seconds) the flow record aging interval.

### Syntax

- **default ip ipfix aging-interval**
- **ip ipfix aging-interval <interval>**
- **no ip ipfix aging-interval**

## Command Parameters

*<interval>*

Specifies (in seconds) the flow record aging interval. The aging interval determines how long a traffic flow that is no longer being received is retained as a flow. Depending on the hardware platform, the parameter range and default value can vary. Use the CLI Help to see the available range for the switch.

## Default

The default varies depending on the platform:

- 5420 Series - 10 seconds
- 5520 Series - 10 seconds
- VSP 7400 Series - 40 seconds

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip ipfix collector

---

Configure a collector for Internet Protocol Flow Information eXport (IPFIX).

## Syntax

- **ip ipfix collector <1-1> {A.B.C.D} exporter-ip {A.B.C.D} [dest-port <1-65535>] [src-port <1-65535>] [export-interval <1-120>] [initial-burst <1-10>]**

## Command Parameters

**{A.B.C.D}**

Specifies the IP address of the collector.

**<1-1>**

Specifies the IPFIX collector ID.

**exporter-ip {A.B.C.D}**

Specifies the IP address of the exporter.

**dest-port <1-65535>**

Specifies the destination port receiving flow information.

**src-port <1-65535>**

Specifies the source port sending flow information.

**export-interval**

Specifies, in seconds, the frequency of template packet exports to the collector. The default value is 60 seconds.

**initial-burst**

Specifies the number of template packets sent when the collector becomes reachable. The default value is 5.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip ipfix enable

---

Enable IPFIX globally.

## Syntax

- **default ip ipfix enable**
- **ip ipfix enable**
- **no ip ipfix enable**

## Default

The default value is disable.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip ipfix observation-domain

---

Assign a unique ID to an IPFIX observation domain.

## Syntax

- **default ip ipfix observation-domain**
- **ip ipfix observation-domain <0-4294967295>**
- **no ip ipfix observation-domain**

## Command Parameters

<0-4294967295>

Specifies the observation domain ID. The default is 0.

## Default

The default value is 0.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip irdp

---

Enable Router Discovery globally so that the switch supports Router Discovery.

## Syntax

- **default ip irdp**
- **default ip irdp enable**
- **ip irdp**
- **ip irdp enable**
- **no ip irdp**
- **no ip irdp enable**

## Command Parameters

**enable**

Enables the router discovery protocol on the switch.

## Default

None

## Command Mode

Global Configuration

---

## ip isid-list

---

Create an I-SID list to use with IS-IS accept policies.

### Syntax

- **ip isid-list WORD<1-32> <0-16777215>**
- **ip isid-list WORD<1-32> list WORD<1-1024>**
- **no ip isid-list WORD<1-32> <0-16777215>**
- **no ip isid-list WORD<1-32> list WORD<1-1024>**

### Command Parameters

**<1-16777215>**

Specifies an I-SID value.

**list WORD<1-1024>**

Specifies the of I-SID values.

**WORD<1-32>**

Specifies a name for the I-SID list.

### Default

None

### Command Mode

Global Configuration

### Usage Guidelines

When creating an I-SID list, you can add I-SID entries until the maximum limit for supported Layer 3 I-SIDs is reached. The system truncates any additional I-SID entries. The maximum limit includes the I-SIDs for locally configured Layer 3 VSNS and the I-SIDs specified for IS-IS accept policy filters.

Use the command **show ip isid-list vrf WORD<1-16>** to view the list of truncated I-SIDs.

When deleting an I-SID list, ensure that the I-SID list is not associated with an IS-IS accept policy. Otherwise the deletion fails. An I-SID list associated with an accept policy cannot be deleted because it must contain at least one constituent I-SID.

---

## ip max-routes-trap enable

---

Enable the switch to send a trap when the maximum number of routes is exceeded.

## Syntax

- **default ip max-routes-trap enable**
- **ip max-routes-trap enable**
- **no ip max-routes-trap enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

## ip more-specific-non-local-route

---

Enable the more-specific-non-local-route feature. If enabled, the switch can enter a more specific nonlocal route into the routing table.

## Syntax

- **default ip more-specific-non-local-route**
- **default ip more-specific-non-local-route enable**
- **ip more-specific-non-local-route**
- **ip more-specific-non-local-route enable**
- **no ip more-specific-non-local-route**
- **no ip more-specific-non-local-route enable**

## Command Parameters

**enable**

Enable more-specific-non-local-route

## Default

The default is disabled.

## Command Mode

Global Configuration

## ip mroute resource-usage (globally)

---

Configure the resource usage counters to query the number of ingress and egress IP multicast streams traversing your switch and enable traps and log messages on the console.



## Syntax

- **default ip mroute resource-usage egress-threshold ingress-threshold**
- **default ip mroute resource-usage ingress-threshold**
- **ip mroute resource-usage egress-threshold <0-32767> [ingress-threshold <0-32767>]**
- **ip mroute resource-usage ingress-threshold <0-32767>**
- **ip mroute resource-usage log-msg [trap-msg]**

## Command Parameters

### egress-threshold <0-32767>

Configures the egress record threshold (S,G). A notification message is sent if this value is exceeded.

The integer is a value between 0-32767. To set this option to the default value, use the default operator with the command. The default is 0.

### ingress-threshold <0-32767>

Configures the ingress record threshold (peps). A notification message is sent if this value is exceeded.

the integer is a value between 0-32767. To set this option to the default value, use the default operator with the command. The default is 0.

### log-msg

Configures the notification method for sending only a log message after the threshold level is exceeded. Use the no operator to later remove this configuration. To set this option to the default value, use the default operator with the command. The default is disabled.

### trap-msg

Configures the notification method for sending only a trap message after the threshold level is exceeded. Use the no operator to later remove this configuration. To set this option to the default value, use the default operator with the command. The default is disabled.

## Default

None

## Command Mode

Global Configuration

## ip mroute resource-usage egress-threshold

Configure the resource usage counters to query the number of ingress and egress IP multicast streams traversing your switch.

## Syntax

- **ip mroute resource-usage egress-threshold <0-32767> ingress-threshold <0-32767>**

## Command Parameters

### egress-threshold <0-32767>

Configures the egress record threshold (S,G). A notification message is sent if this value is exceeded.

The integer is a value between 0-32767. To set this option to the default value, use the default operator with the command. The default is 0.

### ingress-threshold <0-32767>

Configures the ingress record threshold (peps). A notification message is sent if this value is exceeded.

The integer is a value between 0-32767. To set this option to the default value, use the default operator with the command. The default is 0.

## Default

None

## Command Mode

Global Configuration

## ip mroute resource-usage log-msg trap-msg

---

Enable traps and log messages on the console.

## Syntax

- **ip mroute resource-usage log-msg trap-msg**

## Command Parameters

### log-msg

Configures the notification method for sending only a log message after the threshold level is exceeded. Use the no operator to later remove this configuration. To set this option to the default value, use the default operator with the command. The default is disabled.

### trap-msg

Configures the notification method for sending only a trap message after the threshold level is exceeded. Use the no operator to later remove this configuration. To set this option to the default value, use the default operator with the command. The default is disabled.

## Default

None

## Command Mode

Global Configuration

## ip mroute static-source-group

---

Configure static source-group entries in the Protocol Independent Multicast (PIM) multicast routing table.

## Syntax

- **ip mroute static-source-group <A.B.C.D> <A.B.C.D/X>**
- **no ip mroute static-source-group <A.B.C.D> <A.B.C.D/X>**

## Command Parameters

**<A.B.C.D>**

Specifies the group IP address.

**A.B.C.D/X**

Specifies the multicast source IP address and subnet mask for the static source group entry. You cannot create duplicate groups. How you configure the source address depends on the protocol and mode you use. Use the no operator to remove this configuration.

## Default

None

## Command Mode

Global Configuration

## ip mroute stats enable

---

Enable the collection of multicast routing process statistics.

## Syntax

- **default ip mroute stats enable**
- **ip mroute stats enable**
- **no ip mroute stats enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

## ip mroute stream-limit (globally)

---

Limit the number of multicast streams to protect a Central Processor Unit (CPU) from multicast data packet bursts generated by malicious applications.

## Syntax

- **default ip mroute stream-limit**
- **ip mroute stream-limit**
- **no ip mroute stream-limit**

## Default

None

## Command Mode

Global Configuration

## ip msdp apply redistribute (globally)

---

Apply MSDP redistribution filters.

## Syntax

- **default ip msdp apply redistribute**
- **ip msdp apply redistribute**
- **no ip msdp apply redistribute**

## Default

None

## Command Mode

Global Configuration

---

## ip msdp connect—retry (globally)

---

Configure the connect-retry period to specify the amount of time, in seconds, between connection attempts for peering sessions.

### Syntax

- **default ip msdp connect—retry {A.B.C.D} <1-65535>**
- **ip msdp connect—retry {A.B.C.D} <1-65535>**
- **no ip msdp connect—retry {A.B.C.D} <1-65535>**

### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

<1-65535>

Specifies the connect-retry interval in seconds. The default is 30 seconds.

### Default

The default is 30 seconds.

### Command Mode

Global Configuration

---

## ip msdp enable

---

Enable Multicast Source Discovery Protocol (MSDP).

### Syntax

- **default ip msdp enable**
- **ip msdp enable**
- **no ip msdp enable**

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## ip msdp keepalive (globally)

---

Configure keepalive messages to adjust the interval in seconds at which an MSDP peer sends keep alive messages.

### Syntax

- **default ip msdp keepalive {A.B.C.D} <0-21845> <0-65535>**
- **ip msdp keepalive {A.B.C.D} <0-21845> <0-65535>**
- **no ip msdp keepalive {A.B.C.D} <0-21845> <0-65535>**

### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

<0-21845>

Specifies the keep alive interval in seconds. The default is 60 seconds.

<0-65535>

Specifies the hold time interval in seconds. The default is 75 seconds. 0 seconds means the peer never expires. Values 1 and 2 are not allowed.

### Default

The default is 60 seconds.

### Command Mode

Global Configuration

---

## ip msdp md5-authentication (globally)

---

Configure Message Digest (MD) 5 authentication to secure control messages on the TCP connection between MSDP peers.

### Syntax

- **default ip msdp md5-authentication**
- **ip msdp md5-authentication**
- **ip msdp md5-authentication {A.B.C.D} [enable]**
- **no ip msdp md5-authentication {A.B.C.D} [enable]**

### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

**enable**

Enables MD5 authentication.

## Default

The default is disabled.

## Command Mode

Global Configuration

## ip msdp mesh-group (globally)

---

Configure mesh groups to reduce SA flooding. A mesh group does not forward SA messages to other group members.

## Syntax

- **default ip msdp mesh-group WORD<1-64> {A.B.C.D}**
- **ip msdp mesh-group WORD<1-64> {A.B.C.D}**
- **no ip msdp mesh-group WORD<1-64> {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

WORD<1-64>

Specifies the mesh group name.

## Default

None

## Command Mode

Global Configuration

## ip msdp originator-id (globally)

---

Configure the originator ID to set the Rendezvous Point (RP) address inside the Source Active (SA) message.

## Syntax

- **default ip msdp originator-id {A.B.C.D}**
- **ip msdp originator-id {A.B.C.D}**

- **no ip msdp originator-id {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies the MSDP source IP address.

## Default

None

## Command Mode

Global Configuration

## ip msdp password peer (globally)

---

Configure the case sensitive password for MD5 authentication

## Syntax

- **default ip msdp password peer {A.B.C.D}**
- **ip msdp password peer {A.B.C.D} WORD<1-80>**
- **no ip msdp password peer {A.B.C.D} WORD<1-80>**

## Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

WORD<1-80>

Specifies the MD5 authentication password.

## Default

None

## Command Mode

Global Configuration

## ip msdp redistribute (globally)

---

Filter SPB routes to filter which (S,G,RP) entries sent out to all MSDP peers.



## Syntax

- `default ip msdp redistribute`
- `ip msdp redistribute`
- `no ip msdp redistribute`

## Default

None

## Command Mode

Global Configuration

## ip msdp redistribute route-policy (globally)

---

Create the route policy name.

## Syntax

- `default ip msdp redistribute route-policy WORD<1-64>`
- `ip msdp redistribute route-policy WORD<1-64>`
- `no ip msdp redistribute route-policy WORD<1-64>`

## Command Parameters

WORD<1-64>

Specifies the route policy name.

## Default

None

## Command Mode

Global Configuration

## ip msdp sa-filter in (globally)

---

Create the inbound filter.

## Syntax

- `default ip msdp sa-filter in {A.B.C.D}`
- `default ip msdp sa-filter in {A.B.C.D} route-policy WORD<1-64>`
- `ip msdp sa-filter in {A.B.C.D}`

- **ip msdp sa-filter in {A.B.C.D} route-policy WORD<1-64>**
- **no ip msdp sa-filter in {A.B.C.D}**
- **no ip msdp sa-filter in {A.B.C.D} route-policy WORD<1-64>**

## Command Parameters

**{A.B.C.D}**

Specifies the MSDP peer IP address.

**route-policy WORD<1-64>**

Specifies the route policy name for an inbound filter.

## Default

None

## Command Mode

Global Configuration

## ip msdp sa-filter out (globally)

---

Create the outbound filter.

## Syntax

- **default ip msdp sa-filter out {A.B.C.D}**
- **default ip msdp sa-filter out {A.B.C.D} route-policy WORD<1-64>**
- **ip msdp sa-filter out {A.B.C.D}**
- **ip msdp sa-filter out {A.B.C.D} route-policy WORD<1-64>**
- **no ip msdp sa-filter out {A.B.C.D}**
- **no ip msdp sa-filter out {A.B.C.D} route-policy WORD<1-64>**

## Command Parameters

**{A.B.C.D}**

Specifies the MSDP peer IP address.

**route-policy WORD<1-64>**

Specifies the route policy name for an outbound filter.

## Default

None

## Command Mode

Global Configuration

### ip msdp sa-limit (globally)

---

Specifies the maximum number of SA messages to keep in SA cache.

#### Syntax

- **default ip msdp sa-limit {A.B.C.D} <0-6144>**
- **ip msdp sa-limit {A.B.C.D} <0-6144>**
- **no ip msdp sa-limit {A.B.C.D} <0-6144>**

#### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

<0-6144>

Specifies the maximum number of SA messages to keep in SA cache. The default is 6144 messages.

#### Default

The default is 6144.

## Command Mode

Global Configuration

### ip msdp ttl-threshold (globally)

---

Configure the time-to-live (TTL) threshold to limit which multicast data packets the router encapsulated in SA Message forwarded to an MSDP peer.

#### Syntax

- **default ip msdp ttl-threshold {A.B.C.D} <1-255>**
- **ip msdp ttl-threshold {A.B.C.D} <1-255>**
- **no ip msdp ttl-threshold {A.B.C.D} <1-255>**

#### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

<1-255>

Specifies the Time-To-Live value. The default is 1.

## Default

The default is 1.

## Command Mode

Global Configuration

---

## ip name-server

Add or delete IP addresses for DNS servers.

## Syntax

- **default ip name-server primary**
- **default ip name-server secondary**
- **default ip name-server tertiary**
- **ip name-server primary WORD<0-46>**
- **ip name-server secondary WORD<0-46>**
- **ip name-server tertiary WORD<0-46>**
- **no ip name-server primary**
- **no ip name-server primary-dynamic**
- **no ip name-server secondary**
- **no ip name-server secondary-dynamic**
- **no ip name-server tertiary**
- **no ip name-server tertiary-dynamic**

## Command Parameters

<primary|primary-dynamic|secondary|secondary-dynamic|tertiary|tertiary-dynamic>WORD<0-46>

Configures the primary, secondary, or tertiary DNS server address. Enter the IP address in a.b.c.d format for IPv4 (string length 0-46). You can specify the IP address for only one server at a time; you cannot specify all three servers in one command.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

The dynamic DNS parameters only apply to the **no ip name-server** command. The *primary-dynamic*, *secondary-dynamic*, *tertiary-dynamic* parameters are not supported on VSP 8600 Series.

## ip pim (globally)

---

Configure PIM to create a PIM instance, and enable or disable PIM globally on the switch and change default global parameters.

### Syntax

- **default ip pim**
- **default ip pim bootstrap-period**
- **default ip pim disc-data-timeout**
- **default ip pim enable**
- **default ip pim fast-joinprune**
- **default ip pim fwd-cache-timeout**
- **default ip pim join-prune-interval**
- **default ip pim register-suppression-timeout**
- **default ip pim rp-c-adv-timeout**
- **default ip pim unicast-route-change-timeout**
- **ip pim**
- **ip pim bootstrap-period <5-32757>**
- **ip pim disc-data-timeout <5-65535>**
- **ip pim enable**
- **ip pim fast-joinprune**
- **ip pim fwd-cache-timeout <10-86400>**
- **ip pim join-prune-interval <1-18724>**
- **ip pim register-suppression-timeout <6-65535>**
- **ip pim rp-c-adv-timeout <5-26214>**
- **ip pim unicast-route-change-timeout <2-65535>**
- **no ip pim**
- **no ip pim enable**
- **no ip pim fast-joinprune**
- **no ip pim spt-infinite-threshold**

### Command Parameters

**bootstrap-period <5-32757>**

Specify the interval (in seconds) that the elected bootstrap router (BSR) waits between originating bootstrap messages.

**disc-data-timeout <5-65535>**

Specify how long (in seconds) to discard data until the join is received from the rendezvous point (RP). An IP multicast discard record is created after a register packet is sent, until the timer expires or a join is received.

**enable**

Activates PIM on the switch globally.

**fast-joinprune**

Enable the fast join prune interval.

**fwd-cache-timeout <10-86400>**

Specify the forward cache timeout value.

**join-prune-interval <1-18724>**

Specify how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors.

**register-suppression-timeout <6-65535>**

Specify how long (in seconds) the designated router (DR) suppresses sending registers to the RP. The timer starts after the DR receives a register-stop message from the RP.

**rp-c-adv-timeout <5-26214>**

Specify how often (in seconds) a router configured as a candidate RP (C-RP) sends C-RP advertisement messages. After this timer expires, the C-RP router sends an advertisement message to the elected BSR.

**unicast-route-change-timeout <2-65535>**

Specify how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates for PIM. Lowering this value increases how often the switch polls the RTM. This can affect the performance of the switch, especially when a high volume of traffic flows through the switch.

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip pim mode

---

Configure the mode of this interface globally. After you change from one mode to another, the system displays an information message to remind you that traffic does not stop immediately.

### Syntax

- **default ip pim mode**
- **ip pim mode sparse**
- **ip pim mode ssm**

### Command Parameters

<ssm|sparse>

Specifies the mode. Configures Source Specific Multicast (SSM) to optimize PIM-SM by simplifying the many-to-many model (servers-to-receivers).

### Default

The default is sparse.

### Command Mode

Global Configuration

## ip pim rp-candidate group

---

Configure a candidate rendezvous point (C-RP) to serve as backup to the RP router.

### Syntax

- **default ip pim rp-candidate group <A.B.C.D> <A.B.C.D>**
- **ip pim rp-candidate group <A.B.C.D> <A.B.C.D> rp <A.B.C.D>**
- **no ip pim rp-candidate group <A.B.C.D> <A.B.C.D>**

### Command Parameters

{A.B.C.D} {A.B.C.D}

Specifies the IP address and group mask of the multicast group. When combined, they identify the prefix that the local router uses to advertise itself as a C-RP router.

rp {A.B.C.D}

Specifies the IP address of the C-RP router. This address must be one of the local PIM-SM enabled interfaces.

## Default

None

## Command Mode

Global Configuration

## ip pim spt-infinite-threshold

---

Enable PIM Infinite Threshold Policy for IPv4.

## Syntax

- **default ip pim spt-infinite-threshold**
- **ip pim spt-infinite-threshold**
- **no ip pim spt-infinite-threshold**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip pim static-rp

---

Adds a static rendezvous point (RP) entry and activates static RP.

## Syntax

- **default ip pim static-rp**
- **ip pim static-rp <A.B.C.D/X> <A.B.C.D>**
- **no ip pim static-rp**

## Command Parameters

<A.B.C.D/X>

Specifies the IP address and address mask of the multicast group. When combined, the IP address and address mask identify the range of the multicast addresses that the RP handles.



<A.B.C.D>

Specifies the IP address of the static RP.

## Default

The default is disabled.

## Command Mode

Global Configuration

## ip pim virtual-neighbor

---

Configure a virtual neighbor when the next hop for a static route cannot run PIM.

## Syntax

- **ip pim virtual-neighbor <A.B.C.D> <A.B.C.D>**
- **no ip pim virtual-neighbor <A.B.C.D> <A.B.C.D>**

## Command Parameters

<A.B.C.D>

The first IP address indicates the IP address of the selected interface.

<A.B.C.D>

The second IP address indicates the IP address of the neighbor.

## Default

None

## Command Mode

Global Configuration

## ip prefix-list

---

Allows or denies specific route updates. A prefix list policy specifies route prefixes to match. When there is a match, the route is used. Configure a prefix list and apply the list to an IP route policy.

## Syntax

- **ip prefix-list WORD<1-64> {A.B.C.D/X} [id <1-2147483647>] [ge <0-32>] [le <0-32>]**
- **ip prefix-list WORD<1-64> name WORD<1-64>**

- **no ip prefix-list WORD<1-64>**
- **no ip prefix-list WORD<1-64> {A.B.C.D/X}**

## Command Parameters

**<A.B.C.D/X>**

Specifies a prefix entry to add to the prefix list. A.B.C.D/X is the IP address and mask. Use the no operator to remove a prefix entry from the prefix list.

**ge<0-32>**

Specifies the minimum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

**id<1-2147483647>**

Specifies the prefix list ID.

**le<0-32>**

Specifies the maximum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

**name WORD<1-64>**

Specifies a new name for the prefix list.

## Default

None

## Command Mode

Global Configuration

## ip route (globally)

---

You can configure routing switches with a static default route, or they can learn it through a dynamic routing protocol. Use this command to:

- Create static routes for data traffic in the GRT.
- Create static routes for management purposes on VSP 8600 Series:
  - Use the default VRF context to configure static routes in the GRT for the inband VLAN or loopback interface.

## Syntax

- **default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} [dynamic] [enable] [local-next-hop enable] [name] [preference]**
- **ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable [next-hop-vrf WORD<1-16>]**
- **ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable**

- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} name WORD<0-64>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1-255> [next-hop-vrf WORD<1-16>]`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> [local-next-hop enable] [name WORD<0-64>] [next-hop-vrf WORD<1-16>] [preference <1-255>]`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} [dynamic] [enable] [local-next-hop enable] [name] [next-hop-vrf WORD<1-16>] [preference]`

## Command Parameters

### {A.B.C.D}

The first and second <A.B.C.D> specify the IP address and mask for the route destination.

255.255.255.255 is the black hole route. Configures a black hole static route to the destination a router advertises to avoid routing loops when aggregating or injecting routes to other routers.

The default route specifies a route to all networks for which there are no explicit routes in the Forwarding Information Base or the routing table. The default route has a prefix length of zero (RFC 1812).

### enable

Adds a static or default route to the router or VRF.

### local-next-hop enable

Enables the local next hop for this static route.

### name WORD<1-64>

Specifies the static route name.

### next-hop-vrf WORD<1-16>

Specifies the next-hop VRF instance by name.

### preference <1-255>

Specifies the route preference.

### weight <1-65535>

Specifies the static route cost.



### Note

Do not configure a static interface subnet route with a weight of 1.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

The *name* parameter is not supported on VSP 8600 Series.

VSP 8600 Series uses the routing stack to create static routes for data traffic as well as management purposes. For all other platforms, static routes for the management OOB and management VLAN, if supported, must use the Segmented Management Instance. For more information, see [VOSS User Guide](#). The management CLIP can use the Segmented Management Instance or routes in the associated VRF routing table manager (RTM).

## ip route bfd

---

Configure an IPv4 static route for Bidirectional Forwarding Detection (BFD).

### Syntax

- **default ip route bfd {A.B.C.D}**
- **ip route bfd {A.B.C.D}**
- **no ip route bfd {A.B.C.D}**

### Command Parameters

{A.B.C.D}

Specifies the BFD static route IPv4 address.

### Command Mode

Global Configuration

## ip route preference protocol ebgp

---

Configure the global route preference.

### Syntax

- **default ip route preference protocol ebgp**
- **ip route preference protocol ebgp <0-255>**

### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

### Default

The default is 45.

## Command Mode

Global Configuration

## ip route preference protocol ibgp

---

Configure the global route preference.

### Syntax

- **default ip route preference protocol ibgp**
- **ip route preference protocol ibgp <0-255>**

### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

### Default

The default is 175.

## Command Mode

Global Configuration

## ip route preference protocol ospf-extern1

---

Configure the global route preference.

### Syntax

- **default ip route preference protocol ospf-extern1**
- **ip route preference protocol ospf-extern1 <0-255>**

### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

### Default

The default is 120.

## Command Mode

Global Configuration

## ip route preference protocol ospf-extern2

---

Configure the global route preference.

### Syntax

- **default ip route preference protocol ospf-extern2**
- **ip route preference protocol ospf-extern2 <0-255>**

### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

### Default

The default is 125.

## Command Mode

Global Configuration

## ip route preference protocol ospf-inter

---

Configure the global route preference.

### Syntax

- **default ip route preference protocol ospf-inter**
- **ip route preference protocol ospf-inter <0-255>**

### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

### Default

The default is 25.

## Command Mode

Global Configuration

## ip route preference protocol ospf-intra

---

Configure the global route preference.

### Syntax

- **default ip route preference protocol ospf-intra**
- **ip route preference protocol ospf-intra <0-255>**

### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

### Default

The default is 20.

## Command Mode

Global Configuration

## ip route preference protocol rip

---

Configure the global route preference.

### Syntax

- **default ip route preference protocol rip**
- **ip route preference protocol rip <0-255>**

### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

### Default

The default is 100.

## Command Mode

Global Configuration

### ip route preference protocol spbm-level1

---

Configure the global route preference.

#### Syntax

- **default ip route preference protocol spbm-level1**
- **ip route preference protocol spbm-level1 <0-255>**

#### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

#### Default

The default is 7.

## Command Mode

Global Configuration

### ip route preference protocol static

---

Configure the global route preference.

#### Syntax

- **default ip route preference protocol static**
- **ip route preference protocol static <0-255>**

#### Command Parameters

<0-255>

Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

#### Default

The default is 5.



## Command Mode

Global Configuration

## ip routing

---

Enable IP forwarding (routing) on a global level so that the router supports routing. You can use the IP address of any router interface for IP-based network management.

### Syntax

- **default ip routing**
- **ip routing**
- **no ip routing**

### Default

None

## Command Mode

Global Configuration

## ip rsmlt edge-support

---

Configure Routed Split MultiLink trunking (RSMLT)-edge to store the RSMLT peer MAC/IP address-pair in its local config file and restore the configuration if the peer does not restore after a simultaneous reboot of both RSMLT-peer switches. The configuration applies to both IPv4.

### Syntax

- **default ip rsmlt edge-support**
- **ip rsmlt edge-support**
- **no ip rsmlt edge-support**
- **no ip rsmlt peer-address <1-4059>**

### Command Parameters

**edge-support**

Enables RSMLT-edge support.

### Default

The default is disabled.

## Command Mode

Global Configuration

## ip source-route

---

Enables IPv4 source routing globally.

### Syntax

- **default ip source-route**
- **ip source-route**
- **no ip source-route**

### Default

Disabled

## Command Mode

Global Configuration

## ip spb-pim-gw foreign-source (globally)

---

Configures a static foreign source.

### Syntax

- **default ip spb-pim-gw foreign-source {A.B.C.D} group {A.B.C.D}**
- **ip spb-pim-gw foreign-source {A.B.C.D} group {A.B.C.D}**
- **no ip spb-pim-gw foreign-source {A.B.C.D} group {A.B.C.D}**

### Command Parameters

**{A.B.C.D}**

Specifies the multicast foreign source IP address.

**group {A.B.C.D}**

Specifies the group IP address.

### Default

None

## Command Mode

Global Configuration

## ip supernet

---

Enable or disable supernetting. If supernetting is globally enabled, the switch can learn routes with a route mask of less than eight bits. Routes with a mask length less than eight bits cannot have ECMP paths, even if the ECMP feature is globally enabled.

### Syntax

- **default ip supernet**
- **ip supernet**
- **no ip supernet**

### Default

The default is disabled.

### Command Mode

Global Configuration

## ip tcp adjust-mss

---

Adjusts the TCP maximum segment size (MSS) to improve the throughput for the TCP session over a Fabric Extend (FE) adjacency.

### Syntax

- **default ip tcp adjust-mss**
- **ip tcp adjust-mss [<max-segment-size>] [enable]**
- **no ip tcp adjust-mss enable**

### Command Parameters

#### enable

Enables the functionality.

*<max-segment-size>*

Specifies the Maximum Transmission Unit (MTU) size for each packet. Different hardware platforms support different MTU ranges. Use the CLI Help to see the available range for the switch.

### Default

The default varies depending on hardware platform:

- For XA1400 Series, this functionality is enabled, when at least one Fabric Extend (FE) tunnel with a MTU less than or equal to 1500 is configured, and the value is auto-derived.

- For VSP 4900 Series, VSP 7400 Series, 5420 Series, and 5520 Series this functionality is disabled. The default value, when enabled, is 1300.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip ttl

---

Configure the IP routing protocol stack to specify which routing features the switch can use.

## Syntax

- **default ip ttl**
- **ip ttl <1-255>**
- **no ip ttl**

## Command Parameters

**ttl<1-255>**

Configures the default time-to-live (TTL) value for a routed packet. The TTL is the maximum number of seconds before a packet is discarded. The default value of 255 is used whenever a time is not supplied in the datagram header.

## Default

The default value is 255.

## Command Mode

Global Configuration

## ip vrf

---

Creates a VRF instance.

## Syntax

- **default ip vrf WORD<1-16> max-routes**
- **default ip vrf WORD<1-16> max-routes-trap enable**
- **default ip vrf WORD<1-16> vrf-trap enable**

- **ip vrf WORD<1-16>**
- **ip vrf WORD<1-16> ipv6-max-routes <max-routes>**
- **ip vrf WORD<1-16> ipv6-max-routes-trap enable**
- **ip vrf WORD<1-16> max-routes <max-routes>**
- **ip vrf WORD<1-16> max-routes-trap enable**
- **ip vrf WORD<1-16> name WORD<0-16>**
- **ip vrf WORD<1-16> vrfid <1-511>**
- **ip vrf WORD<1-16> vrf-trap enable**
- **no ip vrf WORD<1-16>**
- **no ip vrf WORD<1-16> ipv6-max-routes-trap enable**
- **no ip vrf WORD<1-16> max-routes-trap enable**
- **no ip vrf WORD<1-16> vrf-trap enable**

## Command Parameters

### **ipv6-max-routes <0-7744>**

Specifies the maximum number of IPv6 routes for the VRF. Depending on the hardware platform, the parameter range and default value can vary. Use the CLI Help to see the available range for the switch. For route scaling information, see [VSP 8600 Release Notes](#).

### **ipv6-max-routes-trap enable**

Enables SNMP trap generation based on the configured number of maximum IPv6 routes.

### **max-routes <max-routes>**

Specifies the maximum number of IPv4 routes for the VRF. Depending on the hardware platform, the parameter range and default value can vary. Use the CLI Help to see the available range for the switch. For route scaling information, see [VSP 8600 Release Notes](#).

### **max-routes-trap enable**

Enables the sending of traps after the maximum number of routes is reached. The default is enabled.

### **name WORD<1-16>**

Renames the VRF instance.

### **vrfid <1-511>**

Specifies a VRF ID. The switch supports 512 VRFs.

### **vrf-trap enable**

Enables the device to send VRF-related traps. The default is enabled.

### **WORD<1-16>**

Specifies the name for the VRF.

## Default

None

## Command Mode

Global Configuration

## ipsec policy

Create and configure an Internet Protocol Security (IPsec) policy.

### Syntax

- **default ipsec policy WORD<1-32>**
- **ipsec policy WORD<1-32>**
- **ipsec policy WORD<1-32> action drop**
- **ipsec policy WORD<1-32> action permit**
- **ipsec policy WORD<1-32> laddr WORD<1-32>**
- **ipsec policy WORD<1-32> protocol icmp**
- **ipsec policy WORD<1-32> protocol icmpv6**
- **ipsec policy WORD<1-32> protocol ospfv3**
- **ipsec policy WORD<1-32> protocol tcp sport <1-65535> dport <1-65535>**
- **ipsec policy WORD<1-32> protocol tcp sport <1-65535> dport any**
- **ipsec policy WORD<1-32> protocol udp**
- **ipsec policy WORD<1-32> protocol udp sport <1-65535> dport <1-65535>**
- **ipsec policy WORD<1-32> protocol udp sport <1-65535> dport any**
- **ipsec policy WORD<1-32> raddr WORD<1-32>**
- **no ipsec policy WORD<1-32>**

### Command Parameters

**action <drop|permit>**

Specifies the action the policy takes. The default is permit.

**dport<1-65535|<any>**

Specifies the destination port for TCP and UDP. You can specify any port as the destination port. The default is any.

**laddr WORD<1-32>**

Specifies the local address. This field is optional. laddr is an optional parameter that allows you to have multiple local addresses for each remote address. If you do not configure this parameter, then the IPv6 address 0::0 is the default, which configures this parameter to any address.

**protocol <icmp|icmpv6|ospfv3|tcp|udp>**

Specifies the protocol. The default is TCP.

**raddr WORD<1-32>**

Specifies the remote address. Use the address 0::0 to configure raddr to any, which allows the parameter to act as a wildcard entry with any destination acceptable.

**sport <1-65535>**

Specifies the source port for TCP and UDP.

**WORD<1-32>**

Specifies the policy ID

## Default

The default is disabled.

## Command Mode

Global Configuration

## ipsec policy admin enable

---

Enable an Internet Protocol Security (IPsec) policy.

## Syntax

- **ipsec policy WORD<1-32> admin enable**
- **no ipsec policy WORD<1-32> admin enable**

## Command Parameters

**WORD<1-32>**

Specifies the IPsec policy name.

## Default

The default is disabled.

## Command Mode

Global Configuration

## ipsec policy security-association

---

Link an Internet Protocol Security (IPsec) policy to an IPsec security association.

## Syntax

- **default ipsec policy WORD<1-32> security-association WORD<1-32>**
- **ipsec policy WORD<1-32> security-association WORD<1-32>**
- **no ipsec policy WORD<1-32> security-association WORD<1-32>**

## Default

None

## Command Mode

Global Configuration

# ipsec security-association

---

Create and configure an Internet Protocol Security (IPsec) security association.

## Syntax

- `default ipsec security-association WORD<1-32>`
- `ipsec security-association WORD<1-32>`
- `ipsec security-association WORD<1-32> auth-algo AES-XCBC-MAC`
- `ipsec security-association WORD<1-32> auth-algo AES-XCBC-MAC auth-key WORD<1-256> KeyLength <1-256>`
- `ipsec security-association WORD<1-32> auth-algo MD5`
- `ipsec security-association WORD<1-32> auth-algo MD5 auth-key WORD<1-256> KeyLength <1-256>`
- `ipsec security-association WORD<1-32> auth-algo SHA1`
- `ipsec security-association WORD<1-32> auth-algo SHA1 auth-key WORD<1-256> KeyLength <1-256>`
- `ipsec security-association WORD<1-32> auth-algo SHA2`
- `ipsec security-association WORD<1-32> auth-algo SHA2 auth-key WORD<1-256> KeyLength <1-256>`
- `ipsec security-association WORD<1-32> encap-proto AH`
- `ipsec security-association WORD<1-32> encap-proto ESP`
- `ipsec security-association WORD<1-32> Encrpt-algo 3DES`
- `ipsec security-association WORD<1-32> Encrpt-algo 3DES EncrptKey WORD<1-256> KeyLength <1-256>`
- `ipsec security-association WORD<1-32> Encrpt-algo AES-CBC`
- `ipsec security-association WORD<1-32> Encrpt-algo AES-CBC EncrptKey WORD<1-256> KeyLength <1-256>`
- `ipsec security-association WORD<1-32> Encrpt-algo AES-CTR`
- `ipsec security-association WORD<1-32> Encrpt-algo AES-CTR EncrptKey WORD<1-256> KeyLength <1-256>`
- `ipsec security-association WORD<1-32> Encrpt-algo NULL`
- `ipsec security-association WORD<1-32> Encrpt-algo NULL EncrptKey WORD<1-256> KeyLength <1-256>`
- `ipsec security-association WORD<1-32> key-mode automatic`



- **ipsec security-association WORD<1-32> key-mode manual**
- **ipsec security-association WORD<1-32> lifetime Bytes <1-4294967295>**
- **ipsec security-association WORD<1-32> lifetime seconds <1-4294967295>**
- **ipsec security-association WORD<1-32> mode transport**
- **ipsec security-association WORD<1-32> spi <1-4294967295>**
- **no ipsec security-association WORD<1-32>**

## Command Parameters

**auth-algo <AES-XCBC-MAC| 32 MD5|SHA1|SHA2>**

The authentication algorithm parameter specifies the authorization algorithm, which includes one of the following values:

- AES-XCBC-MAC
- MD5
- SHA1
- SHA2

The default authentication algorithm name is MD5.

**auth-key WORD<1-256> [KeyLength WORD<1-256>]**

The parameter auth-key specifies the authentication key. KeyLength specifies the KeyLength value that can be a string of 1 to 256 characters. The default KeyLength is 128. The KeyLength values are as follows:

- 3DES is 48
- AES-CBC is 32, 48, or 64
- AES-CTR is 32

**encap-proto <AH|ESP>**

Specifies the encapsulation protocol. AH specifies the authentication header and ESP specifies the encapsulation security payload. If you configure the encapsulation protocol as AH, you cannot configure the encryption algorithms and other encryption-related attributes. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to ESP. The default value is ESP.

**Encript-algo <3DES|AES24 CBC|AES-CTR|NULL>**

Specifies the encryption algorithm value as one of the following:

- 3DES-CBC
- AES-CBC
- AES-CTR
- NULL

The default encryption algorithm value is AES-CBC. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to ESP.

**EncriptKey WORD<1-256> [KeyLength WORD<1-256>]**

EncrptKey specifies the encryption key. KeyLength specifies the KeyLength value that can be a string of 1 to 256 characters. The default KeyLength is 128. The KeyLength values are as follows:

- 3DES is 48
- AES-CBC is 32, 48, or 64
- AES-CTR is 32

**key-mode <automatic|manual>**

Specifies the key-mode as one of the following: automatic or manual. The default is manual.

**lifetime <Bytes <1-4294967295>|seconds <1-4294967295>**

Specifies the lifetime value in seconds or kilobytes. The default lifetime value in seconds is 8 hours. The default value in bytes is 4608000 kilobytes.

**mode <transport|tunnel>**

Specifies the mode value in either transport or tunnel.

Transport mode encapsulates the IP payload and provides a secure connection between two end points. The software only supports transport mode.

Tunnel mode encapsulates the entire IP packet and provides a secure tunnel. This software does not support tunnel mode.

The default is transport mode.

**policy WORD<1-32>**

Specifies the policy ID.

**spi <1-4294967295>**

Specifies the security parameters index (SPI) value, which is a unique value. SPI is a tag IPsec adds to the IP header. The tag enables the system that receives the IP packet to determine under which security association to process the received packet. For IPsec to function, each peer must have the same SPI value configured on both peers for a particular policy.

**WORD<1-32>**

Specifies the security association.

**WORD<1-32>**

Specifies the security association and creates the security association.

## Default

None

## Command Mode

Global Configuration

## ipv6 alternative-route

---

Enable IPv6 alternative route.

## Syntax

- **default ipv6 alternative-route**
- **ipv6 alternative-route**
- **no ipv6 alternative-route**

## Default

The default is enabled.

## Command Mode

Global Configuration

## ipv6 autoconfig

---

Enable or disable IPv6 autoconfiguration.

## Syntax

- **ipv6 autoconfig**

## Default

The default is disabled.

## Command Mode

Global Configuration

## ipv6 dhcp-relay fwd-path

---

Create the forwarding path from the client to the server.

## Syntax

- **default ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255>**
- **ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255>**
- **ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> enable**
- **no ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255>**
- **no ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> enable**

## Command Parameters

**enable**

Enables the forwarding path to the server.

**WORD<0-255>**

Configures the forwarding path from the client to the server. The first WORD<0-255> is the IP address configured on an interface (a locally configured IP address) to forward or relay BootP or DHCP. This address is the relay agent. The relay can be a VRRP address.

**WORD<0-255>**

The second WORD<0-255> is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network the system generates an error because IPv6 does not include broadcast.

## Default

The default is disabled.

## Command Mode

Global Configuration

## ipv6 ecmp

---

IPv6 ECMP configuration.

## Syntax

- **default ipv6 ecmp enable**
- **default ipv6 ecmp max-path**
- **ipv6 ecmp enable**
- **ipv6 ecmp max-path <ECMP-Paths>**
- **no ipv6 ecmp enable**

## Command Parameters

**enable**

Enables IPv6 ECMP globally.

**max-path <ECMP-Paths>**

Specifies the maximum number of ECMP paths. Different hardware platforms can support a different number of ECMP paths. For more information on the maximum number of ECMP paths supported on the switch, see the scaling information in [VSP 8600 Release Notes](#).

## Default

Disabled

## Command Mode

Global Configuration

### ipv6 fhs dhcp-guard enable

---

Enable DHCP-guard globally.

#### Syntax

- **default ipv6 fhs dhcp-guard enable**
- **ipv6 fhs dhcp-guard enable**
- **no ipv6 fhs dhcp-guard enable**

#### Default

The default is disabled

## Command Mode

Global Configuration

### ipv6 fhs dhcp-guard policy

---

Configure DHCP-guard policy.

#### Syntax

- **ipv6 fhs dhcp-guard policy WORD<1-64>**
- **no ipv6 fhs dhcp-guard policy WORD<1-64>**

#### Command Parameters

**WORD<1-64>**

Specifies the policy name.

#### Default

None

## Command Mode

Global Configuration

### ipv6 fhs enable

---

Enable First Hop Security (FHS) globally.

## Syntax

- **default ipv6 fhs enable**
- **ipv6 fhs enable**
- **no ipv6 fhs enable**

## Default

The default is disabled

## Command Mode

Global Configuration

## ipv6 fhs ipv6-access-list

---

Create an FHS IP access list or add IP prefixes to an existing IP access list.

## Syntax

- **default ipv6 fhs ipv6-access-list [WORD<1-64>] [WORD<0-46>] [ge|le|mode]**
- **ipv6 fhs ipv6-access-list [WORD<1-64>] [WORD<0-46>] [ge<0-128>] [le<0-128>] [mode <allow | deny>]**
- **no ipv6 fhs ipv6-access-list [WORD<1-64>] [WORD<0-46>]**

## Command Parameters

### ge <0-128>

Specifies the minimum IPv6 mask length. By default, the value is equal to the configured prefix length.

### le <0-128>

Specifies the maximum IPv6 mask length. By default, the value is equal to the configured prefix length.

### mode <allow | deny>

Specifies the access mode. By default, the value is allow.

### WORD<0-46>

Specifies the IPv6 address or the prefix length to be added to the IP access list.

### WORD<1-64>

Specifies the IP access list name.

## Default

None

## Command Mode

Global Configuration

### ipv6 fhs mac-access-list

---

Create an FHS MAC access list or add MAC addresses to an existing MAC access list.

#### Syntax

- **default ipv6 fhs mac-access-list WORD<1-64> <0x00:0x00:0x00:0x00:0x00:0x00> [mode]**
- **ipv6 fhs mac-access-list WORD<1-64> <0x00:0x00:0x00:0x00:0x00:0x00> [mode <allow | deny>]**
- **no ipv6 fhs mac-access-list WORD<1-64> <0x00:0x00:0x00:0x00:0x00:0x00>**

#### Command Parameters

0x00:0x00:0x00:0x00:0x00:0x00

Specifies the MAC address to be added or deleted.

mode <allow | deny>

Specifies the access mode. By default, the value is allow.

WORD<1-64>

Specifies the MAC access list name.

#### Default

None

## Command Mode

Global Configuration

### ipv6 fhs nd-inspection enable (globally)

---

Enables neighbor discovery (ND) inspection globally.

#### Syntax

- **default ipv6 fhs nd-inspection enable**
- **ipv6 fhs nd-inspection enable**
- **no ipv6 fhs nd-inspection enable**

#### Default

The default is disabled.

## Command Mode

Global Configuration

### ipv6 fhs ra-guard enable

---

Enable RA Guard globally.

#### Syntax

- **default ipv6 fhs ra-guard enable**
- **ipv6 fhs ra-guard enable**
- **no ipv6 fhs ra-guard enable**

#### Default

None

## Command Mode

Global Configuration

### ipv6 fhs ra-guard policy

---

Create the RA Guard policy.

#### Syntax

- **ipv6 fhs ra-guard policy WORD<1-64>**
- **no ipv6 fhs ra-guard policy WORD<1-64>**

#### Command Parameters

**WORD<1-64>**

Specifies the name of the RA Guard policy to be created or deleted.

#### Default

None

## Command Mode

Global Configuration



## ipv6 fhs snooping static-binding

---

Enables IPv6 snooping globally. This command enables learning SBT entries on all the VLANs where IPv6 DHCP Snooping is configured. The no form of this command can be used only for deleting static SBT entries.

### Syntax

- **ipv6 fhs snooping static-binding ipv6-address WORD<0-46> vlan <1-4059> mac-address <0x00:0x00:0x00:0x00:0x00:0x00> port {slot/port[/sub-port]}**
- **no ipv6 fhs snooping static-binding ipv6-address WORD<0-46> vlan <1-4059>**

### Command Parameters

**ipv6-address WORD<0-46>**

Specifies the IPv6 address of the binding entry.

**mac-address <0x00:0x00:0x00:0x00:0x00:0x00>**

Specifies the MAC address of the binding entry.

**port {slot/port[/sub-port]}**

Specifies the port of the binding entry.

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

Global Configuration

## ipv6 forwarding (globally)

---

Configure IPv6 forwarding.

## Syntax

- `default ipv6 forwarding`
- `ipv6 forwarding`
- `no ipv6 forwarding`

## Default

By default, forwarding is globally enabled.

## Command Mode

Global Configuration

## ipv6 hop-limit

---

Insert a value into the hop-limit field of the IPv6 header.

## Syntax

- `default ipv6 hop-limit <0-255>`
- `ipv6 hop-limit <0-255>`

## Command Parameters

`<0-255>`

Inserts a value into the hop-limit field of IPv6 header in the range of 0 to 255.

## Default

The default hop limit is 64.

## Command Mode

Global Configuration

## ipv6 icmp addr-unreach

---

Enables or disables ICMP network address unreachable messages.

## Syntax

- `default ipv6 icmp addr-unreach`
- `ipv6 icmp addr-unreach`
- `no ipv6 icmp addr-unreach`

## Default

The default is enabled.

## Command Mode

Global Configuration

# ipv6 icmp echo multicast-request (globally)

---

Enables or disables the processing of IPv6 ICMP messages sent to a multicast address globally.

## Syntax

- **default ipv6 icmp echo multicast-request**
- **ipv6 icmp echo multicast-request**
- **no ipv6 icmp echo multicast-request**

## Command Parameters

### echo multicast-request

Enables or disables the processing of IPv6 ICMP messages sent to a multicast address globally.  
The default value is enabled.

## Default

The default is enabled.

## Command Mode

Global Configuration

# ipv6 icmp drop-fragments

---

Enable Internet Control Message Protocol (ICMP) redirect and unreachable messages. The system inspects each incoming IPv6 ICMP packet to determine if it should drop or forward it.

## Syntax

- **ipv6 icmp drop-fragments**
- **default ipv6 icmp drop-fragments**
- **no ipv6 icmp drop-fragments**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipv6 icmp error-interval

---

Configure the interval (in milliseconds) for sending ICMPv6 error messages.

### Syntax

- **default ipv6 icmp error-interval**
- **ipv6 icmp error-interval <0-2147483647>**

### Command Parameters

<1-2147483647>

Configures the interval (in milliseconds) for sending ICMPv6 error messages. An entry of 0 seconds results in no sent ICMPv6 error messages.

### Default

The default error interval is 1000.

## Command Mode

Global Configuration

## ipv6 icmp error-quota

---

Configure the number of Internet Control Message Protocol (ICMP) error messages that can be sent during the ICMP error interval.

### Syntax

- **default ipv6 icmp error-quota**
- **ipv6 icmp error-quota <0-2000000>**

### Command Parameters

<0-2000000>

Configures the number of internet Control Message Protocol (ICMP) error messages that the system can send during the ICMP error interval. A value of zero instructs the system not to send any ICMP error messages.

## Default

The default error quota is 50.

## Command Mode

Global Configuration

---

## ipv6 icmp port-unreach

Enables or disables ICMP port unreachable messages.

## Syntax

- **default ipv6 icmp port-unreach**
- **ipv6 icmp port-unreach**
- **no ipv6 icmp port-unreach**

## Default

The default is enabled.

## Command Mode

Global Configuration

---

## ipv6 icmp unreachable-msg

Enable Internet Control Message Protocol (ICMP) network unreachable messages.

## Syntax

- **default ipv6 icmp unreachable-msg**
- **ipv6 icmp unreachable-msg**
- **no ipv6 icmp unreachable-msg**

## Default

By default ICMP network unreachable messages are disabled.

## Command Mode

Global Configuration

### ipv6 interface address <IPv6addr/prefixlen>

---

Create CLIPv6 interface and associates it with the given IPv6 address.

#### Syntax

- **ipv6 interface address <IPv6addr/prefixlen>**
- **no ipv6 interface address <IPv6address/prefixlen>**

#### Default

None

## Command Mode

Global Configuration

### ipv6 max-routes-trap

---

Enables SNMP trap generation after the maximum number of IPv6 routes are reached.

#### Syntax

- **default ipv6 max-routes-trap enable**
- **ipv6 max-routes-trap enable**
- **no ipv6 max-routes-trap enable**

#### Default

The default is enabled.

## Command Mode

Global Configuration

### ipv6 mld generate-log

---

Enable MLD log status

#### Syntax

- **default ipv6 mld generate-log**
- **ipv6 mld generate-log**

- `no ipv6 mld generate-log`

## Default

None

## Command Mode

Global Configuration

## ipv6 mld generate-trap

---

Enable MLD traps generation

## Syntax

- `default ipv6 mld generate-trap`
- `ipv6 mld generate-trap`
- `no ipv6 mld generate-trap`

## Default

None

## Command Mode

Global Configuration

## ipv6 mroute stats enable

---

Enable collection of IPv6 multicast route statistics

## Syntax

- `default ipv6 mroute stats enable`
- `ipv6 mroute stats enable`
- `no ipv6 mroute stats enable`

## Default

The default is enabled.

## Command Mode

Global Configuration

---

## ipv6 neighbor

---

Commands to configure IPv6 neighbors globally.

### Syntax

- **ipv6 neighbor WORD<0-128> port {slot/port[/sub-port]} mac 0x00:0x00:0x00:0x00:0x00:0x00 vlan <1-4059>**
- **no ipv6 neighbor WORD<0-128> port {slot/port[/sub-port]}**
- **no ipv6 neighbor WORD<0-128> vlan <1-4059>**

### Command Parameters

**mac 0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC address.

**port {slot/port[/sub-port]}**

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**WORD<0-128>**

IPv6 address in hex colon format.

### Default

None

### Command Mode

Global Configuration

---

## ipv6 pim disc-data-timeout

---

Configure the timeout to discard data.

### Syntax

- **default ipv6 pim disc-data-timeout**
- **ipv6 pim disc-data-timeout <5-65535>**



## Command Parameters

<5-65535>

Specifies the duration in seconds to discard data until the switch receives the join message from the rendezvous point (RP). An IP multicast discard record is created after a register packet is sent, until the timer expires or the switch receives a join message.

## Default

The default is 60.

## Command Mode

Global Configuration

---

## ipv6 pim enable

Enable PIM globally on the switch.

## Syntax

- **default ipv6 pim enable**
- **ipv6 pim enable**
- **no ipv6 pim enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## ipv6 pim fwd-cache-timeout

Configure the forward cache timeout.

## Syntax

- **default ipv6 pim fwd-cache-timeout**
- **ipv6 pim fwd-cache-timeout <10-86400>**

## Command Parameters

<10-86400>

Specifies the forward cache timeout value.

## Default

The default is 210.

## Command Mode

Global Configuration

# ipv6 pim join-prune-interval

---

Configure the interval for join and prune messages.

## Syntax

- **default ipv6 pim join-prune-interval**
- **ipv6 pim join-prune-interval <1-18724>**

## Command Parameters

<1-18724>

Specifies the duration in seconds before the PIM router sends out the next join or prune message to its upstream neighbors.

## Default

The default is 60.

## Command Mode

Global Configuration

# ipv6 pim mode

---

Configure the PIM mode.

## Syntax

- **default ipv6 pim mode**
- **ipv6 pim mode sparse**
- **ipv6 pim mode ssm**

## Command Parameters

**sparse**

Configures the PIM mode on the switch

**ssm**

Configures the PIM mode on the switch

## Default

The default is sparse.

## Command Mode

Global Configuration

---

## ipv6 pim spt-infinite-threshold

Enable PIM Infinite Threshold Policy for IPv6.

## Syntax

- **default ipv6 pim spt-infinite-threshold**
- **ipv6 pim spt-infinite-threshold**
- **no ipv6 pim spt-infinite-threshold**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## ipv6 pim register-suppression-timeout

Specify how long to suppress register messages.

## Syntax

- **default ipv6 pim register-suppression-timeout**
- **ipv6 pim register-suppression-timeout <10-65535>**

## Command Parameters

<10-65535>

Specifies the duration in seconds the designated router (DR) suppresses sending registers to the RP. The timer starts after the DR receives a register-stop message from the RP.

## Default

The default is 60.

## Command Mode

Global Configuration

## ipv6 pim static-rp

---

Enable IPv6 static RP function.

## Syntax

- **default ipv6 pim static-rp**
- **ipv6 pim static-rp**
- **ipv6 pim static-rp WORD<0-255> WORD<0-255>**
- **no ipv6 pim static-rp**

## Command Parameters

**WORD<0-255>**

Specifies the IPv6 address and address mask of the multicast group. When combined, the IPv6 address and address mask identify the range of the multicast addresses that the RP handles.

## Default

The default is disabled.

## Command Mode

Global Configuration

## ipv6 pim unicast-route-change-timeout

---

Configure the polling interval for the routing table manager (RTM).

## Syntax

- **default ipv6 pim unicast-route-change-timeout**
- **ipv6 pim unicast-route-change-timeout <2-65535>**

## Command Parameters

<2-65535>

Specifies the duration in seconds the switch polls the RTM for unicast routing information updates for PIM.

## Default

The default is 5.

## Command Mode

Global Configuration

## ipv6 prefix-list

---

Use prefix lists to allow or deny specific route updates. A prefix list policy specifies route prefixes to match. When there is a match, the route is used. Configure a prefix list and apply the list to a route policy.

## Syntax

- **ipv6 prefix-list WORD<1-64> name WORD<1-64>**
- **ipv6 prefix-list WORD<1-64> WORD<1-256> ge <0- 128>**
- **ipv6 prefix-list WORD<1-64> WORD<1-256> id <1-2147483647>**
- **ipv6 prefix-list WORD<1-64> WORD<1-256> le <0-128>**
- **no ipv6 prefix-list WORD<1-64> [WORD<1-256>]**

## Command Parameters

**ge <0-128>**

Specifies the minimum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

**id <1-2147483647>**

Specifies the prefix list ID.

**le <0-128>**

Specifies the maximum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

**name WORD<1-64>**

Renames the specified prefix list. The name length is from 1 to 64 characters.

**WORD<1-256>**

Specifies the IPv6 address and length.

**WORD<1-64>**

Adds a prefix entry to the prefix list. WORD<1-64> is the prefix-list name. WORD<1-256> is the IPv6 address and length. <ge|le><0- 128> is the minimum and maximum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

## Default

None

## Command Mode

Global Configuration

## ipv6 route

Configure a static route to destination IPv6 address prefixes. Use this command to:

- Create static routes for data traffic in the GRT for any platform.
- Create static routes for management purposes on VSP 8600 Series:
  - Use the default VRF context to configure static routes in the GRT for the inband VLAN or loopback interface.

## Syntax

- **default ipv6 route WORD<0-46>**
- **default ipv6 route WORD<0-46> enable [next-hop WORD<0-46>] [port {slot/port[/sub-port]}] [tunnel <1-2000>] [vlan <1-4059>]**
- **default ipv6 route WORD<0-46> preference [next-hop WORD<0-46>] [port {slot/port[/sub-port]}] [tunnel <1-2000>] [vlan <1-4059>]**
- **default ipv6 route WORD<0-46> name [next-hop WORD<0-46>] [port {slot/port[/sub-port]}] [tunnel <1-2000>] [vlan <1-4059>]**
- **ipv6 route WORD<0-46> cost <1-65535> [next-hop WORD<0-46>] [port {slot/port[/sub-port]}] [preference <1-255>] [tunnel <1-2000>] [vlan <1-4059>]**
- **ipv6 route WORD<0-46> enable [next-hop WORD<0-46>] [port {slot/port[/sub-port]}] [tunnel <1-2000>] [vlan <1-4059>]**
- **ipv6 route WORD<0-46> preference <1-255> [next-hop WORD<0-46>] [port {slot/port[/sub-port]}] [tunnel <1-2000>] [vlan <1-4059>]**
- **no ipv6 route WORD<0-46> [enable] [next-hop WORD<0-46>] [port {slot/port[/sub-port]}] [tunnel <1-2000>] [vlan <1-4059>]**

## Command Parameters

**cost <1-65535>**

Specifies the cost or distance ratio to reach the destination for this node. The default cost is 1.

**enable**

Enables the static route on the port. The default state for a new static route is enable.

**next-hop WORD<0-46>**

Specifies the IPv6 address of the next hop on this route. You do not need to specify the next hop if the devices directly connect to one another. Configure the next hop if the two nodes do not share the same network prefix but reside on the same link.

**port {slot/port[/sub-port]}**

Specifies the port to which this entry applies. You must specify the port if the next hop is a link-local address.

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**preference <1-255>**

Specifies the routing preference of the destination IPv6 address. The default preference is 5.

**tunnel <1-2000>**

Specifies the tunnel to which this entry applies.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**WORD<0-46>**

Specifies the IPv6 destination network address.

## Default

The default state for a new static route is enable.

## Command Mode

Global Configuration

## Usage Guidelines

The *name* parameter is not supported on VSP 8600 Series.

VSP 8600 Series uses the routing stack to create static routes for data traffic as well as management purposes. For all other platforms, static routes for the management OOB and management VLAN, if supported, must use the Segmented Management Instance. For more information, see [VOSS User Guide](#). The management CLIP can use the Segmented Management Instance or routes in the associated VRF routing table manager (RTM).

## ipv6 route bfd

Configure an IPv6 static route for Bidirectional Forwarding Detection (BFD).

## Syntax

- `default ipv6 route bfd WORD<0-128>`
- `default ipv6 route bfd WORD<0-128> port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `default ipv6 route bfd WORD<0-128> vlan <1-4094>`
- `ipv6 route bfd WORD<0-128>`
- `ipv6 route bfd WORD<0-128> port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `ipv6 route bfd WORD<0-128> vlan <1-4094>`
- `no ipv6 route bfd WORD<0-128>`
- `no ipv6 route bfd WORD<0-128> port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `no ipv6 route bfd WORD<0-128> vlan <1-4094>`

## Command Parameters

**WORD<0-128>**

Specifies the BFD static route IPv6 address.

**port**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

**vlan**

Specifies the VLAN ID for the BFD IPv6 static route.

## Command Mode

Global Configuration

## Usage Guidelines

BFD for IPv6 is a demonstration feature on some products. For more information, see [VOSS Feature Support Matrix](#)

## ipv6 route preference protocol

---

Specifies the route preference.

## Syntax

- `default ipv6 route preference protocol ospfv3-extern1`
- `default ipv6 route preference protocol ospfv3-extern2`



- `default ipv6 route preference protocol ospfv3-inter`
- `default ipv6 route preference protocol ospfv3-intra`
- `default ipv6 route preference protocol spbm-level1`
- `default ipv6 route preference protocol static`
- `ipv6 route preference protocol ospfv3-extern1`
- `ipv6 route preference protocol ospfv3-extern2`
- `ipv6 route preference protocol ospfv3-inter`
- `ipv6 route preference protocol ospfv3-intra`
- `ipv6 route preference protocol spbm-level1`
- `ipv6 route preference protocol static`

## Command Parameters

{static | ospfv3-intra | ospfv3-inter | ospfv3-extern1 | ospfv3-extern2 | spbm-level1}

Specifies the protocol type.

<0-255>

Specifies the default preference value for the given protocol.

## Default

None

## Command Mode

Global Configuration

## ipv6 route static

---

Enable static routes globally. If you disable static routes globally, the system removes all enabled static routes from the RTM and does not add new static routes to the RTM.

## Syntax

- `default ipv6 route static enable`
- `ipv6 route static enable`
- `no ipv6 route static enable`

## Command Parameters

**enable**

Enables the static routes globally.

**static**

Modifies IPv6 static route parameters.

## Default

The default is enabled.

## Command Mode

Global Configuration

## Usage Guidelines

VSP 8600 Series uses the routing stack to create static routes for data traffic as well as management purposes. For all other platforms, static routes for the management OOB and management VLAN, if supported, must use the Segmented Management Instance. For more information, see [VOSS User Guide](#). The management CLIP can use the Segmented Management Instance or routes in the associated VRF routing table manager (RTM).

## ipv6 source-route

---

Enables IPv6 source routing globally.

### Syntax

- **default ipv6 source-route**
- **ipv6 source-route**
- **no ipv6 source-route**

### Default

Disabled

### Command Mode

Global Configuration

## ipv6 tunnel

---

Configure a tunnel for IPv6 VLANs or brouter ports to communicate through an IPv4 network.

### Syntax

- **default ipv6 tunnel <1-2000>**
- **default ipv6 tunnel <1-2000> hop-limit**
- **ipv6 tunnel <1-2000> hop-limit <0-255>**
- **ipv6 tunnel <1-2000> source {A.B.C.D} address WORD<0-46> destination {A.B.C.D}**
- **no ipv6 tunnel <1-2000>**

## Command Parameters

**<1-2000>**

Specifies the tunnel ID.

**address WORD<0-46>**

Specifies the IPv6 address and length for the local VLAN or brouter port.

**destination{A.B.C.D}**

Configures the address of the remote endpoint of the tunnel.

**hop-limit <0-255>**

Configures the maximum number of hops in the tunnel.

**source {A.B.C.D}**

Configures the address of the local endpoint of the tunnel, or 0.0.0.0 (for IPv4) or :: (for IPv6) if the device is free to choose its addresses at tunnel establishment.

## Default

The default hop-limit is 255.

## Command Mode

Global Configuration

## i-sid

---

Service Instance Identifier commands.

## Syntax

- **default i-sid**
- **i-sid <0-16777215>**
- **i-sid name <0-16777215> WORD<0-64>**
- **no i-sid**
- **no i-sid <1-16777215>**
- **no i-sid name <1-16777215>**
- **i-sid <1-16777215> elan-transparent**
- **i-sid <1-16777215> elan**

## Command Parameters

**<0-16777215>**

Specifies the service instance identifier (I-SID).

**name WORD<0-64>**

Specifies the I-SID name.

By default, the service is named ISID-x, where x correlates to the I-SID number of the service.

### **elan-transparent**

Specifies the elan-transparent (Transparent UNI) based service.

### **elan**

Specifies the elan (Switched UNI) based service.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

The *name* parameter is not supported on VSP 8600 Series or XA1400 Series.

## i-sid (T-UNI based)

---

Create a Transparent UNI based service instance identifier (I-SID).

## Syntax

- **i-sid <1-16777215> elan-transparent**
- **no i-sid <1-16777215>**

## Command Parameters

**<1-16777215>**

Specifies the Transparent UNI based service instance identifier (I-SID).

### **elan-transparent**

Specifies the elan-transparent (Transparent UNI) based service.

## Default

None

## Command Mode

Global Configuration

## i-sid mac-address-entry

---

Service Instance Identifier FDB commands.

## Syntax

- **i-sid mac-address-entry <1-16777215> flush**
- **i-sid mac-address-entry <1-16777215> sync**

## Command Parameters

**<1-16777215>**

Specifies the FDB based service instance identifier (I-SID).

**flush**

Flushes MAC address on an i-sid

**sync**

Sync forwarding database with the other aggregation switch

## Default

None

## Command Mode

Global Configuration

## lACP (globally)

---

Configure Link Aggregation Control Protocol (LACP) parameters globally. When the LACP system priority is set globally, it applies to all LACP-enabled aggregators and ports.

## Syntax

- **default lACP**
- **default lACP aggr-wait-time**
- **default lACP enable**
- **default lACP fast-periodic-time**
- **default lACP slow-periodic-time**
- **default lACP system-priority**
- **default lACP timeout-scale**
- **lACP aggr-wait-time <200-2000>**
- **lACP enable**
- **lACP fast-periodic-time <200-20000>**
- **lACP slow-periodic-time <10000-30000>**
- **lACP smlt-sys-id 0x00:0x00:0x00:0x00:0x00:0x00**
- **lACP system-priority <0-65535>**
- **lACP timeout-scale <2-10>**

- **no lacp**
- **no lacp enable**

## Command Parameters

**aggr-wait-time <200-2000>**

Sets the aggregation wait time (in milliseconds) globally. The default value is 2000.

**enable**

Enables the Link Aggregation Control Protocol (LACP) globally.

**fast-periodic-time <200-20000>**

Sets the fast-periodic time (in milliseconds) globally. The default is 20000 ms.

**slow-periodic-time <10000-30000>**

Sets the slow periodic time globally. The default value is 1000 ms.

**smlt-sys-id <0x00:0x00:0x00:0x00:0x00:0x00>**

Sets the LACP system ID globally. Enter a MAC address in the following format:  
0x00:0x00:0x00:0x00:0x00:0x00.

**system-priority <0-65535>**

Sets the global LACP system priority. The default value is 32768.

**timeout-scale <2-10>**

Sets the timeout scale globally. The default value is 3.

## Default

The default is disabled.

## Command Mode

Global Configuration

## license-grant

---

Grant license to IO slot.

## Syntax

- **license-grant {slot[-slot][,...]}**
- **no license-grant {slot[-slot][,...]}**

## Command Parameters

**{slot[-slot][,...]}**

Specifies the slot. Valid IO slots are 1-8.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information, see [VOSS User Guide](#).

## link-flap-detect

---

Configure link flap detection to control link state changes on a physical port.

## Syntax

- **default link-flap-detect**
- **default link-flap-detect auto-port-down**
- **default link-flap-detect frequency**
- **default link-flap-detect interval**
- **default link-flap-detect send-trap**
- **link-flap-detect auto-port-down**
- **link-flap-detect frequency <1-9999>**
- **link-flap-detect interval <2-600>**
- **link-flap-detect send-trap**
- **no link-flap-detect auto-port-down**
- **no link-flap-detect send-trap**

## Command Parameters

### auto-port-down

Activates automatic disabling of the port if the link-flap threshold is exceeded. The default is disabled.

### frequency <1-9999>

Configures the number of changes that are allowed during the time specified by the interval command. The default is 20.

### interval <2-600>

Configures the link-flap-detect interval in seconds. The default is 60.

### send-trap

Activates sending traps. The default is enabled.

## Default

None

## Command Mode

Global Configuration

# link-state group

---

Configures the Link-state tracking (LST) group.

## Syntax

- **default link-state group <1-48> enable**
- **link-state group <1-48> downstream interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **link-state group <1-48> downstream mlt <1-512>**
- **link-state group <1-48> enable**
- **link-state group <1-48> upstream interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **link-state group <1-48> upstream mlt <1-512>**
- **no link-state group <1-48> enable**

## Command Parameters

**<1-48>**

Specifies the link-state group ID.

**downstream**

Specifies a downstream interface for the LST group.

**enable**

Enables the command.

**interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Specifies the slot and port for the upstream or downstream LST group.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mlt <1-512>**

Specifies an MLT ID for the upstream or downstream LST group.

**upstream**

Specifies an upstream interface for the LST group.



## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Link-state tracking (LST) is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## lldp tx-hold-multiplier

---

Configure the time to live value in seconds.

## Syntax

- **lldp tx-hold-multiplier <2-10>**

## Command Parameters

<2-10>

Specifies the Tx hold multiplier in seconds.

## Default

Default value is 4 seconds.

## Command Mode

Global Configuration

## lldp tx-interval

---

Configure the interval in seconds in which LLDP frames are transmitted.

## Syntax

- **lldp tx-interval <5-32768>**
- **lldp tx-interval <5-32768> tx-hold-multiplier <2-10>**

## Command Parameters

**tx-hold-multiplier <2-10>**

Specifies the Tx hold multiplier in seconds.

**<5-32768>**

Specifies the global Tx interval in seconds.

## Default

Default value is 30 seconds.

## Command Mode

Global Configuration

## lldp vendor-specific

---

Configure or remove LLDP vendor-specific information on the call server and file server.

## Syntax

- **lldp vendor-specific {call server <1-8> <A.B.C.D> | file server <1-4> <A.B.C.D>}**
- **no lldp vendor-specific {call server <1-8> | file server <1-4> }**

## Command Parameters

**call server <1-8> <A.B.C.D>**

Specifies the call server number and its IP address.

**file server <1-4> <A.B.C.D>**

Specifies the file server number and its IP address.

## Default

None

## Command Mode

Global Configuration

## load-license

---

Load a license file to unlock the licensed features.

## Syntax

- **load-license WORD<0-63>**

## Command Parameters

**WORD<0-63>**

Specifies the license filename.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

The *WORD<0-63>* parameter is only supported on 5420 Series, 5520 Series, VSP 8600 Series, or XA1400 Series.

---

## logging level

---

Determine what messages the system records in the log.

## Syntax

- **default logging level <0-4>**
- **logging level <0-4>**

## Command Parameters

**level <0-4>**

Shows and configures the logging level. The level is one of the following values:

- 0 = Information; all messages are recorded.
- 1 = Warning; only warning and more serious messages are recorded.
- 2 = Error; only error and more serious messages are recorded.
- 3 = Manufacturing; this parameter is not available for customer use.
- 4 = Fatal; only fatal messages are recorded.

## Default

None

## Command Mode

Global Configuration

### logging screen

---

Configure the system to display log messages on screen.

#### Syntax

- **default logging screen**
- **logging screen**
- **no logging screen**

#### Command Parameters

**screen**

Configures the system to display the log messages on screen.

#### Default

None

## Command Mode

Global Configuration

### logging transferFile

---

Configure the remote host address for log transfer. The system transfers the current log file to a remote host when the log file size reaches the configured maximum size.

#### Syntax

- **logging transferFile <1-10> address {A.B.C.D}**
- **no logging transferFile <1-10> address {A.B.C.D}**

#### Command Parameters

**<1-10>**

Specifies the file ID to transfer.

**address <A.B.C.D>**

Specifies the IP address of the host to which to transfer the log file. The remote host must be reachable or the configuration fails.

## Default

None

## Command Mode

Global Configuration

## logging transferFile filename-prefix

---

Create the filename on the remote host. The system transfers the current log file to a remote host when the log file size reaches the configured maximum size.

## Syntax

- **default logging transferFile <1-10> filename-prefix**
- **logging transferFile <1-10> filename-prefix WORD<0-200>**

## Command Parameters

<1-10>

Specifies the file ID to transfer.

filename-prefix WORD<0-2005>

Specifies the name of the file on the remote host. If you do not configure a name, the current log file name is the default.



### Important

If you configure this option, the previously transferred log file is overwritten on the remote server. As a best practice, do not configure a name.

## Default

None

## Command Mode

Global Configuration

## logging write

---

Write to the log file automatically created by the system.

## Syntax

- **logging write WORD<1-1536>**

## Command Parameters

**write WORD<1-1536>**

Writes the designated string to the log file. WORD<1-1536> is the string or command that you append to the log file. If the string contains spaces, you must enclose the string in quotation marks ("").

## Default

None

## Command Mode

Global Configuration

## logical-intf isis

---

Create a logical IS-IS interface.

## Syntax

- **logical-intf isis <1-255> dest-ip {A.B.C.D} name WORD<1-64> mtu <mtu\_value>**
- **logical-intf isis <1-255> vid {vlan-id[-vlan-id][, ...]} primary-vid <2-4059> mlt PT\_MLT<1-512> mtu <mtu\_value>**
- **logical-intf isis <1-255> vid {vlan-id[-vlan-id][, ...]} primary-vid <2-4059> port {slot/port[/sub-port]} name WORD<1-64> mtu <mtu\_value>**
- **no logical-intf isis <1-255>**

## Command Parameters

**<1-255>**

Specifies the ISIS logical interface ID.

**dest-ip {A.B.C.D}**

Specifies the destination IP address for the logical interface.

**mlt PT\_MLT<750-9000>**

Specifies the MLT ID that the logical interface is connected to in an Layer 2 network.

**name WORD<1-64>**

Specifies the administratively-assigned name of this logical interface, which can be up to 64 characters.

**mtu <mtu\_value>**

Specifies the Maximum Transmission Unit (MTU) size for each packet. Different hardware platforms support different MTU ranges. Use the CLI Help to see the available range for the switch.

**Note**

Exception: only supported on XA1400 Series.

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**primary-vid** <2-4059>

Specifies the primary tunnel VLAN ID associated with this Layer 2 IS-IS logical interface.

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

**vid** {vlan-id [-vlan-id] [, ...]}

Specifies the list of VLANs that are associated with this logical interface.

The VLAN ID is in one of the following formats: A single VLAN ID (vlan-id), a range of VLAN IDs [(vlan-id)-(vlan-id)] or a series of VLAN IDs (vlan-id, vlan-id, vlan-id).

## Default

Default MTU value is 1950.

## Command Mode

Global Configuration

## login-message

---

Change the login prompt for CLI.

## Syntax

- **default login-message**
- **login-message WORD<1-1513>**
- **no login-message**

## Command Parameters

**WORD<1-1513>**

Changes the CLI logon prompt. WORD<1-1513> is an American Standard Code for Information Interchange (ASCII) string from 1-1513 characters.

## Default

The default is Login.

## Command Mode

Global Configuration

---

## mac-address-table

Configure MAC address table settings.

## Syntax

- **default mac-address-table aging-time**
- **mac-address-table aging-time <10-1000000>**

## Command Parameters

**aging-time <10-1000000>**

Configure MAC address table aging time.

## Default

The default is 600.

## Command Mode

Global Configuration

---

## macsec clear-stats

Clear MACsec statistics globally or for a specific port.

## Syntax

- **macsec clear-stats**
- **macsec clear-stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## macsec connectivity-association (globally)

---

Create and configure a connectivity-association (CA).



### Note

Configure a CA name in multiples of 4 characters (4 bytes). If the total number of characters in a CA name is not a multiple of 4, it can create interoperability issues with ExtremeXOS products.

## Syntax

- **macsec connectivity-association WORD<5-15> connectivity-association-key WORD<10-64> [key-parity {even | odd}]**
- **no macsec connectivity-association WORD<5-15> connectivity-association-key WORD<10-32>**

## Command Parameters

### key-parity

Specifies Tx key parity using the following values:

- even — generates even-numbered keys
- odd — generates odd-numbered keys

If you do not specify a value for key-parity, the system defaults to 2 AN mode.



### Note

This parameter only applies to static MACsec configurations.

### WORD<10-64>

Specifies the connectivity-association key (CAK) value as a 32-character (128-bit) or a 64 character (256-bit) hexadecimal string.

### WORD<5-15>

Specifies a new connectivity-association name. It is a 15 character alphanumeric string.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## macsec mka clear-stats

Clear MACsec Key Agreement (MKA) statistics globally or for a specific port.

## Syntax

- **macsec mka clear-stats**
- **macsec mka clear-stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information, see [VOSS User Guide](#).

---

## macsec mka profile

Create a MACsec Key Agreement (MKA) profile in global configuration.

## Syntax

- **macsec mka profile WORD<1-16>**
- **no macsec mka profile WORD<1-16>**

## Command Parameters

WORD<1-16>

Specifies the MKA profile name. An MKA profile name can consist only of alphanumeric characters (0-9, A-Z, and a-z). The profile name is case sensitive.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information, see [VOSS User Guide](#).

## max-logins

---

Configure the number of supported rlogin sessions.

## Syntax

- **default max-logins**
- **max-logins <0-8>**

## Command Parameters

<0-8>

Configures the maximum number of inbound remote CLI logon sessions.

## Default

The default is 8.

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## mgmt clip

---

Specifies management CLIP instance CLI mode.

### Syntax

- **mgmt clip**
- **mgmt clip vrf WORD<1-16>**
- **no mgmt clip**

### Command Parameters

**vrf WORD<1-16>**

Associates the management CLIP with a specific VRF. If you do not specify a VRF, the management CLIP uses the GRT. You cannot use mgmtrouter as the VRF.

### Default

None

### Command Mode

Global Configuration

## mgmt convert-commit

---

Commits the new values configured for the IP address, VLAN, vrf, ports-tagged, ports-untagged, I-SID, or default gateway for a Management Instance.

### Syntax

- **mgmt convert-commit**

### Default

None

### Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to VSP 8600 Series.

## mgmt dhcp-client

---

Specifies a DHCP Client configuration for management interfaces.

### Syntax

- **mgmt dhcp-client {cycle | oob | vlan}**
- **no mgmt dhcp-client**

### Command Parameters

#### cycle

Specifies the DHCP Client to attempt to obtain an IP address on the In-Band VLAN management interface, then the Out-of-Band management interface. Cycle attempts until an IP address is obtained.

#### oob

Specifies the DHCP Client to obtain an IP address for the Out-of-Band management interface.

#### vlan

Specifies the DHCP Client to obtain an IP address for the In-Band VLAN management interface.

### Default

The DHCP Client for management interfaces is disabled.



#### Note

Exception: the DHCP Client is enabled by default in cycle mode when:

- The switch ships directly from manufacturing with VOSS Release 8.1.60 or later.

The primary and secondary configuration file is not on the switch.

The primary and secondary configuration file fail to load on the switch.

### Command Mode

Global Configuration

### Usage Guidelines

This command is not supported on VSP 8600 Series. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## mgmt oob

---

Specifies management Out-of-Band (OOB) instance CLI mode.

### Syntax

- **mgmt oob**
- **no mgmt oob**

### Command Parameters

None

### Default

None

### Command Mode

Global Configuration

### Usage Guidelines

This command is not supported on VSP 8600 Series or XA1400 Series. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## mgmt vlan

---

Specifies management VLAN instance CLI mode.

### Syntax

- **mgmt vlan**
- **mgmt vlan i-sid <1-16777215>**
- **mgmt vlan <1-4059>**
- **no mgmt vlan**

### Command Parameters

<1-4059>

Associates the management VLAN with an existing port-based VLAN.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags,

the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**i-sid <1-16777215>**

Specifies the I-SID to create a management VLAN instance on a DvR leaf.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## mirror-by-port

Use port mirroring to aid in diagnostic and security operations.

## Syntax

- **default mirror-by-port <1-479>**
- **default mirror-by-port <1-479> enable**
- **default mirror-by-port <1-479> mode**
- **default mirror-by-port mirror-port <1-479> {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **default mirror-by-port monitor-mlt <1-479> <1-512>**
- **default mirror-by-port monitor-port <1-479> {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} monitor-mlt <1-512>**
- **mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} monitor-mlt <1-512> enable**
- **mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} monitor-mlt <1-512> enable remote-mirror-vlan-id <1-4059>**
- **mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} monitor-mlt <1-512> mode both**
- **mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} monitor-mlt <1-512> mode rx**
- **mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} monitor-mlt <1-512> mode tx**

- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} monitor-mlt <1-512> remote-mirror-vlan-id <1-4059>`
- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} monitor-mlt <1-512> remote-mirror-vlan-id <1-4059> enable`
- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} out-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} out-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} enable`
- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} out-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} mode both`
- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} out-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} mode rx`
- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} out-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} mode tx`
- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} monitor-mlt <1-512> remote-mirror-vlan-id <1-4059>`
- `mirror-by-port <1-479> mode both`
- `mirror-by-port <1-479> mode rx`
- `mirror-by-port <1-479> mode tx`
- `mirror-by-port <1-479> enable`
- `mirror-by-port <1-479> in-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} { monitor-mlt <1-512>|out-port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `mirror-by-port mirror-port <1-479> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `mirror-by-port monitor-mlt <1-479> <1-512>`
- `mirror-by-port monitor-port <1-479> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `no mirror-by-port <1-479>`
- `no mirror-by-port <1-479> enable`
- `no mirror-by-port mirror-port <1-479> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `no mirror-by-port monitor-mlt <1-479> <1-512>`
- `no mirror-by-port monitor-port <1-479> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`



## Command Parameters

**<1-479>**

Specifies the mirror-by-port entry ID in the range of 1 to 479.

**enable**

Enables or disables a mirroring instance already created in the mirror-by-port table.

**in-port** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}* | **monitor-mlt** **<1-512>** | **out-port** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Creates a new mirror-by-port table entry.

- in-port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}* specifies the mirrored port.
- monitor-mlt **<1-512>** specifies the mirroring MLT ID from 1-512.
- out-port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}* specifies the mirroring port.

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mirror-port** **<1-479>** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Modifies the mirrored port. Before you can modify an existing entry, you must disable the entry: no mirror-by-port **<1-479>** enable.

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mode** **<both|tx|rx>**

Sets the mirroring mode. The default is rx. both mirrors both egress and ingress packets. tx mirrors egress packets. rx mirrors ingress packets.

**monitor-ip** **<1-479>** {A.B.C.D} [dscp **<0-63>**] [ttl **<2-255>**]

Creates a mirroring instance for Layer 3 mirroring. The destination must be an IP address {A.B.C.D}. The default DSCP is 0 and the default TTL is 255.

**monitor-isid-offset** **<1-1000>**

Specifies the offset ID that is mapped to the actual monitor I-SID where packets are mirrored. Monitor I-SID = base monitor I-SID + offset ID. The base monitor I-SID is 16776000.

**monitor-mlt** **<1-479>** **<1-512>**

Modifies the monitoring MLT; **<1-479>** **<1-512>** specifies the port mirroring entry id and the MLT ID. Before you can modify an existing entry, you must disable the entry: no mirror-by-port **<1-479>** enable .

**monitor-port** **<1-479>** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Modifies the monitoring ports. Before you can modify an existing entry, you must disable the entry: `no mirror-by-port <1-479> enable`.

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### **monitor-vlan <1-479> <1-4059>**

Modifies the monitoring VLAN. Before you can modify an existing entry, you must disable the entry: `no mirror-by-port <1-479> enable`.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

#### **qos <0-5>**

Specifies the Quality of Service (QoS) profiles for the system. Monitoring I-SID supports six different QoS levels, each QoS level can be configured individually. Default value is 1.

#### **remote-mirror-vlan-id <1-4059>**

Sets the remote mirror VLAN ID.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

The default DSCP is 0. The default TTL is 64.

## Command Mode

Global Configuration

## mlt

Configure MultiLink Trunking (MLT) to set up MLTs on the switch.

## Syntax

- **mlt <1-512>**
- **mlt <1-512> enable**
- **mlt <1-512> encapsulation dot1q**

- **mlt** <1-512> **name** WORD<0-20>
- **mlt** <1-512> **vlan** <1-4059>
- **mlt** <1-512>
- **mlt** <1-512> **private-vlan** {**isolated**|**promiscuous**|**trunk**}
- **no mlt** <1-512>
- **no mlt** <1-512> **encapsulation dot1q**
- **no mlt** <1-512> **name**
- **no mlt** <1-512> **private-vlan**
- **no mlt** <1-512> **vlan** <1-4059>

## Command Parameters

**<1-512>**

Specifies the MLT ID in the range of 1-512.

**enable**

Creates and enables a new MLT.

**encapsulation dot1q**

Sets encapsulation. dot1q enables trunking on the MLT.

**name <0-20>**

Changes the name for this MLT in the range of 0-20 characters.

**private-vlan {isolated|promiscuous|trunk}**

Specifies the private VLAN port type for this MLT.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

You cannot configure an MLT name that uses all numbers, for example, 222.

## mlt <1-512> member

---

Add ports to an MultiLink Trunking (MLT) link aggregation group (LAG) to add an existing VLAN to a link aggregation configuration.

### Syntax

- **mlt <1-512> member {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **mlt <1-512> member {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}  
vlan <1-4059>**
- **no mlt <1-512> member {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### <1-512>

Specifies the MLT ID in the range of 1 to 512.

#### vlan <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

Global Configuration

## monitor-by-isid

---

Create or modify a monitor based on the I-SID entry.

### Syntax

- **default monitor-by-isid <1-1000> enable**
- **monitor-by-isid <1-1000> egress-mlt <1-512>**

- **monitor-by-isid** <1-1000> **egress-ports** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **monitor-by-isid** <1-1000> **enable**
- **monitor-by-isid** <1-1000> **map-to-vid** <1-4093>
- **monitor-by-isid** <1-1000> **monitor-isid-offset** <1-1000> {egress-mlt <1-512> **egress-ports** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} **map-to-vid** <1-4093>}
- **no monitor-by-isid** <1-1000> **egress-mlt**
- **no monitor-by-isid** <1-1000> **egress-ports**
- **no monitor-by-isid** <1-1000> **enable**
- **no monitor-by-isid** <1-1000> **map-to-vid**

## Command Parameters

**<1-1000>**

Specifies the session ID.

**egress-mlt** <1-512>

Specifies the MLT to which the analyzers connect.

**egress-ports** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Specifies the port to which the analyzers connect.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**enable**

Enables monitoring for the specific I-SID entry.

**map-to-vid** <1-4093>

Maps the mirrored packet to a specified VLAN ID for analysis. This parameter is optional.



### Note

If you use the Extreme Integrated Application Hosting (IAH) port 1/s1 as the analyzer port on the monitoring BEB for remote mirroring, you must associate it to VLAN ID 4091.

**monitor-isid-offset** <1-1000>

Specifies the offset ID that is mapped to the actual monitor I-SID where packets are mirrored. Monitor I-SID = Base monitor I-SID + Offset ID. The base monitor I-SID is 16776000.

## Default

None

## Command Mode

Global Configuration

## monitor-statistics

---

Change monitor timer commands.

### Syntax

- **default monitor-statistics**
- **default monitor-statistics duration**
- **default monitor-statistics interval**
- **monitor-statistics duration <1-1800>**
- **monitor-statistics interval <1-600>**

### Command Parameters

**duration <1-1800>**

Change monitor time duration.

**interval <1-600>**

Change monitor time interval.

### Default

None

## Command Mode

Global Configuration

## monitor-statistics duration

---

Change monitor time duration.

### Syntax

- **monitor-statistics duration <1-1800>**

### Command Parameters

**<1-1800>**

Monitors statistics time duration in seconds.

## Default

None

## Command Mode

Global Configuration

---

## monitor-statistics interval

Change monitor time interval.

## Syntax

- **monitor-statistics interval <1-600>**

## Command Parameters

<1-600>

Monitor statistics time interval in seconds.

## Default

None

## Command Mode

Global Configuration

---

## multicast software-forwarding

Enables the IP multicast software forwarding feature. If you enable this feature, the system forwards the initial packets of an IP multicast data stream it receives and creates a corresponding hardware record for subsequent packets.

## Syntax

- **multicast software-forwarding**

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## no license

---

Revokes a license on the switch.

### Syntax

- **no license macsec**
- **no license premier**

### Command Parameters

#### macsec

Revokes the MACsec license.

#### premier

Revokes the Premier license.

### Default

None.

### Command Mode

Global Configuration

### Usage Guidelines

This command only applies to 5520 Series.

---

## ntp

---

Enable Network Time Protocol (NTP) globally.

### Syntax

- **default ntp**
- **no ntp**
- **ntp**

### Default

The default is disabled.

### Command Mode

Global Configuration



## ntp authentication-key

---

Creates an authentication key for Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA1) authentication

### Syntax

- **default ntp authentication-key <1-65534>**
- **default ntp authentication-key <1-65534> type**
- **no ntp authentication-key <1-65534>**
- **ntp authentication-key <1-65534> type <md5|sha1>**
- **ntp authentication-key <1-65534> WORD<0-20> type <md5|sha1>**
- **ntp authentication-key <1-65534> WORD<0-20>**

### Command Parameters

<1-65534>

Creates the key ID.

type <md5|sha1>

Specifies the type of authentication, whether MD5 or SHA1. The default is MD5 authentication.

WORD<0-20>

Specifies the secret key.

### Default

The default configuration removes the secret key.

### Command Mode

Global Configuration

## ntp interval

---

Specifies the time interval between successive NTP updates.

### Syntax

- **default ntp interval**
- **ntp interval <1-2185> OR <4-17>**

### Command Parameters

interval <1-2185> OR <4-17>

Specifies the time interval between successive NTP updates.

VSP 8600 Series specifies the time interval between successive NTP updates in minutes.

VOSS switches specify the time interval between successive NTP updates as a power of 2 in seconds.

## Default

For VSP 8600 Series, the default for NTPv3 is 15 minutes. The default value for NTPv4 is 6 minutes.

For VOSS, the default for NTPv4 is 2 to the power of 8 seconds.

## Command Mode

Global Configuration

## Usage Guidelines

NTPv3 is supported on VSP 8600 Series only. Interval range 1 to 2185 is supported on VSP 8600 Series only.

NTPv3 is deprecated for VOSS. Interval range 4 to 17 is supported on VOSS only.

## ntp master <1-16>

---

Configures the Network Time Protocol (NTP) in master mode.

## Syntax

- **ntp master**
- **ntp master <1-16>**
- **default ntp master**
- **default ntp master stratum**
- **no ntp master**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - NTPv4 Master Mode is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

---

## ntp restrict

---

Configures the Network Time Protocol (NTP) IPv4 or IPv6 restrict entry.

### Syntax

- **ntp restrict WORD<0-255>**
- **no ntp restrict WORD<0-255>**

### Command Parameters

WORD<0-255>

Specifies the IPv4 or IPv6 address.

### Default

The default is none.

### Command Mode

Global Configuration

### Usage Guidelines

DEMO FEATURE - NTPv4 Restrict is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

---

## ntp server

---

Add an IP address for a Network Time Protocol (NTP) server or modify existing NTP server parameters. For NTPv3, you can configure a maximum of 10 IPv4 NTP servers. For NTPv4, you can configure a maximum of 10 IPv4 NTP servers and 10 IPv6 NTP servers.

### Syntax

- **default ntp server WORD<0-255>**
- **default ntp server WORD<0-255> auth-enable**
- **default ntp server WORD<0-255> authentication-key**
- **default ntp server WORD<0-255> enable**
- **default ntp server WORD<0-255> source-ip**
- **no ntp server WORD<0-255>**
- **no ntp server WORD<0-255> source-ip**
- **no ntp server WORD<0-255> auth-enable**
- **no ntp server WORD<0-255> enable**

- **ntp server WORD<0-255>**
- **ntp server WORD<0-255> auth-enable**
- **ntp server WORD<0-255> authentication-key <0-65534>**
- **ntp server WORD<0-255> enable**
- **ntp server WORD<0-255> source-ip**

## Command Parameters

### auth-enable

Activates MD5 or SHA1 authentication on this Network Time Protocol (NTP) server. Without this option, the NTP server will not have any authentication by default.

### authentication-key <0-65534>

Specifies the key ID value used to generate the MD5 or SHA1 digest for the Network Time Protocol (NTP) server. The default authentication key is 0, which indicates disabled authentication.

### enable

Activates the Network Time Protocol (NTP) server.

### source-ip WORD <0-46>

Specifies the source IP for the server. If you do not configure source-ip, by default, the source-ip entry is initialized to 0.0.0.0. The IP address specified can be any local interface. This parameter applies only to NTPv3.

### WORD<0-255>

Specifies the IPv4 or IPv6 address of the NTP server.

## Default

The default configuration does not use MD5 authentication.

## Command Mode

Global Configuration

## Usage Guidelines

NTPv3 is only supported on VSP 8600 Series. NTPv3 is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

The *source-ip WORD <0-46>* parameter is only supported on VSP 8600 Series.

## ntp version

---

Configures the NTP version to either NTPv3 or NTPv4.

## Syntax

- `default ntp version`
- `ntp version 3`
- `ntp version 4`

## Default

The default is NTPv3.

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

---

## ovsdb

Enters OVSDb configuration mode

## Syntax

- `ovsdb`

## Default

None

## Command Mode

Global Configuration

---

## password

Configure password options.

## Syntax

- `default password`
- `default password default-lockout-time`
- `default password lockout WORD<0-46>`
- `default password lockout WORD<0-46> time`
- `default password password-history`

- **no password lockout WORD<0-46>**
- **password default-lockout-time <60-65000>**
- **password lockout WORD<0-46>**
- **password lockout WORD<0-46> time <60-65000>**
- **password password-history <3-32>**

## Command Parameters

### **access level WORD<2-8>**

Permits or blocks this access level. The available access level values are as follows: l l2 l3 ro rw rwa. The default access level is allow all.

### **aging-time day <1-365>**

Configures the expiration period for passwords in days, from 1-365. The default aging time is 90 days.

### **default-lockout-time <60-65000>**

Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60-65000 range. The default lockout time is 60 seconds.

### **lockout WORD<0-46> time <60-65000>**

Configures the host lockout time. WORD<0-46> is the host IP address in the format a.b.c.d. <60-65000> is the lockout-out time, in seconds, in the 60-65000 range.

### **min-passwd-len <10-20>**

Configures the minimum length for passwords in high-secure mode. The default minimum password length is 10 characters.

### **password-history <3-32>**

Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. The default password history is 3.

## Default

None

## Command Mode

Global Configuration

## password access-level

---

Enable CLI access levels to control the configuration actions of various users

## Syntax

- **default password access-level**
- **no password access-level WORD<2-8>**

- **password access-level WORD<2-8>**
- **password access-level WORD<2-8> default-lockout-time <60-65000>**
- **password access-level WORD<2-8> min-passwd-len <10-20>**
- **password access-level WORD<2-8> aging-time <1-365>**
- **password access-level WORD<2-8> password-history <3-32>**

## Command Parameters

**access level WORD<2-8>**

Allows or blocks this access level.

**aging-time day <1-365>**

Configures the expiration period for passwords in days, from 1-365.

**default-lockout-time <60-65000>**

Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60-65000 range.

**min-passwd-len <10-20>**

Configures the minimum length for passwords in high-secure mode.

**password-history <3-32>**

Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history.

**WORD<2-8>**

Permits or blocks this access level. The available access levels are:

- l1
- l2
- l3
- ro
- rw
- rwa

## Default

By default, all access levels are permitted.

## Command Mode

Global Configuration

## password aging-time

---

Configure the duration of your password for when it expires.



### Note

If you enable enhanced secure mode using the boot config flag `enhancedsecure-mode` command, the aging-time can be configurable for each user level: Administrator, Privilege, Operator, Auditor, and Security.

If you configure the aging time for each user level, the aging time must be more than the global change interval value and the pre-pass notification value.

If you do not enable enhanced secure mode, the aging time is a global value for all users.

## Syntax

- **default password aging-time**
- **default password aging-time user WORD<1-255>**
- **password aging-time day <1-365> user WORD<1-255>**
- **password aging-time day <1-365>**

## Command Parameters

**day <1-365>**

Configures the password expiry date. The default is 90 days.

**user WORD<1-255>**

Specifies the user name.

## Default

The default is 90 days.

## Command Mode

Global Configuration

## password change-interval

---

Specify the time interval between consecutive password changes.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flag `enhancedsecure-mode` command.

## Syntax

- **default password change-interval**



- **password change-interval <1-999>**

## Command Parameters

<1-999>

Configures the minimum interval between consecutive password changes in hours. The default is 24 hours.

## Default

The default is 24 hours.

## Command Mode

Global Configuration

## password create-user

---

Configure multiple users in each role based on their user names. You can configure the following roles: administrator, security, auditor, operator, privilege. An administrator role also exists, but only one administrator can exist, and is the user who can configure user access.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command.

## Syntax

- **password create-user auditor WORD<1-255>**
- **password create-user operator WORD<1-255>**
- **password create-user privilege WORD<1-255>**
- **password create-user security WORD<1-255>**

## Command Parameters

{**auditor | operator | privilege | security**}

The administrator is the highest level, and has access to all of the configurations and show commands, can view the log file and security commands. Only one administrator can exist for the system.

The privilege level has access to all of the commands the administrator has access to, and is known as the emergency-admin. A user at the privilege level always has to be authenticated within the switch locally, with no RADIUS or TACACS+ authentication allowed. The privilege level must login to the switch through the console port only.

The operator level has access to all configurations for packet forwarding on Layer 2 and Layer 3, and has access to show commands to view the configuration, but cannot view the audit logs access security, or password commands.

The security level has access only to security settings and can view configurations.

The auditor can view log files, and can view all configurations, but password configurations.

#### WORD<1-255>

Specifies the user name of the person to connect a particular user role level with a username.

## Default

None

## Command Mode

Global Configuration

## password default-lockout-time

Change the default lockout time after three invalid attempts.

## Syntax

- **default password default-lockout-time**
- **default password default-lockout-time min-passwd-len**
- **default password default-lockout-time min-passwd-len password-history**
- **default password default-lockout-time password-history**
- **password default-lockout-time <60-65000>**
- **password default-lockout-time <60-65000> min-passwd-len <10-20>**
- **password default-lockout-time <60-65000> min-passwd-len <10-20> password-history <3-32>**
- **password default-lockout-time <60-65000> password-history <3-32>**

## Command Parameters

#### <60-65000>

Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60-65000 range. The default lockout time is 60 seconds.

#### min-passwd-len <10-20>

Set the minimum length of passwords in hsecure mode.

#### password-history <3-32>

Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. The default password history is 3.

## Default

None

## Command Mode

Global Configuration

# password default-lockout-retries

---

Configure the default login attempts.

## Syntax

- **password default-lockout-retries <1-255>**
- **default password default-lockout-retries**

## Command Parameters

**1-255>**

Specifies the number of default login attempts. The default is 3.

## Default

The default is 3.

## Command Mode

Global Configuration

## Usage Guidelines

This command is not supported on VSP 8600 Series.

# password delete-user

---

Delete a user.

## Syntax

- **password delete-user WORD<1-255>**

## Command Parameters

**WORD<1-255>**

Specifies the user name of the person to connect a particular user role level with a username.

## Default

None

## Command Mode

Global Configuration

## password hash

---

Configure the secure hash algorithm level for password hashing.

## Syntax

- **default password hash**
- **password hash sha1**
- **password hash sha2**

## Command Parameters

**sha1**

Specifies SHA1 160-bit password hash.

**sha2**

Specifies SHA2 512-bit password hash.

## Default

The default is SHA2.

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series.

## password lockout

---

Lock out the host ip address

## Syntax

- **default password lockout WORD<0-46>**
- **default password lockout WORD<0-46> time**
- **no password lockout WORD<0-46>**

- **password lockout WORD<0-46>**
- **password lockout WORD<0-46> time <60-65000>**

## Command Parameters

**lockout WORD<0-46>**

Specifies the host IP address in the format a.b.c.d.

**time <60-65000>**

Specifies the lockout-out time, in seconds, in the 60-65000 range.

## Default

None

## Command Mode

Global Configuration

## password max-sessions

---

Specify the number of password attempts before lockout.

## Syntax

- **default password max-sessions user-name WORD<1-255>**
- **password max-sessions <1-8> user-name WORD<1-255>**

## Command Parameters

**max-sessions <1-8>**

Specifies the number of logon attempts.

**user-name WORD<1-255>**

Specifies the user name

## Default

The default is 3.

## Command Mode

Global Configuration

## password min-passwd-len

---

Configure the minimum password length in enhanced secure mode. The minimum length is 8 characters in enhanced secure ON mode.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command.

## Syntax

- **default password min-passwd-len**
- **password min-passwd-len <8-32>**

## Command Parameters

<8-32>

Configures the minimum character length required. The default is 8 in enhanced secure ON mode. In enhanced secure mode, if you configure anything lower than 8 characters, the switch displays an error message.

## Default

The default is 8 characters in enhanced secure ON mode.

## Command Mode

Global Configuration

## password password-history

---

Configure the minimum number of previous passwords to remember.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command.

## Syntax

- **default password password-history**
- **password password-history <1-99>**

## Command Parameters

<1-99>

Configures the minimum number of previous passwords to remember. The default is 3.

## Default

The default is 3.

## Command Mode

Global Configuration

## password password-rule

---

Configure the password complexity rule options. To meet the minimum password rule, you must have at least one of each of the following characters: uppercase, lowercase, numeric, and special character.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command.

## Syntax

- **default password password-rule**
- **password password-rule <1-2> <1-2> <1-2> <1-2>**

## Command Parameters

<1-2> <1-2> <1-2> <1-2>

The first <1-2> configures the minimum uppercase characters required.

The second <1-2> configures the minimum number of lowercase characters required.

The third <1-2> configures the minimum number of lowercase characters required.

The fourth <1-2> configures the minimum number of special characters required.

The default for each of these variables is 1.

## Default

The default is 1111.

## Command Mode

Global Configuration

## password post-expiry-notification-interval

---

Configure the system to provide a notification after the password expiry date at various intervals.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command.

## Syntax

- **default password post-expiry-notification-interval**
- **password post-expiry-notification-interval <1-99> <1-99> <1-99>**

## Command Parameters

<1-99> <1-99> <1-99>

The first <1-99> configures the first post password expiry notification. The default is one day after the expiration.

The second <1-99> value configures the second post password expiry notification. The default is 7 days after the notification.

The third <1-99> configures the third post password expiry notification. The default is 30 days after the expiration.

## Default

The default values for the three notifications are one day after the expiration, 7 days after the expiration, 30 days after the expiration.

## Command Mode

Global Configuration

# password post-pass-expiry-notification-interval

---

Configure the system to provide a notification after the password expiry date at various intervals.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command.

## Syntax

- **default password post-pass-expiry-notification-interval**
- **password post-pass-expiry-notification-interval <1-99> <1-99> <1-99>**

## Command Parameters

<1-99> <1-99> <1-99>

The first <1-99> configures the first post password expiry notification. The default is one day after the expiration.

The second <1-99> value configures the second post password expiry notification. The default is 7 days after the notification.

The third <1-99> configures the third post password expiry notification. The default is 30 days after the expiration.



## Default

The default values for the three notifications are one day after the expiration, 7 days after the expiration, 30 days after the expiration.

## Command Mode

Global Configuration

## password pre-expiry-notification-interval

---

Configure the system to provide a notification of the password expiry date at various intervals.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command.

## Syntax

- **default password pre-expiry-notification-interval**
- **password pre-expiry-notification-interval <1-99> <1-99> <1-99>**

## Default

The default values for the three notifications are at 30 days before the expiration, 7 days before the expiration, and then on the day of expiration.

## Command Mode

Global Configuration

## password pre-pass-expiry-notification-interval

---

Configure the system to provide a notification of the password expiry date at various intervals.



### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command.

## Syntax

- **default password pre-pass-expiry-notification-interval**
- **password pre-pass-expiry-notification-interval <1-99> <1-99> <1-99>**

## Command Parameters

<1-99> <1-99> <1-99>

The first <1-99> configures the first pre-password expiry notification. The default is 30 days after the expiration.

The second <1-99> value configures the second pre-password expiry notification. The default is 7 days after the notification.

The third <1-99> configures the third pre-password expiry notification. The default is the day of the notification.

## Default

The default values for the three notifications are at 30 days before the expiration, 7 days before the expiration, and then on the day of expiration.

## Command Mode

Global Configuration

## password set-password

---

Enable the setting of a new password in case the password expires.

## Syntax

- **password set-password user-name WORD<1-255>**

## Command Parameters

**user-name WORD<1-255>**

Specifies the username.

## Default

None

## Command Mode

Global Configuration

## passwordprompt

---

Change the password prompt for CLI sessions.

## Syntax

- **default passwordprompt**
- **no passwordprompt**
- **passwordprompt WORD<1-1510>**

## Command Parameters

**WORD <1-1510>**

Changes the CLI password prompt. WORD <1-1510> is an ASCII string from 1-1510 characters.

## Default

The default is Password.

## Command Mode

Global Configuration

## pluggable-optical-module

---

Configure Digital Diagnostic Monitoring to get information concerning the status of the transmitted and received signals to allow better fault isolation and error detection.

## Syntax

- **default pluggable-optical-module ddm-alarm-portdown**
- **default pluggable-optical-module ddm-monitor**
- **default pluggable-optical-module ddm-monitor-interval**
- **default pluggable-optical-module ddm-traps-send**
- **no pluggable-optical-module ddm-alarm-portdown**
- **no pluggable-optical-module ddm-monitor**
- **no pluggable-optical-module ddm-traps-send**
- **pluggable-optical-module ddm-alarm-portdown**
- **pluggable-optical-module ddm-monitor**
- **pluggable-optical-module ddm-monitor-interval <5-60>**
- **pluggable-optical-module ddm-traps-send**
- **pluggable-optical-module reset {slot/port[/sub-port]}**

## Command Parameters

**ddm-alarm-portdown**

Sets the port down when an alarm occurs. When enabled, the port goes down when any alarm occurs.

**ddm-monitor**

Enables the monitoring of the digital diagnostic monitoring (DDM). When enabled, you see the internal performance condition (temperature, voltage, bias, Tx power and Rx power) of the pluggable transceiver. The default is disable.

**ddm-monitor-interval <5-60>**

Configures the digital diagnostic monitoring (DDM) monitor interval in the range of 5 to 60 in seconds. If any alarm occurs, the user gets the log message before the specific interval configured by the user. The default value is 5 seconds.

#### **ddm-traps-send**

Enables or disables the sending of trap messages. When enabled, the trap message is sent to the Device manager, any time the alarm occurs. The default is enable.

#### **reset** {*slot/port[/sub-port]*}

Reset a transceiver to simulate removal and reinsertion of the transceiver, which can be helpful in troubleshooting. For example, if authentication of the transceiver fails, you can reset the transceiver to begin the authentication process again. Before you use this command, ensure the port is administratively down to avoid link flaps.

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is disable.

## Command Mode

Global Configuration

## **poe fast-poe-enable**

---

Enables Fast PoE on the switch. You must save the running PoE configuration file after you enable Fast PoE.

## Syntax

- **default poe fast-poe-enable**
- **no poe fast-poe-enable**
- **poe fast-poe-enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## poe perpetual-poe-enable

---

Enables Perpetual PoE on the switch. You must save the running PoE configuration file after you enable Perpetual PoE.

### Syntax

- **default poe perpetual-poe-enable**
- **no poe perpetual-poe-enable**
- **poe perpetual-poe-enable**

### Default

The default is disabled.

### Command Mode

Global Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## poe poe-pd-detect-type

---

Configure the PD detection mode.

### Syntax

- **default poe poe-pd-detect-type**
- **poe poe-pd-detect-type 802dot3af**
- **poe poe-pd-detect-type 802dot3af\_and\_legacy**
- **poe poe-pd-detect-type 802dot3at**
- **poe poe-pd-detect-type 802dot3at\_and\_legacy**
- **poe poe-pd-detect-type 802dot3bt**
- **poe poe-pd-detect-type 802dot3bt\_type3**
- **poe poe-pd-detect-type 802dot3bt\_type4**

### Command Parameters

**802dot3af**

Sets PD detection mode in 802.3af.

**802dot3af\_and\_legacy**

Sets PD detection mode in 802.3af and legacy.

#### **802dot3at**

Sets PD detection mode in 802.3at.

#### **802dot3at\_and\_legacy**

Sets PD detection mode in 802.3at and legacy.

#### **poe poe-pd-detect-type 802dot3bt**

Sets PD detection mode in 802dot3bt.

#### **802dot3bt\_type3**

Sets PD detection mode in 802.3bt Type 3 (60W).

#### **802dot3bt\_type4**

Sets PD detection mode in 802.3bt Type 4 (90W).

## Default

The default is 802dot3at\_and\_legacy.

## Command Mode

Global Configuration

## Usage Guidelines

The *802dot3bt\_type3* parameter applies only to VSP4900-12MXU-12XE, 5520 Series, and 5420 Series.

The *802dot3bt\_type4* parameter applies only to 5420 Series and 5520 Series.

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## poe poe-power-usage-threshold

---

Configure the power usage threshold.

## Syntax

- **default poe poe-power-usage-threshold**
- **poe poe-power-usage-threshold <1-99>**

## Command Parameters

<1-99>

Specifies the PoE usage threshold in the range of 1-99 percent.

## Default

The default is 80 percentage

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## portlock enable

Enable port locking for the security of the ports from any modifications.

## Syntax

- **default portlock enable**
- **no portlock enable**
- **portlock enable**

## Default

None

## Command Mode

Global Configuration

---

## preconfig slot

Designates a slot for IOC Module Pre-Configuration.

## Syntax

- **preconfig slot <1-8> WORD <1-20> [lock]**
- **no preconfig slot <1-8> [lock]**

## Command Parameters

<1-8>

Specifies the slot number designated for preconfiguration.

WORD <1-20>

Specifies the card type that can be assigned to the preconfigured slot.

## lock

Specifies that the IO card is locked to the preconfigured slot.



### Note

IO cards that do not match the card type assigned to the preconfigured slot do not operate.

## Default

None

## Command Mode

GigabitEthernet Interface Configuration

## prompt

---

Change the root level prompt or the system name for run-time mode.

## Syntax

- **default prompt**
- **no prompt**
- **prompt WORD <0-255>**

## Command Parameters

**WORD <0-255>**

Specifies the box level or root level prompt in the range of 0 to 255.

## Default

None

## Command Mode

Global Configuration

## qos egressmap

---

Modify the egress mappings to change traffic priorities. As a best practice, use the default mappings.

## Syntax

- **default qos egressmap lp**
- **default qos egressmap ds**



- **qos egressmap lp <0-7> <0-7>**
- **qos egressmap lp <0-7> <0-7> ds <0-7> WORD <1-6>**
- **qos egressmap ds <0-7> WORD<1-6>**

## Command Parameters

**<0-7>**

Specifies the Quality of Service (QoS) level in the range of 0 to 7.

**lp <0-7>**

Maps the Quality of Service (QoS) level to IEEE 802.1p priority. Each QoS level has a default IEEE 1P value:

- level 0-1
- level 1-0
- level 2-2
- level 3-3
- level 4-4
- level 5-5
- level 6-6
- level 7-7

**ds <0-7>**

Maps Quality of Service (QoS) level to Differentiated Services Code Point (DSCP).

**WORD<1-6>**

Specifies the DiffServ code point in hexadecimal, binary, or decimal.

## Default

None

## Command Mode

Global Configuration

## qos ingressmap

---

Modify the ingress mappings to change traffic priorities. As a best practice, use the default mappings.

## Syntax

- **default qos ingressmap lp**
- **default qos ingressmap ds**
- **qos ingressmap lp <0-7> <0-7>**
- **qos ingressmap ds <0-63> <0-7>**
- **qos ingressmaplp <0-7> <0-7> ds <0-63> <0-7>**

## Command Parameters

**ip <0-7> <0-7>**

Maps the IEEE 802.1p bit to Quality of Service (QoS) level. Each QoS level has a default IEEE 1P value:

- level 0-1
- level 1-0
- level 2-2
- level 3-3
- level 4-4
- level 5-5
- level 6-6
- level 7-7

**ds <0-63> <0-7>**

Maps the Differentiated Services Code Point (DSCP) to Quality of Service (QoS) level.

## Default

None

## Command Mode

Global Configuration

## qos queue-profile <1-6>

---

Configure a queue profile

## Syntax

- **no qos queue-profile <1-6>**
- **qos queue-profile <1-6> apply**
- **qos queue-profile <1-6> member add {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **qos queue-profile <1-6> member remove {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **qos queue-profile <1-6> name WORD<0-64>**

## Command Parameters

**apply**

Applies queue profile settings.

**member add {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Adds a port member.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**member remove** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Removes a port member.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**name** WORD<0-64>

Changes the queue profile name.

## Default

None

## Command Mode

Global Configuration

## qos queue-profile queue <1-6> <0-7>

Configure a queue of a specific queue profile.

## Syntax

- **default qos queue-profile queue <1-6> <0-7> {min-weight | rate-limit-enable}**
- **no qos queue-profile queue <1-6> <0-7> {min-weight | rate-limit-enable}**
- **qos queue-profile queue <1-6> <0-7> {min-weight <1-100> | rate-limit-enable}**

## Command Parameters

**min-weight <1-100>**

Configures the queue weight for weighted round robin (WRR), or the rate-limit in percentage of the link rate for queue shaping enabled on the queue.

For rate-limit-enabled queues, 50 indicates 50% bandwidth. The overall rate-limit-enabled queues cannot sum higher than 100 min-weight.

If rate-limiting is not enabled, this parameter configures the weight in the WRR scheduler. These values are not associated with bandwidth percentage.

The following list identifies the default minimum weight for each queue:

- Queue 0 – 10
- Queue 1 – 20
- Queue 2 – 30
- Queue 3 – 40
- Queue 4 – 50
- Queue 5 – 50
- Queue 6 – Rate limited to 50% of configured shaper rate
- Queue 7 – Rate limited to 5% of configured shaper rate

#### rate-limit-enable

Enables rate limiting on a weighted queue. By default, rate limiting is enabled for queues 6 and 7 only; it is disabled for queues 0 through 5.

## Default

None

## Command Mode

Global Configuration

## radius

---

Configure the switch to authenticate users identity through a central database.

## Syntax

- **default radius**
- **default radius access-priority-attribute**
- **default radius access-priority-attribute accounting**
- **default radius access-priority-attribute attribute-value**
- **default radius access-priority-attribute clear-stat**
- **default radius access-priority-attribute include-cli-commands**
- **default radius accounting attribute-value**
- **default radius accounting enable**
- **default radius accounting include-cli-commands**
- **default radius auth-info-attr-value**
- **default radius clear-stat**
- **default radius cli-commands-attribute**
- **default radius enable**
- **default radius maxserver**
- **default radius mcast-addr-attr-value**

- `default radius secure-flag`
- `no radius`
- `no radius accounting`
- `no radius accounting enable`
- `no radius accounting include-cli-commands`
- `no radius cli-cmd-count`
- `no radius cli-profile`
- `no radius enable`
- `no radius mcast-addr-attr-value`
- `no radius secure-flag`
- `no radius secure-profile WORD<1-16>`
- `radius`
- `radius access-priority-attribute <192-240>`
- `radius accounting attribute-value <192-240>`
- `radius accounting enable`
- `radius accounting include-cli-commands`
- `radius auth-info-attr-value <0-255>`
- `radius clear-stat`
- `radius cli-commands-attribute <192-240>`
- `radius enable`
- `radius maxserver <1-10>`
- `radius secure-flag`
- `radius secure-profile WORD<1-16>`
- `radius secure-profile WORD<1-16> ca-cert-file WORD<0-128>`
- `radius secure-profile WORD<1-16> ca-cert-file WORD<0-128> WORD<1-128>`
- `radius secure-profile WORD<1-16> cert-file WORD<0-128>`
- `radius secure-profile WORD<1-16> cert-file WORD<0-128> WORD<1-128>`
- `radius secure-profile WORD<1-16> key-file WORD<0-128>`
- `radius secure-profile WORD<1-16> key-file WORD<0-128> WORD<1-128>`
- `radius secure-profile WORD<1-16> key-pwd WORD<0-255>`

## Command Parameters

`access-priority-attribute <192-240>`

Specifies the value of the Access Priority attribute in the range of 192 to 240 and the default is 192.

`accounting {attribute-value <192-240>|enable|include-cli-commands}`

Enables Remote Dial-In User Services (RADIUS) accounting. The default is false.

`auth-info-attr-value <0-255>`

Specifies the value of the authentication-information attribute in the range of 0 to 255. The default is 91.

**ca-cert-file WORD<0-128>**

Specifies the full path of the certification authority (CA) certificate file. Alternatively, you can specify the filename only, and the file is retrieved from the current directory.

**cert-file WORD<0-128>**

Specifies the full path of the server certificate file. Alternatively, you can specify the filename only, and the file is retrieved from the current directory.

**clear-stat**

Clears the RADIUS statistics.

**cli-commands-attribute <192-240>**

Specifies the value of the CLI commands attribute in the range of 192 to 240 and the default is 195.

**command-access-attribute <192-240>**

Specifies the value of the command access attribute in the range of 192 to 240 and the default is 194.

**key-file WORD<0-128>**

Specifies the full path of the private key file. Alternatively, you can specify the filename only, and the file is retrieved from the current directory.

**key-pwd WORD<0-255>**

Specifies the private key password for the RADSec profile.

**maxserver<1-10>**

Specific to RADIUS authentication. Sets the maximum number of servers allowed for the device. The range is between 1 and 10. The default is 10.

**mcast-addr-attr-value <0-255>**

Specifies the value of the multicast address attribute in the range of 0 to 255. The default is 90.

**secure-flag**

Specifies whether RADIUS Security (RADSec) is globally enabled. The default is disabled..86

**secure-profile WORD<1-16>**

Specifies the RADSec profile name.

**WORD<1-128>**

Specifies the name of the installed file.

## Command Mode

Global Configuration

## Usage Guidelines

The *ca-cert-file WORD<0-128>*, *cert-file WORD<0-128>*, *key-file WORD<0-128>*, *key-pwd WORD<0-255>*, *secure-flag*, *secure-profile WORD<1-16>*, and *WORD<1-128>* parameters are not supported on the VSP 8600 Series.

## radius access-priority-attribute

---

Configure radius access priority.

### Syntax

- **default radius access-priority-attribute**
- **radius access-priority-attribute <192-240>**

### Command Parameters

<192-240>

Specifies the value of the Access Priority attribute in the range of 192 to 240. The default is 192.

### Default

The default value of access-priority-attribute is 192.

### Command Mode

Global Configuration

## radius accounting attribute-value

---

Configure radius accounting attribute.

### Syntax

- **default radius accounting attribute-value**
- **radius accounting attribute-value <192-240>**

### Command Parameters

<192-240>

CLI Command attribute value.

### Default

The default value of the attribute-value is 193.

## Command Mode

Global Configuration

### radius accounting enable

---

Enable or disable radius accounting.

#### Syntax

- **default radius accounting enable**
- **no radius accounting enable**
- **radius accounting enable**

#### Default

The default value is disabled.

## Command Mode

Global Configuration

### radius accounting include-cli-commands

---

Enable or disable to include the CLI commands to the radius accounting.

#### Syntax

- **default radius accounting include-cli-commands**
- **no radius accounting include-cli-commands**
- **radius accounting include-cli-commands**

#### Default

The default value of include-cli-commands is disabled.

## Command Mode

Global Configuration

### radius auth-info-attr-value

---

Set the authentication information attribute value.

#### Syntax

- **default radius auth-info-attr-value**



- **radius auth-info-attr-value <0-255>**

## Command Parameters

<0-255>

Specifies the value of the authentication-information attribute in the range of 0 to 255. The default is 91.

## Default

The default value of auth-info-attr-value is 91.

## Command Mode

Global Configuration

---

## radius clear-stat

Clear the radius statistics.

## Syntax

- **radius clear-stat**

## Default

None

## Command Mode

Global Configuration

---

## radius cli-cmd-count

Configure a Remote Access Dial-In User Services (RADIUS) accounting interim request to create a log whenever more than forty CLI commands are executed.

## Syntax

- **default radius cli-cmd-count**
- **radius cli-cmd-count <1-40>**

## Command Parameters

<1-40>

Specifies a value of the CLI command count in the range of 1 to 40.

## Default

The default value is 40.

## Command Mode

Global Configuration

# radius cli-profile

---

Use Remote Access Dial-In User Services (RADIUS) CLI profiling to grant or deny CLI command access to users being authenticated by way of the RADIUS server.

## Syntax

- **default radius cli-profile**
- **no radius cli-profile**
- **radius cli-profile**

## Default

The default is disabled/false.

## Command Mode

Global Configuration

# radius command-access-attribute

---

Configure Remote Access Dial-In User Services (RADIUS) authentication and RADIUS accounting attributes to determine the size of the packets received.

## Syntax

- **default radius command-access-attribute**
- **radius command-access-attribute <192-240>**

## Command Parameters

**command-access-attribute <192-240>**

Specifies the Remote Dial-In User Services (RADIUS) authentication attribute value is an integer value of the CLI command count in the range of 192 to 240.

## Default

The default value is 194.

## Command Mode

Global Configuration

## radius dynamic-server client

---

Configure a client to process dynamic session changes.

### Syntax

- `default radius dynamic-server client WORD<0-46>`
- `default radius dynamic-server client WORD<0-46> enable`
- `default radius dynamic-server client WORD<0-46> port`
- `default radius dynamic-server client WORD<0-46> secret`
- `no radius dynamic-server client WORD<0-46>`
- `no radius dynamic-server client WORD<0-46> enable`
- `no radius dynamic-server client WORD<0-46> port`
- `no radius dynamic-server client WORD<0-46> secret`
- `radius dynamic-server client WORD<0-46> enable`
- `radius dynamic-server client WORD<0-46> port <1024-65535>`
- `radius dynamic-server client WORD<0-46> port <1024-65535> enable`
- `radius dynamic-server client WORD<0-46> port <1024-65535> secret WORD<0-32>`
- `radius dynamic-server client WORD<0-46> port <1024-65535> secret WORD<0-32> enable`
- `radius dynamic-server client WORD<0-46> secret WORD<0-32>`
- `radius dynamic-server client WORD<0-46> secret WORD<0-32> enable`

### Command Parameters

`enable`

Enables the RADIUS Dynamic Authorization client.

`port <1024-65535>`

Specifies the port value.

`secret WORD<0-32>`

Specifies a value for secret key.

`WORD<0-46>`

Specifies the client address.

### Default

None

## Command Mode

Global Configuration

### radius enable

---

Enable or disable Remote Access Dial-In User Services (RADIUS) authentication globally on the device to allow further configuration to take place.

#### Syntax

- **default radius enable**
- **no radius enable**
- **radius enable**

#### Default

The default value is disabled.

## Command Mode

Global Configuration

### radius maxserver

---

Configure the maximum number of servers allowed to be configured

#### Syntax

- **default radius maxserver**
- **radius maxserver <1-10>**

#### Command Parameters

<1-10>

Number of maximum server allowed to be configured.

#### Default

The default value is 10.

## Command Mode

Global Configuration

---

## radius mcast-addr-attr-value

---

Configure the multicast address attribute value.

### Syntax

- **default radius mcast-addr-attr-value**
- **radius mcast-addr-attr-value <0-255>**

### Default

The default value is 90.

### Command Mode

Global Configuration

---

## radius reachability keep-alive-timer

---

Specifies, in seconds, the interval between checks when radius server is reachable.

### Syntax

- **default radius reachability keep-alive-timer**
- **radius reachability keep-alive-timer <30-600>**

### Command Parameters

**<30-600>**

Specifies, in seconds, the interval between checks when radius server is reachable. The default is 180 seconds.

### Default

The default is 180 seconds.

### Command Mode

Global Configuration

---

## radius reachability mode

---

Specifies status-server mode or use-radius mode. Statusserver mode provides a standard-compliant method for RADIUS reachability. Use-radius mode requires the configuration of dummy packets that are sent to RADIUS servers.

## Syntax

- **radius reachability mode status-server**
- **radius reachability mode use-radius**

## Command Parameters

### use-radius

Use dummy radius packets to check radius reachability.

## Default

The default is use-radius mode.

## Command Mode

Global Configuration

---

## radius reachability password

Configure the radius request password.

## Syntax

- **default radius reachability password**
- **radius reachability password WORD<1-16>**

## Command Parameters

### WORD<1-16>

Configures the RADIUS request password.

## Default

The default is extremenetworks

## Command Mode

Global Configuration

---

## radius reachability unreachable-timer

Specifies, in seconds, the interval between checks when radius server is unreachable.

## Syntax

- **default radius reachability unreachable-timer**

- **radius reachability unreachable-timer <30-600>**

## Command Parameters

<30-600>

Specifies, in seconds, the interval between checks when radius server is unreachable. The default is 60 seconds.

## Default

The default is 60 seconds.

## Command Mode

Global Configuration

---

## radius reachability username

Configure the RADIUS request username.

## Syntax

- **default radius reachability username**
- **radius reachability username WORD<1-16>**

## Command Parameters

WORD<1-16>

Configures the RADIUS request username.

## Default

The default is extremenetworks.

## Command Mode

Global Configuration

---

## radius server host

Add a Remote Access Dial-In User Services (RADIUS) server to enable RADIUS service on the switch.

## Syntax

- **default radius server host WORD<0-46> used-by {cli|eapol|endpoint-tracking|snmp|web} [acct-enable|acct-port|enable|key|port|priority|**

- ```

    retry|secure-enable|secure-log-level|secure-mode|secure-profile|
    source-ip|timeout]
  • no radius server host WORD<0-46> used-by {cli|eapol|endpoint-tracking|
    snmp|web} [acct-enable|acct-port|enable|secure-enable]
  • radius server host WORD<0-46> {key WORD<0-32>|used-by {cli|eapol|
    endpoint-tracking|snmp|web}}
  • radius server host WORD<0-46> key WORD<0-32> [acct-enable|acct-port
    <1-65536>|enable|port <1-65536>|priority <1-10>|retry <0-6>|secure-
    enable|secure-log-level|secure-mode|secure-profile|source-ip WORD
    <0-46>|timeout <1-20>|used-by {cli|eapol|endpoint-tracking|snmp|web}]
  • radius server host WORD<0-46> used-by {cli|eapol|endpoint-tracking|
    snmp|web} [acct-enable|acct-port|enable|key|port|priority|retry|
    secure-enable|secure-log-level|secure-mode|secure-profile|source-ip|
    timeout]

```

## Command Parameters

### acct-enable

Enables Remote Dial-In User Services (RADIUS) accounting on this server. The default is enabled.

### acct-port <1-65536>

Configures a UDP port of the Remote Dial-In User Services (RADIUS) accounting server. The default is 1816.

### enable

Enables this server.

### host WORD <0-46>

Creates a host server. Remote Dial-In User Services (RADIUS) supports IPv4 addresses. WORD <0-46> specifies an address in A.B.C.D or x:x:x:x:x:x format.

### key WORD<0-32>

Configures a secret key in the range of 0-20 characters.

### port <1-65536>

Configures a UDP port of the Remote Dial-In User Services (RADIUS) server.

### priority <1-10>

Configures the priority value for this server. The default is 10.

### retry <0-6>

Configures the maximum number of authentication retries. The default is 3.

### secure-enable

Enable secure mode on the server.

### secure-log-level

Specifies the RADIUS secure server log severity level. Possible values are:

- critical
- debug



- error
- info
- warning

**secure-mode**

Specifies the protocol for establishing the secure connection with the server.

**secure-profile**

Specifies the secure profile name.

**source-ip WORD <0-46>**

Configures an IP address as the source address when transmitting RADIUS packets. Remote Dial-In User Services (RADIUS) supports IPv4 addresses. WORD <0-46> specifies an address in A.B.C.D or x:x:x:x:x:x format.

**timeout <1-20>**

Configures the number of seconds before the authentication request times out. The default is 8.

**used-by {cli|eapol|endpoint-tracking|snmp|web}**

Configures how the server functions:

- cli - configures the server for CLI authentication
- eapol - configures the server for Extensible Authentication Protocol over LAN (EAPoL) authentication
- endpoint-tracking - configures the server for Endpoint Tracking authentication

**used-by endpoint-tracking** does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

- snmp - configures the server for Simple Network Management Protocol (SNMP) accounting
- web - configures the server for web authentication

The default is cli.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

The *secure-enable*, *secure-log-level*, *secure-mode*, and *secure-profile* parameters are not supported on the VSP 8600 Series.

The *source-ip WORD <0-46>* parameter is only supported on the VSP 8600 Series.

---

## radius sourceip-flag

---

Configure the source IP address if the outgoing interface on the switch fails so that configuration changes be made to define the new Remote Access Dial-In User Services (RADIUS) Client on the RADIUS Server.

### Syntax

- **default radius sourceip-flag**
- **no radius sourceip-flag**
- **radius sourceip-flag**

### Default

The default is disabled/false.

### Command Mode

Global Configuration

### Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

---

## radius-snmp

---

Enable Remote Access Dial-In User Services (RADIUS) accounting to log all of the activity of each remote user in a session on the centralized RADIUS accounting server.

### Syntax

- **default radius-snmp**
- **default radius-snmp abort-session-timer**
- **default radius-snmp acct-enable**
- **default radius-snmp re-auth-timer**
- **default radius-snmp user**
- **no radius-snmp**
- **no radius-snmp acct-enable**
- **radius-snmp**
- **radius-snmp abort-session-timer <30-65535>**
- **radius-snmp acct-enable**
- **radius-snmp re-auth-timer <30-65535>**
- **radius-snmp user WORD<0-20>**

## Command Parameters

### **abort-session-timer <30-65535>**

Specifies the timer to be used for sending a stop accounting message for this particular Simple Network Management Protocol (SNMP) session. The timer value ranges from 30 to 65535. This default is 180.

### **acct-enable**

Enables Remote Dial-In User Services (RADIUS) accounting globally. RADIUS accounting cannot be enabled unless a valid server is configured. This feature is disabled by default.

### **re-auth-timer <30-65535>**

Timer to be sent for re-authentication the Simple Network Management Protocol (SNMP) session. The timer value ranges from 30 to 65535. The default is 180.

### **user WORD<0-20>**

Specifies the username for the Simple Network Management Protocol (SNMP) access. WORD<0-20> specifies the username in a range of 0 to 20 characters. The default is `snmp_user`.

## Default

The default value is disabled.

## Command Mode

Global Configuration

## rmon alarm

Creates an alarm interface.

## Syntax

- **default rmon alarm <1-65535>**
- **default rmon alarm <1-65535> owner**
- **no rmon alarm <1-65535>**
- **rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta }**
- **rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta }  
falling-threshold <-2147483647-2147483647> event <1-65535>**
- **rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta }  
falling-threshold <-2147483647-2147483647> event <1-65535> owner  
WORD<1-127>**
- **rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta }  
falling-threshold <-2147483647-2147483647> event <1-65535> rising-  
threshold <-2147483647-2147483647> event <1-65535>**
- **rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta }  
falling-threshold <-2147483647-2147483647> event <1-65535> rising-  
threshold <-2147483647-2147483647> event <1-65535> owner WORD<1-127>**

- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } owner WORD<1-127>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } rising-threshold <-2147483647-2147483647> event <1-65535>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } rising-threshold <-2147483647-2147483647> event <1-65535> falling-threshold <-2147483647-2147483647> event <1-65535>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } rising-threshold <-2147483647-2147483647> event <1-65535> falling-threshold <-2147483647-2147483647> event <1-65535> owner WORD<1-127>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } rising-threshold <-2147483647-2147483647> event <1-65535> owner WORD<1-127>`

## Command Parameters

`{absolute | delta}`

Specifies the sample type.

`<1-3600>`

Specifies the sampling interval.

`<1-65535>`

Specifies the interface index number from 1-65535.

`event <1-65535>`

Specifies the event number.

`falling-threshold <-2147483647-2147483647>`

Specifies the falling threshold value for the sampled statistic.

`owner WORD<1-127>`

Specifies the name of the owner. The default value is CLI if the entry is configured using CLI. The default is SNMP if the entry is configured using EDM or SNMP.

`rising-threshold <-2147483647-2147483647>`

Specifies the rising threshold value for the samples statistic.

`WORD<1-536>`

Specifies the variable name or OID, case sensitive.

## Default

None

## Command Mode

Global Configuration

## rmon event

---

Creates an event.

### Syntax

- **default rmon event <1-65535>**
- **default rmon event <1-65535> community**
- **default rmon event <1-65535> description**
- **default rmon event <1-65535> owner**
- **no rmon event <1-65535>**
- **no rmon event <1-65535> log**
- **rmon event <1-65535>**
- **rmon event <1-65535> community WORD<1-127>**
- **rmon event <1-65535> description WORD<0-127>**
- **rmon event <1-65535> log**
- **rmon event <1-65535> owner WORD<1-127>**
- **rmon event <1-65535> trap**

### Command Parameters

**<1-65535>**

Specifies the event index number.

**community WORD<1-127>**

Specifies the SNMP community where you can send SNMP traps, with a string length 1 to 127. You can set the community, but the trap is not filtered out. The trap is sent to all configured snmp-server hosts, regardless of the value of this field.

**description WORD<0-127>**

Specifies the event description.

**log**

Specifies if this event stores a log when the event is triggered by the alarm.

**owner WORD<1-127>**

Specifies the name of the event owner. The default value is CLI if the entry is configured using CLI. The default is SNMP if the entry is configured using EDM or SNMP.

**trap**

Specifies if this event will send a trap when the event is triggered by the alarm. The trap will be sent to all the snmp-server hosts configured in the snmp table.

### Default

None

## Command Mode

Global Configuration

## rmon history

Creates a history control interface.

### Syntax

- **default rmon history <1-65535>**
- **default rmon history <1-65535> buckets**
- **default rmon history <1-65535> interval**
- **default rmon history <1-65535> owner**
- **no rmon history <1-65535>**
- **rmon history <1-65535> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **rmon history <1-65535> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} buckets <1-65535>**
- **rmon history <1-65535> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} interval <1-3600>**
- **rmon history <1-65535> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} owner WORD<1-127>**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**<1-65535>**

Specifies the index number of the history control interface.

**buckets <1-65535>**

Specifies the number of buckets requested. The default is 50.

**interval <1-3600>**

Specifies the the time interval in seconds over which the data is sampled for each bucket. The default is 1800.

**owner WORD<1-127>**

Specifies the name of the entry owner. The default value is CLI if the entry is configured using CLI. The default is SNMP if the entry is configured using EDM or SNMP.

## Default

None

## Command Mode

Global Configuration

## rmon stats

---

Creates an ether-stats control interface.

## Syntax

- **default rmon stats <1-65535>**
- **default rmon stats <1-65535> owner**
- **no rmon stats <1-65535>**
- **rmon stats <1-65535> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **rmon stats <1-65535> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} owner WORD<1-127>**
- **rmon stats <1-65535> owner WORD<1-127>**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**<1-65535>**

Specifies the index number of the ether stats control interface.

**owner WORD<1-127>**

Specifies the name of the entry owner. The default value is CLI if the entry is configured using CLI. The default is SNMP if the entry is configured using EDM or SNMP.

## Default

None

## Command Mode

Global Configuration

---

## rmon util-method

---

Controls whether port utilization is calculated in half or full duplex.

### Syntax

- **default rmon util-method**
- **rmon util-method <half|full>**

### Command Parameters

<half|full>

Controls whether port utilization is calculated in half or full duplex.

### Default

The default is half.

### Command Mode

Global Configuration

---

## route-map

---

Configure and enable a route policy so that the switch can control routes that certain packets can take.

### Syntax

- **default route-map WORD<1-64> <1-65535>**
- **no route-map WORD<1-64> <1-65535>**
- **route-map WORD<1-64> <1-65535>**
- **route-map WORD<1-64> <1-65535> { permit | deny }**

### Command Parameters

<1-65535>

Specifies the sequence number for the route policy.

<permit|deny>

Permit or deny the route.

WORD<1-64>

Specifies the policy name.

### Default

None



## Command Mode

Global Configuration

### router bfd

---

Enables Bidirectional Forwarding Detection (BFD) on the global router.

#### Syntax

- **default router bfd enable**
- **no router bfd enable**
- **router bfd [enable]**

#### Default

The default is disabled.

## Command Mode

Global Configuration

### router bgp

---

Access the router configuration mode to configure the Border Gateway Protocol (BGP) commands.

#### Syntax

- **router bgp**
- **router bgp WORD<0-11>**
- **router bgp WORD<0-11> enable**

#### Command Parameters

**enable**

Enables BGP on the router.

**WORD <0-11>**

Specifies the AS number. You cannot enable BGP until you change the local AS to a value other than 0.

#### Default

None

## Command Mode

Global Configuration

### router bgp as-4-byte enable

---

Globally enable 4-byte autonomous system numbers.

#### Syntax

- **default router bgp as-4-byte enable**
- **no router bgp as-4-byte enable**
- **router bgp as-4-byte enable**

#### Default

The default is disabled.

## Command Mode

Global Configuration

### router bgp as-dot enable

---

Globally enable the AS dot representation for 4-byte AS numbers.

#### Syntax

- **default router bgp as-dot enable**
- **no router bgp as-dot enable**
- **router bgp as-dot enable**

#### Default

The default is disabled.

## Command Mode

Global Configuration

### router isis

---

Enter Intermediate-System-to-Intermediate-System (IS-IS) Router Configuration mode.

#### Syntax

- **default router isis**

- **no router isis**
- **router isis**

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## router isis enable

Enable Intermediate-System-to-Intermediate-System (IS-IS) globally. If you use the default or no format of this command, you disable IS-IS globally.

## Syntax

- **default router isis enable**
- **no router isis enable**
- **router isis enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## router isis remote

Enter Intermediate-System-to-Intermediate-System (IS-IS) Router Remote Configuration mode.

## Syntax

- **default router isis remote**
- **no router isis remote**
- **router isis remote**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## router isis remote enable

Enables router Intermediate-System-to-Intermediate-System (IS-IS) remote configuration globally.

## Syntax

- `default router isis remote [enable]`
- `no router isis remote [enable]`
- `router isis remote [enable]`

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## router ospf

Enable OSPF for the switch. If you do not use an optional parameter with the command, you enter the OSPF Router Configuration mode.

## Syntax

- `default router ospf`
- `default router ospf enable`
- `default router ospf ipv6-enable`
- `no router ospf`
- `no router ospf enable`
- `no router ospf ipv6-enable`
- `router ospf`

- **router ospf enable**
- **router ospf ipv6-enable**

## Command Parameters

### enable

Enables OSPF routing on the switch.

### ipv6-enable

Enables OSPFv3 for IPv6 routing.

## Default

None

## Command Mode

Global Configuration

## router rip enable

---

Enable RIP globally.

## Syntax

- **default router rip enable**
- **no router rip enable**
- **router rip**
- **router rip enable**
- **router rip enable vrf <1-511>**

## Command Parameters

### enable

Globally enables RIP on the VRF or switch.

### vrf <1-511>

Enables RIP for a particular VRF. <1-511> denotes the range of the VRF id.

## Default

None

## Command Mode

Global Configuration

---

## router rip ipv6-enable

---

Enable RIPng globally.

### Syntax

- **default router rip ipv6-enable**
- **no router rip ipv6-enable**
- **router rip ipv6-enable**

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## router vrf

---

Enable VRF for the switch.

### Syntax

- **router vrf WORD <1-16>**

### Command Parameters

WORD<0-16>

Specifies the VRF name.

### Default

None

### Command Mode

Global Configuration

---

## router vrrp

---

Enable VRRP for the switch.

### Syntax

- **router vrrp**

## Default

None

## Command Mode

Global Configuration

## run spbm

---

Configure all SPBM, CFM, IS-IS and interface level settings in one command.

## Syntax

- **run spbm**
- **run spbm clean**

## Command Parameters

### clean

Removes existing SPBM configurations, disables CFM, and returns the CFM MEP-ID and level configurations to default values.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

If the switch uses Zero Touch Fabric Configuration, you must run the following commands before you use the **run spbm clean** command:

- **no** Auto-sense **onboarding i-sid**
- **no vlan i-sid <1-4059>**

## run spbm interface

---

Configures IS-IS SPBM port and MLT interfaces.

## Syntax

- **run spbm interface**
- **run spbm interface clean**

## Command Parameters

### clean

Deletes specified IS-IS port and MLT interfaces.

## Default

None

## Command Mode

Global Configuration

---

## run vms layer-2 switch

Runs the Layer 2 Video Surveillance install script.

## Syntax

- **run vms layer-2 switch <5-99> [syntax]**

## Command Parameters

### <5-99>

Specifies a switch value, which is then used as a common element to configure switch parameters such as nickname, VLAN ID, SPB and IP parameters.

### syntax

Specifies that the switch displays all the commands run by the script on the console. Use this parameter to see errors that the script encounters.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



---

## run vms layer-3 switch

---

Configures basic parameters to quickly deploy a video surveillance system.

The Layer 3 Video Surveillance install script performs the same function as the **run vms endura** script. However, the switch continues to support the **run vms endura** script for backward compatibility.

### Syntax

- **run vms layer-3 switch <5-99> [syntax | verbose]**

### Command Parameters

#### <5-99>

Specifies a switch value in the range 5 to 99, which is used to seed unique values in the configuration script. This value is then used as a common element to configure switch parameters such as nickname, VLAN ID, SPB and IP parameters.

#### syntax

Specifies that the switch displays all the commands run by the script on the console. Use this parameter to see errors that the script encounters.

#### verbose

Specifies that the switch prompts you to accept or change the default configuration values.

### Default

None

### Command Mode

Global Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## sflow agent-ip

---

Specifies the agent IP address (IPv4).

### Syntax

- **no sflow agent-ip**
- **sflow agent-ip {A.B.C.D}**

## Command Parameters

**sflow agent-ip {A.B.C.D}**

Specifies the agent IP address (IPv4).

## Default

None

## Command Mode

Global Configuration

## sflow collector

---

Configure an sFlow collector to determine the device to which the sFlow agent sends sFlow datagrams.

## Syntax

- **default sflow collector <1-2>**
- **default sflow collector <1-2> port**
- **default sflow collector <1-2> timeout**
- **no sflow collector <1-2>**
- **no sflow collector <1-2> address {A.B.C.D}**
- **no sflow collector <1-2> owner WORD<1-20>**
- **sflow collector <1-2>**
- **sflow collector <1-2> address {A.B.C.D}**
- **sflow collector <1-2> address {A.B.C.D} vrf WORD<1-16>**
- **sflow collector <1-2> owner WORD<1-20>**
- **sflow collector <1-2> port <1-65535>**
- **sflow collector <1-2> timeout <1-65535>**

## Command Parameters

**<1-2>**

Specifies the ID to export sFlow datagrams to the collector ID.

**address {A.B.C.D}**

Specifies the collector IP address.

**owner WORD<1-20>**

Specifies the sFlow collector name.

**port <1-65535>**

Specifies the destination UDP port. The default port is 6343.

**timeout <1-65535>**

Specifies the time remaining (in seconds) before the collector is released. The default is 0, which means you are not using the collector.

**vrf**

Specifies the name of the VRF used to reach the collector.

## Default

None

## Command Mode

Global Configuration

---

## sflow enable

Globally enables sFlow.

## Syntax

- **default sflow enable**
- **no sflow enable**
- **sflow enable**

## Default

None

## Command Mode

Global Configuration

---

## slot shutdown

Slot shutdown.

## Syntax

- **default slot shutdown {slot[-slot][,...]}**
- **no slot shutdown {slot[-slot][,...]}**
- **slot shutdown {slot[-slot][,...]}**

## Command Parameters

{slot[-slot][,...]}

Specifies the slot number. The valid slot numbers differ depending on hardware platform. For more information about slot numbers, see your hardware documentation.

## Default

None

## Command Mode

Global Configuration

## slpp (globally)

---

Enable the Simple Loop Prevention Protocol (SLPP) globally and for a VLAN to detect a loop and automatically stop it. The VLAN configuration controls the boundary of SLPP-PDU transmission.

## Syntax

- **default slpp**
- **default slpp enable**
- **default slpp tx-interval**
- **no slpp**
- **no slpp enable**
- **no slpp vid <1-4059>**
- **slpp enable**
- **slpp tx-interval <500-5000>**
- **slpp vid <1-4059>**

## Command Parameters

### enable

Enables or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process. If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets. The default is disabled.

### tx-interval <500-5000>

Configures the SLPP packet transmit interval, expressed in milliseconds, in a range from 500-5000. The default is 500.

### vid <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Global Configuration

## slpp-guard ethertype

---

Configures Set SLPP Guard ethertype.

### Syntax

- **default slpp-guard ethertype**
- **slpp-guard ethertype <0x0600-0xffff>**

### Command Parameters

<0x0600-0xffff>

Specifies a hexadecimal value ranging from 0x0600– 0xffff. The default value is 0x8102.

### Default

The default value is 0x8102.

## Command Mode

Global Configuration

## smtp

---

Configures SMTP to generate email notifications for component failures, critical conditions, or general system health status.

### Syntax

- **default smtp enable**
- **no smpt enable**
- **smpt enable**
- **smtp domain-name WORD<1-254>**
- **smtp event-id add WORD<1-1100**
- **smtp event-id remove WORD<1-1100>**
- **smtp port <1-65535>**
- **smtp receiver-email add WORD<3-1274>**
- **smtp receiver-email remove WORD<3-1274>**
- **smtp sender-email WORD<3-254>**
- **smtp server WORD<1-256>**
- **smtp status-send-timer <0 | 30-43200>**

## Command Parameters

### **status-send-timer** <0 | 30-43200>

Specifies the interval, in seconds, at which the switch sends status information. The default is 30 seconds. A value of 0 means the switch does not send status information.

### **domain-name** WORD<1-254>

Specifies the hostname or IPv4 address.

### **enable**

Enables SMTP.

### **event id** {add | remove} WORD<1-1100>

Add or remove log event to the list of events that generate email notification. You can specify multiple event IDs in a single command by separating them with a comma. The event ID can be up to 10 digits in hexadecimal format.

### **port** <1-65535>

Specifies the SMTP server TCP port number. The default is 25.

### **receiver-mail** {add | remove} WORD<3-1274>

Adds or removes an email address to the recipient list. The recipients receive the email notification generated by the switch. The maximum length for the address is 254 characters.

### **sender-mail** WORD<3-254>

Specifies the email address that displays it in the From field of the message that the switch generates. By default, the switch uses <SystemName>@default.com.

### **server** WORD<1-256>

Specifies the SMTP server address. You can use either a hostname or IPv4 address. If you use a hostname, you must configure the DNS client on the switch.

## Default

The default is disabled.

## Command Mode

Global Configuration

## snmplog

---

Use SNMP trap logging to log to the system log file. This allows you to send SNMP logs to a system log server.

## Syntax

- **default snmplog**
- **default snmplog enable**
- **no snmplog enable**
- **snmplog enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## snmp-server authentication-trap enable

Activate the generation of authentication traps.

## Syntax

- **default snmp-server authentication-trap**
- **no snmp-server authentication-trap**
- **snmp-server authentication-trap enable**

## Default

The default is disabled/false.

## Command Mode

Global Configuration

---

## snmp-server community

Create a community to use in forming a relationship between an SNMP agent and one or more SNMP managers. You require SNMP community strings to access the system using SNMP-based management software.

## Syntax

- **no snmp-server community WORD<1-32>**
- **no snmp-server community-by-index WORD<1-32>**
- **snmp-server community WORD<1-32> group WORD<0-32>**
- **snmp-server community WORD<1-32> group WORD<0-32> secname WORD<1-32>**
- **snmp-server community WORD<1-32> index WORD<1-32> secname WORD<1-32>**
- **snmp-server community WORD<1-32> index WORD<1-32> secname WORD<1-32> context WORD<0-32>**
- **snmp-server community WORD<1-32> secname WORD<1-32>**
- **snmp-server community WORD<1-32> secname WORD<1-32> context WORD<0-32>**

## Command Parameters

**community-by-index WORD<1-32>**

Specifies the community string by index to delete.

**context WORD<0-32>**

Specifies the context in which management information is accessed when you use the specified community string.

**group WORD<0-32>**

Specifies the group name.

**index WORD<0-32>**

Specifies the unique index value of a row in this table.

**secname WORD<0-32>**

Maps the community string to the security name in the VACM Group Member Table. The range is 0-32 characters.

**WORD<1-32>**

Specifies a community string, from 1-32 characters.

## Default

None

## Command Mode

Global Configuration

## snmp-server contact

---

Configure the contact information for the system.

## Syntax

- **default snmp-server contact**
- **no snmp-server contact**
- **snmp-server contact WORD<0-255>**

## Command Parameters

**WORD<0-255>**

Changes the sysContact information for the switch. WORD<0-255> is an ASCII string from 0-255 characters (for example a phone extension or e-mail address.)

## Default

None



## Command Mode

Global Configuration

### snmp-server force-iphdr-sender enable

---

Configure the SNMP and IP sender flag to the same value.

#### Syntax

- **default snmp-server force-iphdr-sender**
- **default snmp-server force-iphdr-sender enable**
- **no snmp-server force-iphdr-sender**
- **no snmp-server force-iphdr-sender enable**
- **snmp-server force-iphdr-sender enable**

#### Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

### snmp-server force-trap-sender enable

---

Send the configured source address (sender IP as the sender network in the notification message).

#### Syntax

- **default snmp-server force-trap-sender**
- **default snmp-server force-trap-sender enable**
- **no snmp-server force-trap-sender**
- **no snmp-server force-trap-sender enable**
- **snmp-server force-trap-sender enable**

#### Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## snmp-server group

Create a new user group member to logically group users who require the same level of access. Create new access for a group in the View-based Access Control Model (VACM) table to provide access to managed objects.

## Syntax

- `no snmp-server group WORD<1-32>`
- `no snmp-server group WORD<1-32> WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-no-priv`
- `snmp-server group WORD<1-32> WORD<0-32> auth-no-priv notify-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-no-priv read-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-no-priv write-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-priv`
- `snmp-server group WORD<1-32> WORD<0-32> auth-priv notify-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-priv read-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-priv write-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> no-auth-no-priv`
- `snmp-server group WORD<1-32> WORD<0-32> no-auth-no-priv notify-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> no-auth-no-priv read-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> no-auth-no-priv write-view WORD<0-32>`

## Command Parameters

auth-no-priv

Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the auth-no-priv parameter is included, it creates one entry for SNMPv3 access.

**auth-priv**

Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the auth-priv parameter is included, it creates one entry for SNMPv3 access.

**group WORD<1-32>**

Assigns the group name for data access. The range is 1-32 characters. Use the no operator to remove this configuration.

**no-auth-no-priv**

Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the no-auth-no-priv parameter is included, it creates three entries, one for SNMPv1, one for SNMPv2c access, and one for SNMPv3c access.

**notify-view WORD<0-32>**

Specifies the view name in the range of 0-32 characters.

**read-view WORD<0-32>**

Specifies the view name in the range of 0-32 characters.

**WORD<1-32> WORD<1-32>**

The first WORD<1-32> specifies the group name for data access.

The second WORD<1-32> specifies the context name.

If you use a particular group name value but with different context names, you create multiple entries for different contexts for the same group. You can omit the context name and use the default. If the context name value ends in the wildcard character (\*), the resulting entries match a context name that begins with that context. For example, a context name value of foo\* matches contexts starting with foo, such as foo6 and fofofum.

Use the no operator to remove this configuration.

**write-view WORD<0-32>**

Specifies the view name in the range of 0-32 characters.

## Default

None

## Command Mode

Global Configuration

## snmp-server host v1

---

Configure an SNMP host so that the switch can forward SNMP traps to a host for monitoring.

## Syntax

- `no snmp-server host WORD<1-256> port <1-65535> v1 WORD<1-32>`
- `no snmp-server host WORD<1-256> v1 WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v1 WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v1 WORD<1-32> filter WORD<1-32>`
- `snmp-server host WORD<1-256> v1 WORD<1-32>`
- `snmp-server host WORD<1-256> v1 WORD<1-32> filter WORD<1-32>`

## Command Parameters

`filter WORD<1-32>`

Specifies a filter profile name.

`port<1-65535>`

Specifies the host server port number.

`v1 WORD <1-32> [filter WORD<1-32>]`

Specifies the SNMP v1 security name.

`WORD<1-256>`

Specifies either an IPv4 or IPv6 address.

## Default

None

## Command Mode

Global Configuration

## snmp-server host v2

Configure an SNMPv2 host so that the switch can forward SNMP traps to a host for monitoring.

## Syntax

- `default snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32>`
- `default snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> mms`
- `default snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> retries`
- `default snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> timeout`
- `default snmp-server host WORD<1-256> v2c WORD<1-32>`
- `default snmp-server host WORD<1-256> v2c WORD<1-32> mms`
- `default snmp-server host WORD<1-256> v2c WORD<1-32> retries`

- `default snmp-server host WORD<1-256> v2c WORD<1-32> timeout`
- `no snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32>`
- `no snmp-server host WORD<1-256> v2c WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> filter WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> inform`
- `snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> inform mms <0-2147483647>`
- `snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> inform retries <0-255>`
- `snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> inform timeout <1-2147483647>`
- `snmp-server host WORD<1-256> v2c WORD<1-32>`
- `snmp-server host WORD<1-256> v2c WORD<1-32> filter WORD<1-32>`
- `snmp-server host WORD<1-256> v2c WORD<1-32> inform`
- `snmp-server host WORD<1-256> v2c WORD<1-32> inform mms <0-2147483647>`
- `snmp-server host WORD<1-256> v2c WORD<1-32> inform retries <0-255>`
- `snmp-server host WORD<1-256> v2c WORD<1-32> inform timeout <1-2147483647>`

## Command Parameters

`filter WORD<1-32>`

Specifies a filter profile name.

`inform`

Specifies the notify type.

`mms <0-2147483647>`

Specifies the maximum message size.

`port <1-65535>`

Specifies the port number that needs to be changed.

`retries <0-255>`

Specifies the number of retries.

`timeout <1-2147483647>`

Specifies the timeout value.

`v2c WORD<1-32>`

Specifies the SNMPv2 security name

`WORD<1-256>`

Specifies the IPv4 or IPv6 host address.

## Default

None

## Command Mode

Global Configuration

## snmp-server host v3

Configure an SNMPv3 host so that the switch can forward SNMP traps to a host for monitoring.

## Syntax

- `default snmp-server host WORD<1-256> port <1-65535> v3 WORD<1-32>`
- `default snmp-server host WORD<1-256> port <1-65535> v3 WORD<1-32> retries`
- `default snmp-server host WORD<1-256> port <1-65535> v3 WORD<1-32> timeout`
- `default snmp-server host WORD<1-256> v3 WORD<1-32>`
- `default snmp-server host WORD<1-256> v3 WORD<1-32> retries`
- `default snmp-server host WORD<1-256> v3 WORD<1-32> timeout`
- `no snmp-server host WORD<1-256> port <1-65535> v3 WORD<1-32>`
- `no snmp-server host WORD<1-256> v3 WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> filter WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform retries <0-255>`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform timeout <1-2147483647>`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32>`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> filter WORD<1-32>`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform retries <0-255>`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform timeout <1-2147483647>`

## Command Parameters

**{noAuthNoPriv|authNoPriv|authPriv}**

Specifies the security level.

**filter WORD<1-32>**

Specifies a filter profile name.

**inform**

Specifies the notify type.

**mms <0-2147483647>**

Specifies the maximum message size.

**port <1-65535>**

Specifies the port number that needs to be changed.

**retries <0-255>**

Specifies the number of retries.

**timeout <1-2147483647>**

Specifies the timeout value.

**v3c WORD<1-32>**

Specifies the SNMPv3 security name

**WORD<1-256>**

Specifies the IPv4 or IPv6 host address.

## Default

None

## Command Mode

Global Configuration

## snmp-server location

---

Configure the sysLocation information for the system. <WORD 0-255> is an ASCII string from 0-255 characters.

## Syntax

- **default snmp-server location**
- **no snmp-server location**
- **snmp-server location WORD<0-255>**

## Command Parameters

**WORD <0-255>**

Specifies an ASCII string from 0-255 characters.

## Default

None

## Command Mode

Global Configuration

---

## snmp-server login-success-trap enable

Configure the generation of login success traps.

## Syntax

- **default snmp-server login-success-trap**
- **no snmp-server login-success-trap**
- **snmp-server login-success-trap enable**

## Default

The default is disabled/false.

## Command Mode

Global Configuration

---

## snmp-server name

Configure the sysName information for the system. WORD<0-255> is an ASCII string from 0-255 characters.

## Syntax

- **default snmp-server name**
- **no snmp-server name**
- **snmp-server name WORD<0-255>**

## Command Parameters

WORD <0255>

Specifies an ASCII string from 0-255 characters.



## Default

None

## Command Mode

Global Configuration

---

## snmp-server notify-filter

Configure the notify table to select management targets to receive notifications, as well as the type of notification to send to each management target.

## Syntax

- **no snmp-server notify-filter WORD<1-32> WORD<1-32>**
- **snmp-server notify-filter WORD<1-32> WORD<1-32>**

## Command Parameters

WORD<1-32> WORD<1-32>

The first WORD<1-32> specifies the name of the filter profile.

The second WORD<1-32> identifies the filter subtree OID. If the Subtree OID uses a '+' prefix (or no prefix), this indicates include. The '-' prefix, this indicates exclude.

## Default

None

## Command Mode

Global Configuration

---

## snmp-server sender-ip

Configure the IP interface from which the SNMP traps originate if the switch has multiple interfaces. This command applies to in-band management cases only. In case of out-of-band management, any configuration of the command is ignored.

## Syntax

- **snmp-server sender-ip {A.B.C.D} {w.x.y.z}**

## Command Parameters

{A.B.C.D} {w.x.y.z}

For in-band management case: Specifies the source IP address (w.x.y.z) to use when sending the Trap notification packet to the SNMP server <A.B.C.D>. This command only applies when the force-trap-sender parameter is enabled. Moreover, the source IP (w.x.y.z) must be a CLIP address.



#### Note

If the source IP address is either specified as 0.0.0.0 or is not a CLIP address, the source IP address is ignored and the switch automatically uses the IP address of the local interface that is closest (from an IP routing table perspective) to the destination SNMP server and the settings from this command are ignored.

If the reachability to the SNMP server is over an IS-IS/SPB IP shortcut NNI, the switch automatically uses the IS-IS IP source address and the settings from this command are ignored.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## snmp-server user

---

Create a user on the local system in the USM table to authorize a user on a particular SNMP engine.

## Syntax

- **no snmp-server user WORD<1-32>**
- **snmp-server user WORD<1-32>**

## Command Parameters

**WORD<1-32>**

Specifies the group access name.

## Default

None

## Command Mode

Global Configuration

### snmp-server user WORD<1-32> group

---

Add a user to a group to logically group users who require the same level of access.

#### Syntax

- **snmp-server user WORD<1-32> [group WORD<1-32>]**
- **snmp-server user WORD<1-32> [group WORD<1-32>] [md5]**
- **snmp-server user WORD<1-32> [group WORD<1-32>] [md5] [aes | des]**
- **snmp-server user WORD<1-32> [group WORD<1-32>] [sha]**
- **snmp-server user WORD<1-32> [group WORD<1-32>] [sha] [aes | des]**

#### Command Parameters

**group WORD<1-32>**

Specifies the group access name.

**md5**

Specifies an authentication protocol. If no value is entered, no authentication capability exists.

**sha**

Specifies an authentication protocol. If no value is entered, no authentication capability exists.

**aes**

Specifies a privacy protocol. If no value is entered, no authentication capability exists.

**des**

Specifies a privacy protocol. If no value is entered, no authentication capability exists.

#### Default

None.

## Command Mode

Global Configuration

### snmp-server user engine-id

---

Create a new user in the USM table to authorize a user on a particular SNMP engine.

## Syntax

- `no snmp-server user engine-id WORD<16-97>`
- `snmp-server user engine-id WORD<16-97>`
- `snmp-server user engine-id WORD<16-97> WORD<1-32>`
- `snmp-server user engine-id WORD<16-97> WORD<1-32> [md5 | sha]`
- `snmp-server user engine-id WORD<16-97> WORD<1-32> [md5] [aes | des]`
- `snmp-server user engine-id WORD<16-97> WORD<1-32> [sha]`
- `snmp-server user engine-id WORD<16-97> WORD<1-32> [sha] [aes | des]`

## Command Parameters

### md5

Specifies an authentication protocol. If no value is entered, no authentication capability exists.

### sha

Specifies an authentication protocol. If no value is entered, no authentication capability exists.

### aes

Specifies a privacy protocol. If no value is entered, no authentication capability exists.

### des

Specifies a privacy protocol. If no value is entered, no authentication capability exists.

## Default

None

## Command Mode

Global Configuration

## snmp-server user WORD<1-32> md5

Create a user on a remote system with MD5.

## Syntax

- `snmp-server user WORD<1-32> md5`
- `snmp-server user WORD<1-32> md5 [aes]`
- `snmp-server user WORD<1-32> md5 [aes] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [aes] [read-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [aes] [read-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [aes] [read-view WORD<0-32>] [write-view WORD<0-32>]`

- `snmp-server user WORD<1-32> md5 [aes] [read-view WORD<0-32>] [write-view WORD<0-32>] [notify-view]`
- `snmp-server user WORD<1-32> md5 [aes] [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [aes] [write-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [des]`
- `snmp-server user WORD<1-32> md5 [des] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [des] [read-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [des] [read-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [des] [read-view WORD<0-32>] [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [des] [read-view WORD<0-32>] [write-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [des] [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [des] [write-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [read-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [read-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [read-view WORD<0-32>] [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [read-view WORD<0-32>] [write-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> md5 [write-view WORD<0-32>] [notify-view]`

## Command Parameters

### md5

Specifies an authentication protocol. If no value is entered, no authentication capability exists.

### aes

Specifies a privacy protocol. If no value is entered, no authentication capability exists.

### des

Specifies a privacy protocol. If no value is entered, no authentication capability exists.

### notify-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

### read-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

#### **write-view WORD<0-32>**

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

### Default

None

### Command Mode

Global Configuration

---

## **snmp-server user WORD<1-32> notify-view**

Specify a view name for the created user on the local system in the USM table.

### Syntax

- **snmp-server user WORD<1-32> notify-view WORD<0-32>**

### Command Parameters

#### **notify-view WORD<0-32>**

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

### Default

None

### Command Mode

Global Configuration

---

## **snmp-server user WORD<1-32> read-view**

Specify a view name for the created user on the local system in the USM table.

### Syntax

- **snmp-server user WORD<1-32> [read-view WORD<1-32>]**
- **snmp-server user WORD<1-32> [read-view WORD<1-32>] [notify-view WORD<0-32>]**

- **snmp-server user WORD<1-32> [read-view WORD<0-32>] [write-view WORD<0-32>]**
- **snmp-server user WORD<1-32> [read-view WORD<0-32>] [write-view WORD<0-32>] [notify-view WORD<0-32>]**

## Command Parameters

### notify-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

### read-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

### write-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

## Default

None

## Command Mode

Global Configuration

## snmp-server user WORD<1-32> sha

Create a user on a remote system with sha.

## Syntax

- **snmp-server user WORD<1-32> sha**
- **snmp-server user WORD<1-32> sha [aes]**
- **snmp-server user WORD<1-32> sha [aes] [notify-view WORD<0-32>]**
- **snmp-server user WORD<1-32> sha [aes] [read-view WORD<0-32>]**
- **snmp-server user WORD<1-32> sha [aes] [read-view WORD<0-32>] [notify-view WORD<0-32>]**
- **snmp-server user WORD<1-32> sha [aes] [read-view WORD<0-32>] [write-view WORD<0-32>]**
- **snmp-server user WORD<1-32> sha [aes] [read-view WORD<0-32>] [write-view WORD<0-32>] [notify-view]**
- **snmp-server user WORD<1-32> sha [aes] [write-view WORD<0-32>]**
- **snmp-server user WORD<1-32> sha [aes] [write-view WORD<0-32>] [notify-view WORD<0-32>]**

- `snmp-server user WORD<1-32> sha [des]`
- `snmp-server user WORD<1-32> sha [des] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [des] [read-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [des] [read-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [des] [read-view WORD<0-32>] [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [des] [read-view WORD<0-32>] [write-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [des] [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [des] [write-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [read-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [read-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [read-view WORD<0-32>] [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [read-view WORD<0-32>] [write-view WORD<0-32>] [notify-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [write-view WORD<0-32>]`
- `snmp-server user WORD<1-32> sha [write-view WORD<0-32>] [notify-view]`

## Command Parameters

### sha

Specifies an authentication protocol. If no value is entered, no authentication capability exists.

### aes

Specifies a privacy protocol. If no value is entered, no authentication capability exists.

### des

Specifies a privacy protocol. If no value is entered, no authentication capability exists.

### notify-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

### read-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

### write-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.



## Default

None

## Command Mode

Global Configuration

---

## snmp-server user WORD<1-32> write-view

Specify a view name for the created user on the local system in the USM table.

## Syntax

- **snmp-server user WORD<1-32> [write-view WORD<0-32>]**
- **snmp-server user WORD<1-32> [write-view WORD<0-32>] [notify-view WORD<0-32>]**

## Command Parameters

### notify-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

### write-view WORD<0-32>

Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.

## Default

None

## Command Mode

Global Configuration

---

## snmp-server view

Create a new entry in the MIB view table. The default Layer 2 MIB view cannot modify SNMP settings. However, a new MIB view created with Layer 2 permission can modify SNMP settings.

## Syntax

- **no snmp-server view WORD<1-32> WORD<1-32>**
- **snmp-server view WORD <1-32> WORD <1-32>**

## Command Parameters

**WORD <1-32>**

Specifies a new entry with this group name. The range is 1-32 characters.

**WORD <1-32> WORD<1-32>**

Specifies the prefix that defines the set of MIB objects accessible by this SNMP entity. The range is 1-32 characters.

## Default

None

## Command Mode

Global Configuration

---

## spanning-tree mstp forward-time

Configure the MSTP forward delay for the bridge.

## Syntax

- **default spanning-tree mstp forward-time**
- **spanning-tree mstp forward-time <400-3000>**

## Command Parameters

**<400-3000>**

Configures the MSTP forward delay for the bridge, in hundredths of a second.

## Default

None

## Command Mode

Global Configuration

---

## spanning-tree mstp max-age

Assign the MSTP maximum age time for the bridge

## Syntax

- **default spanning-tree mstp max-age**
- **spanning-tree mstp max-age <600-4000>**

## Command Parameters

<600-4000>

Assigns the MSTP maximum age time for the bridge, in one hundredths of a second.

## Default

The default is 2000.

## Command Mode

Global Configuration

---

## spanning-tree mstp max-hop

Assign the maximum hop count for the bridge.

## Syntax

- **default spanning-tree mstp max-hop**
- **spanning-tree mstp max-hop <100-4000>**

## Command Parameters

<100-4000>

Assigns the MSTP bridge maximum hop count. The range is 100 to 4000 one hundredths of a second.

## Default

The default is 2000.

## Command Mode

Global Configuration

---

## spanning-tree mstp msti (globally)

Configure Multiple Spanning Tree Protocol (MSTP) to set the MSTP configuration version.

## Syntax

- **default spanning-tree mstp msti <1-63>**
- **default spanning-tree mstp msti <1-63> priority**
- **spanning-tree mstp msti <1-63> priority <0-65535>**

## Command Parameters

<1-63>

Specifies the instance parameter.

**priority** <0-65535>

Configures the MSTP bridge priority. Allowed values are:

- 4096
- 8192
- 12288
- 16384
- 20480
- 24576
- 28672
- 32768
- 36864
- 40960
- 45056
- 49152
- 53248
- 57344
- 61440

## Default

None

## Command Mode

Global Configuration

## spanning-tree mstp pathcost-type

---

Assign the Multiple Spanning Tree Protocol (MSTP) default pathcost version.

## Syntax

- **default spanning-tree mstp pathcost-type**
- **spanning-tree mstp pathcost-type bits16**
- **spanning-tree mstp pathcost-type bits32**

## Command Parameters

<bits16|bits32>

Specifies the pathcost value.

## Default

The default is 32 bits.

## Command Mode

Global Configuration

# spanning-tree mstp priority (globally)

---

Assign the Multiple Spanning Tree Protocol (MSTP) bridge priority.

## Syntax

- **default spanning-tree mstp priority**
- **spanning-tree mstp priority <0-61440>**

## Command Parameters

**<0-61440>**

Assigns the MSTP bridge priority. The values configured for port priority must be in steps of 4096.

## Default

The default is 32768.

## Command Mode

Global Configuration

# spanning-tree mstp region

---

Assign the Multiple Spanning Tree Protocol (MSTP) region.

## Syntax

- **default spanning-tree mstp region**
- **default spanning-tree mstp region config-id-sel**
- **default spanning-tree mstp region region-name**
- **default spanning-tree mstp region region-version**
- **spanning-tree mstp region config-id-sel <0-255>**
- **spanning-tree mstp region region-name WORD<1-32>**
- **spanning-tree mstp region region-version <0-65535>**

## Command Parameters

**config-id-sel** <0-255>

Assigns the MSTP region configuration ID number.

**region-name** WORD<1-32>

Assigns the MSTP region name.

**region-version** <0-65535>

Assigns the MSTP region version.

## Default

The default region and version is 0.

## Command Mode

Global Configuration

## spanning-tree mstp tx-holdcount

---

Assign the Multiple Spanning Tree Protocol (MSTP) transmit hold count.

## Syntax

- **default spanning-tree mstp tx-holdcount**
- **spanning-tree mstp tx-holdcount <1-10>**

## Command Parameters

<1-10>

Assigns the MSTP transmit hold count.

## Default

The default is 3.

## Command Mode

Global Configuration

## spanning-tree mstp version

---

Assigns the bridge version.

## Syntax

- **default spanning-tree mstp version**
- **spanning-tree mstp version mstp**
- **spanning-tree mstp version rstp**
- **spanning-tree mstp version stp-compatible**

## Command Parameters

### mstp

Configures the version as MSTP.

### rstp

Configures the version as RSTP.

### stp-compatible

Configures the version as STP compatible.

Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A switch in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Nortel STP. MSTP spanning tree groups are not the same as Nortel STP spanning tree groups.

Using a switch in MSTP mode with another chassis in STP mode can create a loop in the network. You must configure protocol migration to true on all spanning-tree enabled interfaces when you change the spanning tree version from STP-compatible to MSTP for those interfaces to work in the proper mode.

## Default

The default is MSTP.

## Command Mode

Global Configuration

## spanning-tree rstp forward-time

---

Configure the Rapid Spanning Tree Protocol (RSTP) forward delay for the bridge.

## Syntax

- **default spanning-tree rstp forward-time**
- **spanning-tree rstp forward-time <400-3000>**

## Command Parameters

<400-3000>

Configures the RSTP forward delay for the bridge, in hundredths of a second.

## Default

The default is 1500 (15 seconds).

## Command Mode

Global Configuration

---

## spanning-tree rstp group-stp enable

Enable or disables Rapid Spanning Tree Protocol (RSTP) for a specific STG.

## Syntax

- **default spanning-tree rstp group-stp enable**
- **no spanning-tree rstp group-stp enable**
- **spanning-tree rstp group-stp enable**

## Default

The default value is enabled.

## Command Mode

Global Configuration

---

## spanning-tree rstp hello-time

Configure the hello-time delay for the bridge.

## Syntax

- **default spanning-tree rstp hello-time**
- **spanning-tree rstp hello-time <100-1000>**

## Command Parameters

<100-1000>

Configures the hello-time for a port in one hundredths of a second.

## Default

The default is 200 (2 seconds).

## Command Mode

Global Configuration



---

## spanning-tree rstp max-age

---

Assign the Rapid Spanning Tree Protocol (RSTP) maximum age time for the bridge

### Syntax

- **default spanning-tree rstp max-age**
- **spanning-tree rstp max-age <600-4000>**

### Command Parameters

<600-4000>

Assigns the RSTP maximum age time for the bridge, in one hundredths of a second.

### Default

The default value is 2000 (2 seconds).

### Command Mode

Global Configuration

---

## spanning-tree rstp pathcost-type

---

Assign the Rapid Spanning Tree Protocol (RSTP) default pathcost version.

### Syntax

- **default spanning-tree rstp pathcost-type**
- **spanning-tree rstp pathcost-type bits16**
- **spanning-tree rstp pathcost-type bits32**

### Command Parameters

<bits16|bits32>

Specifies the pathcost value.

### Default

The default is 32 bits.

### Command Mode

Global Configuration

---

## spanning-tree rstp priority (globally)

---

Assign the Rapid Spanning Tree Protocol (RSTP) bridge priority.

### Syntax

- `default spanning-tree rstp priority`
- `spanning-tree rstp priority <0-61440>`

### Command Parameters

`<0-61440>`

Assigns the RSTP bridge priority in a range of 0 to 61440 in steps of 4096.

### Default

The default is 32768.

### Command Mode

Global Configuration

---

## spanning-tree rstp tx-holdcount

---

Assign the Rapid Spanning Tree Protocol (RSTP) transmit hold count.

### Syntax

- `default spanning-tree rstp tx-holdcount`
- `spanning-tree rstp tx-holdcount <1-10>`

### Command Parameters

`<1-10>`

Assigns the RSTP transmit hold count.

### Default

The default is 6.

### Command Mode

Global Configuration

---

## spanning-tree rstp version

---

Configure the Rapid Spanning Tree Protocol (RSTP) to set the RSTP configuration.

### Syntax

- **default spanning-tree rstp version**
- **spanning-tree rstp version rstp**
- **spanning-tree rstp version stp-compatible**

### Command Parameters

**rstp**

Configures the version as RSTP.

**stp-compatible**

Configures the version as STP-compatible.

### Default

The default is RSTP.

### Command Mode

Global Configuration

---

## spanning-tree tc-receive-alarm-threshold count

---

Specifies the number of packets used to establish the threshold rate.

### Syntax

- **default spanning-tree tc-receive-alarm-threshold count**
- **spanning-tree tc-receive-alarm-threshold count <1-1000>**

### Command Parameters

**count <1-1000>**

Specifies the number of packets used to establish the threshold rate. The default is 2.

### Default

The default is 2.

### Command Mode

Global Configuration

---

## spanning-tree tc-receive-alarm-threshold interval

---

Specifies the time interval (in minutes) used to establish the threshold rate.

### Syntax

- **default spanning-tree tc-receive-alarm-threshold interval**
- **spanning-tree tc-receive-alarm-threshold interval <1-15>**

### Command Parameters

**interval <1-15>**

Specifies the time interval (in minutes) used to establish the threshold rate. The default is 1.

### Default

The default is 1.

### Command Mode

Global Configuration

---

## spbm

---

Enable Shortest Path Bridging MAC (SPBM) globally.

### Syntax

- **default spbm**
- **no spbm**
- **spbm**

### Default

The default is disabled.

### Command Mode

Global Configuration

### Usage Guidelines

To ensure proper cleanup of MAC tables after you run the **no spbm** command, save the configuration, and then reboot the switch.

## spbm ethertype

---

Configure the ethertype for Shortest Path Bridging MAC (SPBM).

### Syntax

- **default spbm ethertype**
- **spbm ethertype 0x8100**
- **spbm ethertype 0x88a8**

### Command Parameters

**0x8100**

Configures the ethertype to 0x8100.

**0x88a8**

Configures the ethertype to 0x88a8.

### Default

The default is 0x8100.

### Command Mode

Global Configuration

## spbm nick-name server

---

Enable a dynamic nickname server.

### Syntax

- **no spbm nick-name server**
- **spbm nick-name server**

### Default

Disabled

### Command Mode

Global Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## spbm nick-name server prefix

---

Configure a nickname allocation prefix.

### Syntax

- `default spbm nick-name server prefix`
- `spbm nick-name server prefix x.xx.xx`

### Command Parameters

x.XX.XX

Specifies the nickname server allocation prefix. x.xx.xx uses the form X.X0.00 from 0.00.00 to F.F0.00. An interval, X.X0.00 to X.XF.FF, can provide up to 4,000 nicknames.

### Default

The default nickname allocation range is A.00.00-A.0F.FF.

### Command Mode

Global Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ssh (configuration)

---

Modify Secure Shell (SSH) configuration parameters to support public and private key encryption connections.

### Syntax

- `default ssh [dsa-auth] [max-sessions] [pass-auth] [port] [rekey data-limit] [rekey enable] [rekey time-interval] [rsa-auth] [secure] [timeout] [version] [x509v3-auth enable] [x509v3-auth revocation-check-method] [x509v3-auth username overwrite] [x509v3-auth username strip-domain] [x509v3-auth username use-domain]`
- `no ssh [authentication-type] [authentication-type aead-aes-128-gcm-ssh] [authentication-type aead-aes-256-gcm-ssh] [authentication-type hmac-sha1] [authentication-type hmac-sha2-256] [dsa-auth] [dsa-host-key] [dsa-user-key WORD<1-15>] [encryption-type] [encryption-type 3des-cbc] [encryption-type aead-aes-128-gcm-ssh] [encryption-type aead-aes-256-gcm-ssh] [encryption-type aes128-cbc] [encryption-type aes128-ctr] [encryption-type aes192-cbc] [encryption-type aes192-ctr]`

- ```
[encryption-type aes256-cbc] [encryption-type aes256-ctr] [encryption-type
blowfish-cbc] [encryption-type rijndael128-cbc] [encryption-type
rijndael192-cbc] [key-exchange-method] [key-exchange-method diffie-
hellman-group14-sha1] [key-exchange-method diffie-hellman-group-
exchange-sha256] [pass-auth] [rekey enable] [rsa-auth] [rsa-host-key]
[rsa-user-key WORD<1-15>] [secure] [x509v3-auth enable] [x509v3-auth
username overwrite] [x509v3-auth username strip-domain] [x509v3-auth
username use-domain]
```
- `ssh` [authentication-type aead-aes-128-gcm-ssh] [authentication-type aead-aes-256-gcm-ssh] [authentication-type hmac-sha1] [authentication-type hmac-sha2-256] [dsa-auth] [dsa-host-key] [dsa-host-key <1024-1024>] [dsa-user-key WORD<1-15>] [dsa-user-key WORD<1-15> size <1024-1024>] [encryption-type 3des-cbc] [encryption-type aead-aes-128-gcm-ssh] [encryption-type aead-aes-256-gcm-ssh] [encryption-type aes128-cbc] [encryption-type aes128-ctr] [encryption-type aes192-cbc] [encryption-type aes192-ctr] [encryption-type aes256-cbc] [encryption-type aes256-ctr] [encryption-type blowfish-cbc] [encryption-type rijndael128-cbc] [encryption-type rijndael192-cbc] [key-exchange-method diffie-hellman-group14-sha1] [key-exchange-method diffie-hellman-group-exchange-sha256] [max-sessions <0-8>] [pass-auth] [port <22, 1024..49151>] [reset] [rekey data-limit <1-6>] [rekey enable] [rekey time-interval <1-6>] [rsa-auth] [rsa-host-key] [rsa-host-key <1024-2048>] [rsa-user-key WORD<1-15>] [secure] [timeout <1-120>] [version v2only] [x509v3-auth enable] [x509v3-auth revocation-check-method none] [x509v3-auth revocation-check-method ocsp] [x509v3-auth username overwrite] [x509v3-auth username strip-domain] [x509v3-auth username use-domain WORD<1-254>]

## Command Parameters

`authentication-type` [aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [hmac-sha1] [hmac-sha2-256]

Specifies the authentication type.

`data-limit` <1-6>

Specifies the rekey data limit in Gigabytes (GB).

`dsa-auth`

Enables or disables the DSA authentication.

`dsa-host-key` <1024-1024>

Generates an SSH DSA host key. The range of the host key size is 512 to 1024. The default is 1024. The range depends on your hardware.

`dsa-user-key` WORD<1-15> <1024-1024>]

Creates the DSA user key file. WORD<1-15> specifies the user access level. If you configured enhanced secure mode the access levels are: admin|operator|auditor|security|priv.

In enhanced secure mode access level is role based. If you do not enable enhanced secure mode, the valid user access levels are:

- rwa for read-write-all
- rw for read-write
- ro for read-only
- rwl3 for read-write for Layer 3
- rwl2 for read-write for Layer 2
- rwl1 for Layer 1

The default size is 1024 bits. The range depends on your hardware.

**key-exchange-method** [diffie-hellman-group14-sha1][diffie-hellman-group-exchange-sha256]

Specifies the key-exchange type.

**max-sessions** <0-8>

Specifies the maximum number of SSH sessions allowed. A value from 0 to 8. Default is 4.

**pass-auth**

Enables password authentication.

**port** <22, 1024..49151>

Sets the Secure Shell (SSH) connection port. <22,1024..49151> is the TCP port number. The default is 22.

**reset**

Reset (bounce) the Secure Shell (SSH) connection.

**rsa-auth**

Enable RSA authentication.

**rsa-host-key** <1024-2048>

Generates the SSH RSA host key. The range of the SSH host key size is 512 to 2048. The default is 2048.

**rsa-user-key** [<1024-2048>]

Generates a new SSH RSA user key.

**secure**

Enables Secure Shell (SSH) in secure mode and immediately disables the access services SNMP, FTP, TFTP, rlogin, and Telnet.



**Note**

rlogin is only supported on VSP 8600 Series.

After ssh secure is enabled, you can choose to enable individual non-secure protocols. However, after you save the configuration and restart the system, the non-secure protocol is again disabled, even though it is shown as enabled in the configuration file.

After you enable ssh secure, you cannot enable non-secure protocols by disabling ssh secure.



`encryption-type` [`3des-cbc`][`aead-aes-128-gcm-ssh` ][`aead-aes-256-gcm-ssh`] [`aes128-cbc`]  
[`aes128-ctr`][`aes192-cbc`][`aes192-ctr`][`aes256-cbc`][`aes256-ctr`][`blowfish-cbc`] [`rijndael128-cbc`]  
[`rijndael192-cbc`]

Specifies the encryption-type.

`time-interval` <1-6>

Specifies the rekey time interval in hours.

`timeout` <1-120>

The Secure Shell (SSH) connection authentication timeout in seconds. Default is 60 seconds.

`version` <v2only>

Sets the Secure Shell (SSH) version. The default is v2only.

`x509v3-auth` {[`enable`][`revocation-check-method` <none | ocsp>]}[`username` <overwrite | strip-domain | use-domain WORD<1-254>]}

Specifies the Secure Shell (SSH) X.509 V3 authentication configuration for Two-Factor Authentication.

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

**x509v3-auth** is available for demonstration purposes on some products. For more information, see [VOSS User Guide](#).

The key exchange method `diffie-hellman-group-exchange-sha256` is not supported on VSP 8600 Series

## ssh client

---

Configures the SSH client parameter.

## Syntax

- **default ssh client enable**
- **no ssh client enable**
- **ssh client enable**

## Command Parameters

**enable**

Enables SSH client.

## Default

Enabled

## Command Mode

Global Configuration

## ssh install-user-key

---

Import DSA and RSA Private or Public Keys.

## Syntax

- **ssh install-user-key WORD<1-15> {rwa | rw | ro | rwl1 | rwl2 | rwl3, enhanced-secured mode : admin | operator | auditor | security | priv } WORD<1-15> {public |private} WORD<1-15> {dsa | rsa}**
- **no ssh install-user-key**

## Command Parameters

WORD<1-15> {rwa | rw | ro | rwl1 | rwl2 | rwl3, enhanced-secured mode : admin | operator | auditor | security | priv }

Specifies the user access level.

You must enable SSH globally before you can generate SSH DSA user keys.

If enhanced secure mode is disabled, the valid user access levels for the switch are:

- rwa — Specifies read-write-all.
- rw — Specifies read-write.
- ro — Specifies read-only.
- rwl1 — Specifies read-write for Layer 1.
- rwl2 — Specifies read-write for Layer 2.
- rwl3 — Specifies read-write for Layer 3.

If you enable enhanced secure mode, the switch uses role-based authentication. You associate each username with a specific role and the appropriate authorization rights to commands based on that role.

If enhanced secure mode is enabled, the valid user access levels for the switch are:

- admin—Specifies a user role with access to all of the configurations, show commands, and the ability to view the log file and security commands. The administrator role is the highest level of user roles.
- operator—Specifies a user role with access to all of the configurations for packet forwarding on Layer 2 and Layer 3, and has access to show commands to view the configuration, but cannot view the audit logs and cannot access security and password commands.

- **auditor**—Specifies a user role that can view log files and view all configurations, except password configuration.
- **security**—Specifies a user role with access only to security settings and the ability to view the configurations.
- **priv**—Specifies a user role with access to all of the commands that the administrator has access to, and is referred to as an emergency-admin. However, the user with the privilege role must be authenticated within the switch locally. RADIUS and TACACS+ authentication is not accessible. A user role at the privilege level must login to the switch through the console port only.

**WORD<1-15> {public |private}**

Specifies the public key or the private key type to copy from `/intflash/shared` to `/intflash/.ssh`.

**WORD<1-15> {dsa | rsa}**

Specifies the DSA or RSA signature algorithm for the public key or the private key to copy.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command is not supported on VSP 8600 Series.

## ssh keyboard-interactive-auth

---

Configures the SSH server to use keyboard-interactive authentication. By default, keyboard-interactive authentication is disabled and the SSH server uses password authentication.

## Syntax

- **default ssh keyboard-interactive-auth**
- **no ssh keyboard-interactive-auth**
- **ssh keyboard-interactive-auth**

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## ssh rekey

---

Configure SSH rekey parameters on the switch. SSH Rekeying is a SSHv2 feature that allows the SSH server/client to force a key-exchange between server and client while changing the encryption and integrity keys.

### Syntax

- **default ssh rekey enable**
- **no ssh rekey enable**
- **ssh rekey enable**

### Command Parameters

**enable**

Enables SSH rekey on the switch.

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## ssh rekey data-limit

---

Configures SSH rekey data limit in GB.

### Syntax

- **default ssh rekey data-limit**
- **ssh rekey data-limit <1-6>**

### Command Parameters

**<1-6>**

Specifies the SSH rekey data limit in GB.

### Default

The default is 1 GB.

### Command Mode

Global Configuration

---

## ssh rekey time-interval

---

Sets SSH rekey time interval in hours.

### Syntax

- **default ssh rekey time-interval**
- **ssh rekey time-interval <1-6>**

### Command Parameters

<1-6>

Specifies the SSH rekey time interval in hours.

### Default

The default is 1 hour.

### Command Mode

Global Configuration

---

## ssh sftp

---

SSH is enabled when SFTP is disabled.

### Syntax

- **default ssh sftp**
- **no ssh sftp enable**
- **ssh sftp enable**

### Command Parameters

**enable**

Enables or disables ssh sftp. The default is enabled.

### Default

The default is enabled.

### Command Mode

Global Configuration

---

## ssh x509v3-auth ca-name

---

Configure the X.509 V3 Certificate Authority trustpoint.

### Syntax

- **ssh x509v3-auth ca-name WORD<1-45>**
- **no ssh x509v3-auth ca-name WORD<1-45>**

### Command Parameters

WORD<1-45>

Specifies the name of the X.509 V3 Certificate Authority trustpoint.

### Default

None

### Command Mode

Global Configuration Mode

### Usage Guidelines

This command is not supported on VSP 8600 Series.

---

## ssh x509v3-auth cert-subject-name

---

Configure the X.509 V3 digital certificate subject name to be used as the identity certificate.

### Syntax

- **ssh x509v3-auth cert-subject-name WORD<1-45>**
- **no ssh x509v3-auth cert-subject-name WORD<1-45>**

### Command Parameters

WORD<1-45>

Specifies the digital certificate subject name to be used as the identity certificate.

### Default

None

## Command Mode

Global Configuration Mode

## Usage Guidelines

This command is not supported on VSP 8600 Series.

## ssl certificate

---

Create and install a new self-signed SSL server certificate.

## Syntax

- **ssl certificate**
- **ssl certificate validity-period-in-days <30-3650>**

## Command Parameters

**validity-period-in-days <30-3650>**

Number of days for which the certificate remains valid.

## Default

The default is 365.

## Command Mode

Global Configuration

## ssl reset

---

Install current SSL server certificate.

## Syntax

- **ssl reset**

## Command Parameters

**reset**

Install current SSL server certificate; if missing, create and install a new self-signed certificate.

## Default

None

## Command Mode

Global Configuration

## sys clipId-topology-ip

---

Configure the circuitless IP (CLIP) ID as the topology IP.

### Syntax

- **default sys clipId-topology-ip**
- **no sys clipId-topology-ip**
- **sys clipId-topology-ip <1-256>**

### Command Parameters

<1-256>

Specifies the CLIP interface ID.

### Default

The default is 0.

## Command Mode

Global Configuration

### Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## sys control

---

Configure Linux system control TCP timestamp and TCP keepalive parameters.

### Syntax

- **default sys control tcp-timestamp**
- **no sys control tcp-timestamp**
- **sys control tcp-timestamp**
- **default sys control tcp-keepalive-interval**
- **sys control tcp-keepalive-interval <1-3600>**
- **default sys control tcp-keepalive-probes**
- **sys control tcp-keepalive-probes <1-50>**



- **default sys control tcp-keepalive-time**
- **sys control tcp-keepalive-time <5-65535>**

## Command Parameters

- **tcp-keepalive-interval <1-3600>**  
Configures the TCP keepalive interval. <1-3600> is the keepalive interval value in seconds.
- **tcp-keepalive-probes <1-50>**  
Configures the TCP keepalive probes. <1-50> is the number of keepalive probes.
- **tcp-keepalive-time <5-65535>**  
Configures the TCP keepalive time. <5-65535> is the keepalive time in seconds.
- **tcp-timestamp**  
Enables or disables the TCP timestamp.

## Default

The TCP timestamp default is enabled. You can disable tcp timestamp with the command **no sys control tcp-timestamp**. The system displays the following warning message when a new configuration is applied:

```
Warning: Existing TCP connections won't be affected. A config save and
reboot is required to apply this configuration for all TCP connections.
```

The TCP keepalive interval default is 10.

The TCP keepalive time default is 60.

The TCP keepalive probes default is 5.

## Command Mode

Global Configuration

## Usage Guidelines

The *tcp-keepalive-interval*, *tcp-keepalive-probes*, and *tcp-keepalive-time* parameters are not supported on VSP 8600 Series.

## sys control virtual-ist

---

Enable MAC move protection on virtual interswitch trunk (vIST).

## Syntax

- **sys control virtual-ist mac-move-protection**
- **no sys control virtual-ist mac-move-protection**

## Command Parameters

### mac-move-protection

Enables or disabled MAC move protection on v1ST.

## Default

The default value is enabled.

## Command Mode

Global Configuration

---

## sys default-ping-context

Configure the default context for executing **ping** commands and **traceroute** commands.

## Syntax

- **sys default-ping-context grt**
- **sys default-ping-context mgmt**
- **sys default-ping-context vrf WORD<1-64>**

## Command Parameters

### grt

Specifies the Global Router (grt) context as the default context for **ping** commands and **traceroute** commands.

### mgmt

Specifies the management (mgmt) context as the default context for **ping** commands and **traceroute** commands.

### vrf

Specifies the Virtual Router Forwarding (vrf) context as the default context for **ping** commands and **traceroute** commands.

### WORD<1-64>

Specifies the vrf name.

## Default

The default context is grt.

## Command Mode

Global Configuration

## Usage Guidelines

This command is not supported on VSP 8600 Series.

## sys force-msg

---

Use the force message control option to extend the message control feature functionality to the software and hardware log messages.

To enable the message control feature, you must specify an action, control interval, and maximum message number. After you enable the feature, the log messages, which get repeated and cross the maximum message number in the control interval, trigger the force message feature.

You can either suppress the message or send a trap notification, or both.

## Syntax

- **no sys force-msg WORD<4-4>**
- **sys force-msg WORD<4-4>**

## Command Parameters

**WORD<4-4>**

Adds a forced message control pattern.

WORD<4-4> is a string of 4 characters. You can add a four-byte pattern into the force-msg table. The software and the hardware log messages that use the first four bytes matching one of the patterns in the force-msg table undergo the configured message control action.

You can specify up to 32 different patterns in the force-msg table, including a wildcard pattern (\*\*\*). If you specify the wildcard pattern, all messages undergo message control.

## Default

None

## Command Mode

Global Configuration

## sys force-topology-ip-flag

---

Activate or disable the flag that Configure the CLIP ID as the topology IP.

## Syntax

- **default sys force-topology-ip-flag**
- **default sys force-topology-ip-flag enable**
- **no sys force-topology-ip-flag**

- **no sys force-topology-ip-flag enable**
- **sys force-topology-ip-flag**
- **sys force-topology-ip-flag enable**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

---

## sys locator-led

Enable or disable the switch Locator LED.

## Syntax

- **no sys locator-led**
- **sys locator-led**

## Default

The default is off.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

---

## sys msg-control

Configure system message control to suppress duplicate error messages on the console and to determine the action to take if they occur.

## Syntax

- **default sys msg-control**
- **default sys msg-control action**
- **default sys msg-control control-interval**
- **default sys msg-control max-msg-num**
- **no sys msg-control**
- **sys msg-control**
- **sys msg-control action both**
- **sys msg-control action send-trap**
- **sys msg-control action suppress-msg**
- **sys msg-control control-interval <1-30>**
- **sys msg-control max-msg-num <2-500>**

## Command Parameters

**action <both|send-trap| suppress-msg>**

Configures the message control action. You can either suppress the message or send a trap notification, or both. The default is suppress-msg.

**control-interval <1-30>**

Configures the message control interval in minutes. The default control-interval is 5.

**max-msg-num <2-500>**

Configures the number of occurrences of a message after which the control action occurs. The default is 5 messages.

## Default

None

## Command Mode

Global Configuration

## sys mtu

---

Enable support for jumbo frames on the switch.

## Syntax

- **default sys mtu**
- **sys mtu <1522-9600>**

## Command Parameters

<1522-9600>

Activates Jumbo frame support for the data path. The value can be 1522, 1950, or 9600 bytes. 1950 or 9600 bytes activate Jumbo frame support.

## Default

The default value is 1950 bytes.

## Command Mode

Global Configuration

---

## sys name

Configure system identification to specify the name of the switch.

## Syntax

- **default sys name**
- **sys name WORD<0-255>**

## Command Parameters

name WORD<0-255>

Configures the system or root level prompt name for the switch. WORD<0-255> is an ASCII string from 1-255 characters (for example, LabSC7 or Closet4).

## Default

The default differs depending on hardware platform.

## Command Mode

Global Configuration

---

## sys power slot

Enable power management. This command is not available on all hardware platforms.

## Syntax

- **default sys power slot <1-4|1-8|SF1-SF3>**
- **no sys power slot <1-4|1-8|SF1-SF3>**
- **sys power slot <1-4|1-8|SF1-SF3>**

## Command Parameters

<1-4|1-8|SF1-SF3>

Identifies the slot to supply power to.

## Default

None

## Command Mode

Global Configuration

---

## sys power slot-priority

Configure the priority of slots to shut down if there isn't enough power available. This command is not available on all hardware platforms.

## Syntax

- **default sys power slot-priority <3-8>**
- **sys power slot priority <3-8>**

## Command Parameters

<3-8>

Identifies the slot to prioritize.

## Default

None

## Command Mode

Global Configuration

---

## sys priv-exec-password

Enable authentication for the Privileged EXEC command mode for enhanced security.

## Syntax

- **sys priv-exec-password**
- **no sys priv-exec-password**
- **default sys priv-exec-password**

## Default

The default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

When you enable authentication for the Privileged EXEC CLI command mode, the changes do not affect any CLI sessions that are currently open. For the changes to take effect, you must first log out from your current CLI session and log back in on a new session.

## sys security-console

---

Configure the serial management ports to drop a connection that is interrupted for any reason. If you enable serial port dropping, the serial management ports drop the connection for the following reasons: modem power failure, link disconnection, and loss of the carrier.

Serial ports interrupted due to link disconnection, power failure, or other reasons force out the user and end the user session. Ending the user session ensures a maintenance port is not available with an active session that can allow unauthorized use by someone other than the authenticated user, and prevents the physical hijacking of an active session by unplugging the connected cable and plugging in another.

## Syntax

- **sys security-console**

## Default

The default is disabled if enhanced secure mode is disabled. The default is enabled if enhanced secure mode is enabled.

## Command Mode

Global Configuration

## sys software auto-commit

---

Enable the auto-commit feature for software upgrades.

If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires.

If you do not enable the auto-commit option, you must enter the software commit command before the commit timer expires to commit the new software version otherwise the system restarts automatically to the previous (committed) version.



## Syntax

- **default sys software auto-commit enable**
- **no sys software auto-commit enable**
- **sys software auto-commit enable**

## Default

The default is enabled.

## Command Mode

Global Configuration

---

## sys software commit-time

Configure the commit feature for software upgrades to allow maximum time to ensure that the upgrade is successful. You must enter the software commit command before the commit timer expires to commit the new software version otherwise the system restarts automatically to the previous (committed) version.

## Syntax

- **default sys software commit-time**
- **sys software commit-time <10-60>**

## Command Parameters

<10-60>

Specifies the commit timer in minutes.

## Default

The default is 10 minutes.



### Note

The VSP 8600 Series default is 15 minutes.

## Command Mode

Global Configuration

---

## sys system-default



### Note

This command is deprecated.

The following is an example of a log message that displays if you enter this command:

```
WARNING: The "sys-default" command has been deprecated. Please use the  
"boot config flags factorydefaults" command instead
```

Reset the switch to the default passwords and configuration.



#### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command. Only the user with the administrator role can use the command. After the administrator issues the command, the administrator must reboot the switch.

## Syntax

- **sys system-default**

## Default

None

## Command Mode

Global Configuration

## sys usb disable

---

Disable the USB drive.



#### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command. Only the user with the administrator role can use the command. After the administrator issues the command, the administrator must reboot the switch.

## Syntax

- **default sys usb disable**
- **no sys usb disable**
- **sys usb disable**

## Default

None

## Command Mode

Global Configuration

### sys usb enable

---

Enable the USB drive.



#### Note

You can only access this command after you enable enhanced secure mode using the boot config flags `enhancedsecure-mode` command. Only the user with the administrator role can use the command. After the administrator issues the command, the administrator must reboot the switch.

## Syntax

- **default sys usb enable**
- **no usb enable**
- **sys usb enable**

## Default

None

## Command Mode

Global Configuration

### sys vim-speed

---

Configure all of the ports on an installed Versatile Interface Module (VIM) to operate at the same speed.



#### Note

This command is not supported on all VIMs. Some VIMs must operate with all ports at the same speed, while others can operate with ports at different speeds. For more information, see [VSP 8600 Release Notes](#).

## Syntax

- **default sys vim-speed**
- **sys vim-speed {10000 | 25000}**

## Command Parameters

{10000 | 25000}

Configures all VIM ports to operate at either 10 Gbps or 25 Gbps.

## Default

The default is 25 Gbps.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

---

## syslog certificate

Configure the Certificate Authority trustpoint for the syslog.

## Syntax

- **syslog certificate ca-common-name WORD<1-45>**
- **no syslog certificate ca-common-name WORD<1-45>**

## Command Parameters

ca-common-name WORD<1-45>

Specifies the Certificate Authority common name.

## Default

None

## Command Mode

Global Configuration Mode

## Usage Guidelines

This command is not supported on VSP 8600 Series.

---

## syslog enable

The syslog commands enable or disable sending the logging message to remote syslog server.

## Syntax

- **default syslog enable**
- **no syslog enable**

- **syslog enable**

## Command Parameters

**enable**

Enables the sending of syslog messages on the switch.

## Default

The default is disabled.

## Command Mode

Global Configuration

## syslog host

---

Configure the syslog host and related parameters for sending the logging the message.

## Syntax

- **default syslog host <1-10>**
- **default syslog host <1-10> enable**
- **default syslog host <1-10> facility**
- **default syslog host <1-10> maperror**
- **default syslog host <1-10> mapfatal**
- **default syslog host <1-10> mapinfo**
- **default syslog host <1-10> mapwarning**
- **default syslog host <1-10> severity**
- **default syslog host <1-10> udp-port**
- **default syslog host <1-10>**
- **default syslog host <1-10> secure-forwarding mode**
- **default syslog host <1-10> secure-forwarding tcp-port**
- **no syslog host <1-10>**
- **no syslog host <1-10> enable**
- **no syslog host <1-10> secure-forwarding mode tls server-cert-nam**
- **syslog host <1-10>**
- **syslog host <1-10> address WORD<0-46>**
- **syslog host <1-10> enable**
- **syslog host <1-10> facility { local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 }**

- `syslog host <1-10> maperror { emergency | alert | critical | error | warning | notice | info | debug }`
- `syslog host <1-10> mapfatal { emergency | alert | critical | error | warning | notice | info | debug }`
- `syslog host <1-10> mapinfo { emergency | alert | critical | error | warning | notice | info | debug }`
- `syslog host <1-10> mapwarning { emergency | alert | critical | error | warning | notice | info | debug }`
- `syslog host <1-10> secure-forwarding mode none`
- `syslog host <1-10> secure-forwarding mode tls server-cert-name WORD<1-64>`
- `syslog host <1-10> severity { info | warning | error | fatal }`
- `syslog host <1-10> severity { info | warning | error | fatal } { info | warning | error | fatal }`
- `syslog host <1-10> severity { info | warning | error | fatal } { info | warning | error | fatal } { info | warning | error | fatal }`
- `syslog host <1-10> severity { info | warning | error | fatal } { info | warning | error | fatal } { info | warning | error | fatal } { info | warning | error | fatal }`
- `syslog host <1-10> udp-port <514-530>`
- `syslog host <1-10> secure-forwarding tcp-port <1025-49151>`

## Command Parameters

**address** WORD<0-46>

Configures a host location for the syslog host. WORD<0-46> is the IP address of the UNIX system syslog host.

**enable**

Enables the syslog host.

**facility** {local0|local1|local2|local3|local4|local5|local6|local7}

Specifies the UNIX facility used in messages to the syslog host. {local0|local1|local2|local3|local4|local5|local6|local7} is the UNIX system syslog host facility (LOCAL0 to LOCAL7).

**host**

Specifies host settings.

**maperror** {emergency|alert|critical|error|warning|notice|info|debug}

Specifies the syslog severity to use for Error messages.

**mapfatal** {emergency|alert|critical|error|warning|notice|info|debug}

Specifies the syslog severity to use for Fatal messages.

**mapinfo** {emergency|alert|critical|error|warning|notice|info|debug}

Specifies the syslog severity level to use for Information messages.

**mapwarning** {emergency|alert|critical|error|warning|notice|info|debug}

Specifies the syslog severity to use for Warning messages.

**secure-forwarding mode {none | tls server-certname WORD<1-64>}**

Specifies the mode of secure forwarding of syslog on the host. The default mode is none, that is, tls mode is disabled by default.

**secure-forwarding tcp-port <1025-49151>**

Set the tcp-port for secure forwarding of syslog for host. The default tcp-port is 1025. The tcp-port 6000 cannot be used, as it is used as an internal port for Internal Spanning Tree (IST).

**severity <info|warning|error|fatal>**

Specifies the severity levels for which syslog messages should be sent for the specified modules.

**udp-port <514-530>**

Specifies the UDP port number on which to send syslog messages to the syslog host. This is the UNIX system syslog host port number (514 to 530).

## Default

None

## Command Mode

Global Configuration

## syslog ip-header-type

---

Configure the syslog message IP header type.

## Syntax

- **syslog ip-header-type circuitless-ip**
- **syslog ip-header-type default**

## Command Parameters

**circuitless-ip**

Set the ip address in syslog header to circuitless-ip

**default**

Set the ip address in syslog header to default

## Default

The default is default.

## Command Mode

Global Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## syslog max-hosts <1-10>

---

Specify the maximum number of syslog hosts supported.

### Syntax

- **default syslog max-hosts**
- **syslog max-hosts <1-10>**

### Default

The default is 5.

### Command Mode

Global Configuration

## syslog tls-min-ver

---

Configure the minimum version of TLS protocol supported by the syslog client.

### Syntax

- **syslog tls-min-ver {tlsv11 | tlsv12}**
- **default syslog tls-min-ver**

### Command Parameters

tlsver11 | tlsver12

Specifies the minimum version of the TLS protocol supported by the syslog client.

- tlsver11 - configures version 1.1
- tlsver12 - configures version 1.2

### Default

None

### Command Mode

Global Configuration Mode



## Usage Guidelines

This command is not supported on VSP 8600 Series.

## syslog root-cert

---

Configure the root certificate for a syslog client.

### Syntax

- **no syslog root-cert install-filename <file-name>**
- **syslog root-cert install-filename <file-name>**

### Command Parameters

**install-filename <file-name>**

Specifies the name of the root certificate to be installed on the store.

### Default

None

### Command Mode

Global Configuration

## tacacs accounting

---

Determines for which applications TACACS+ collects accounting information. Use TACACS+ accounting to track the services that users access and the amount of network resources that users consume.

### Syntax

- **default tacacs accounting cli**
- **no tacacs accounting cli**
- **tacacs accounting disable**
- **tacacs accounting disable cli**
- **tacacs accounting enable cli**

### Command Parameters

**cli**

Specifies the command line as the application.

**disable**

Disables the accounting function for the specified application.

**enable**

Enables the accounting function for the specified application.

**Default**

None. If unassigned, TACACS+ does not perform the accounting function.

**Command Mode**

Global Configuration

---

**tacacs authentication**

---

Determines which applications TACACS+ authenticates.

**Syntax**

- **default tacacs authentication all**
- **default tacacs authentication cli**
- **default tacacs authentication web**
- **no tacacs authentication all**
- **no tacacs authentication cli**
- **no tacacs authentication web**
- **tacacs authentication all**
- **tacacs authentication cli**
- **tacacs authentication web**

**Command Parameters****all**

TACACS+ authenticates all applications.

**cli**

TACACS+ authenticates command line connections.

**web**

TACACS+ authenticates web connections.

**Default**

The default value is cli.

**Command Mode**

Global Configuration

---

## tacacs authorization

---

Enables command authorization for a particular privilege level. Use this option to limit the use of certain commands to different users. To use TACACS+ authorization, you must also use TACACS+ authentication.

### Syntax

- **default tacacs authorization**
- **no tacacs authorization enable**
- **no tacacs authorization level <1-6>**
- **tacacs authorization disable**
- **tacacs authorization enable**
- **tacacs authorization level <1-6>**
- **tacacs authorization level all**
- **tacacs authorization level none**

### Command Parameters

**disable**

Disables command authorization.

**enable**

Enables command authorization.

**level <1-6>**

Enables command authorization for a specific privilege level.

**level all**

Enables command authorization for all privilege levels.

**level none**

Disables command authorization for all privilege levels.

### Default

The default is disabled.

### Command Mode

Global Configuration

---

## tacacs protocol enable

---

Globally enables or disables TACACS+.

## Syntax

- `default tacacs protocol enable`
- `no tacacs protocol enable`
- `tacacs protocol enable`

## Default

The default is disabled.

## Command Mode

Global Configuration

---

## tacacs server host

---

Configures the entry for the primary TACACS+ server.

## Syntax

- `default tacacs server {A.B.C.D}`
- `default tacacs server {A.B.C.D} port`
- `default tacacs server {A.B.C.D} single-connection`
- `default tacacs server {A.B.C.D} single-connection source source-ip-interface enable`
- `default tacacs server {A.B.C.D} source source-ip-interface enable`
- `default tacacs server {A.B.C.D} timeout`
- `default tacacs server host {A.B.C.D} source {A.B.C.D}`
- `no tacacs server {A.B.C.D}`
- `no tacacs server {A.B.C.D} single-connection`
- `no tacacs server {A.B.C.D} source source-ip-interface enable`
- `tacacs server host {A.B.C.D}`
- `tacacs server host {A.B.C.D} key WORD<0-128>`
- `tacacs server host {A.B.C.D} port <1-65535>`
- `tacacs server host {A.B.C.D} port <1-65535> source {A.B.C.D} source-ip-interface enable`
- `tacacs server host {A.B.C.D} single-connection`
- `tacacs server host {A.B.C.D} source {A.B.C.D}`
- `tacacs server host {A.B.C.D} source {A.B.C.D} source-ip-interface enable`
- `tacacs server host {A.B.C.D} timeout <10-30>`

## Command Parameters

**{A.B.C.D}**

Specifies the IP address of the primary TACACS+ server.

**Key WORD<0-128>**

Configures the secret key to share with this TACACS+ server. If the key length is zero, that indicates no encryption is used.

**port <1-65535>**

Configures the TCP port on which the client establishes a connection to the server. A value of 0 indicates that the system specified default value is used. The default is 49.

**single-connection**

Specifies if the TCP connection between the device and the TACACS+ server is a single connection. If you do not enable the single-connection parameter, the system uses the default connection type that opens and closes a connection for each communication session.

**Source {A.B.C.D}**

Configures the IP address of the interface to use with this server. If you do not configure an address, the system uses 0.0.0.0 as the default.



**Note**

Available only on VSP 8600 Series.

**source-ip-interface enable**

Enables the source address. You must enable this parameter if you configure a valid source IP address. The default is disabled.



**Note**

Available only on VSP 8600 Series.

**timeout <10-30>**

Configures the maximum time, in seconds, to wait for this TACACS+ server to reply. The default is 10 seconds.

## Default

None

## Command Mode

Global Configuration

## tacacs server secondary-host

---

Configures the entry for the secondary TACACS+ server.

## Syntax

- `default tacacs server {A.B.C.D}`
- `default tacacs server {A.B.C.D} port`
- `default tacacs server {A.B.C.D} single-connection`
- `default tacacs server {A.B.C.D} single-connection source source-ip-interface enable`
- `default tacacs server {A.B.C.D} source source-ip-interface enable`
- `default tacacs server {A.B.C.D} timeout`
- `no tacacs server {A.B.C.D}`
- `no tacacs server {A.B.C.D} single-connection`
- `no tacacs server {A.B.C.D} source source-ip-interface enable`
- `tacacs server secondary-host {A.B.C.D}`
- `tacacs server secondary-host {A.B.C.D} key WORD<0-128>`
- `tacacs server secondary-host {A.B.C.D} port <1-65535>`
- `tacacs server secondary-host {A.B.C.D} single-connection`
- `tacacs server secondary-host {A.B.C.D} source {A.B.C.D} source-ip-interface enable`
- `tacacs server secondary-host {A.B.C.D} timeout <10-30>`

## Command Parameters

**{A.B.C.D}**

Specifies the IP address of the secondary TACACS+ server.

**Key WORD<0-128>**

Configures the secret key to share with this TACACS+ server. If the key length is zero, that indicates no encryption is used.

**port <1-65535>**

Configures the TCP port on which the client establishes a connection to the server. A value of 0 indicates that the system specified default value is used. The default is 49.

**single-connection**

Specifies if the TCP connection between the device and the TACACS+ server is a single connection. If you do not enable the single-connection parameter, the system uses the default connection type that opens and closes a connection for each communication session.

**Source {A.B.C.D}**

Configures the IP address of the interface to use with this server. If you do not configure an address, the system uses 0.0.0.0 as the default.



### Note

Available only on VSP 8600 Series.

**Source-ip-interface enable**

Enables the source address. You must enable this parameter if you configure a valid source IP address. The default is disabled.

**Note**

Available only on VSP 8600 Series.

**Timeout <10-30>**

Configures the maximum time, in seconds, to wait for this TACACS+ server to reply. The default is 10 seconds.

## Default

None

## Command Mode

Global Configuration

---

## telnet-access sessions

Configures the number of supported inbound Telnet sessions.

## Syntax

- **default telnet-access sessions**
- **telnet-access sessions <0-8>**

## Command Parameters

<0-8>

Configures the allowable number of inbound Telnet sessions.

## Default

The default is 8.

## Command Mode

Global Configuration

---

## udp checksum

Enable the User Datagram Protocol (UDP) checksum calculation on the switch.

## Syntax

- **default udp checksum**

- `no udp checksum`
- `udp checksum`

## Default

The default is enabled.

## Command Mode

Global Configuration

---

## username

---

Change user profile.

## Syntax

- `default username WORD<1-20> level 11`
- `default username WORD<1-20> level 12`
- `default username WORD<1-20> level 13`
- `default username WORD<1-20> level ro`
- `default username WORD<1-20> level rw`
- `default username WORD<1-20> level rwa`
- `no username WORD<1-20> enable`
- `username add WORD<1-20> level ro enable`
- `username add WORD<1-20> level rw enable`
- `username add WORD<1-20> level rwa enable`
- `username WORD<1-20> level 11`
- `username WORD<1-20> level 12`
- `username WORD<1-20> level 13`
- `username WORD<1-20> level ro`
- `username WORD<1-20> level rw`
- `username WORD<1-20> level rwa`

## Command Parameters

<WORD>

Username.

add



Create a user.

**Note**

This parameter is available only for demonstration purposes on the VSP 8600 Series.

**level**

The level assigned to the new user.

**ro**

Read-only user name reset to default.

**rw**

Read-write user name reset to default.

**rwa**

Change read write all enable password.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

## virtual-ist

---

Virtual interswitch trunk (VIST) improves upon the Layer 2 and Layer 3 resiliency by using a virtualized IST channel through the SPBM cloud.

## Syntax

- **default virtual-ist peer-ip**
- **no virtual-ist peer-ip**
- **virtual-ist peer-ip {A.B.C.D} vlan <1-4059>**

## Command Parameters

**peer-ip {A.B.C.D}**

Specifies the peer IP address—the IP address of the IST VLAN on the other aggregation switch.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Global Configuration

## virtual-service (globally)

---

Configures virtual service on the switch.

## Syntax

- **default virtual-service** WORD<1-128> mem-size
- **default virtual-service** WORD<1-128> num-cores
- **no virtual-service** WORD<1-128> disk WORD<1-32>
- **no virtual-service** WORD<1-128> enable
- **no virtual-service** WORD<1-128> vport WORD<1-32> connect-type
- **no virtual-service** WORD<1-128> vport WORD<1-32> vlan <1-4096>
- **virtual-service** WORD<1-128> disk WORD<1-32> size <1-30>
- **virtual-service** WORD<1-128> enable
- **virtual-service** WORD<1-128> mem-size <1-50000>
- **virtual-service** WORD<1-128> num-cores <1-6>
- **virtual-service** WORD<1-128> vport WORD<1-32>
- **virtual-service** WORD<1-128> vport WORD<1-32> connect-type {ovs | sriov | vtd}
- **virtual-service** WORD<1-128> vport WORD<1-32> port WORD<1-32>
- **virtual-service** WORD<1-128> vport WORD<1-32> port WORD<1-32> nic-type [virtio | e1000]
- **default virtual-service** WORD<1-128> vport WORD<1-32> port WORD<1-32> nic-type
- **virtual-service** WORD<1-128> vport WORD<1-32> vlan <1-4096>

## Command Parameters

### **connect-type {ovs | sriov | vtd}**

Specifies the connection type for the virtual port created. The default is VT-d. The switch supports the following maximums for virtual ports:

- Open vSwitch (OVS) - 16
- Single Root Input/Output Virtualization (SR-IOV) - 16
- Virtualization Technology for Directed Input/Output (VT-d) - 2

### **disk WORD<1-32>**

Specifies the disk assigned to the virtual service.

### **enable**

Enables the virtual service.

### **mem-size <1-50000>**

Specifies the memory size in Megabytes assigned to the virtual service. The default value is 1024 Megabytes.

### **nic-type [virtio | e1000]**

Specifies the Virtual Port NIC type. The default is e1000.



#### Note

Configure this value only when the **connect-type** parameter is **ovs**.

### **num-cores <1-6>**

Specifies the number of cores assigned to the virtual service. The default value is 1.

### **port<1-32>**

Specifies the name of the IAH port associated with the virtual port. Depending on hardware, the switch can support the following IAH ports:

- 1/s1
- 1/s2

### **size <1-30>**

Specifies the size of the disk in Gigabytes.

### **vlan <1-4096>**

Specifies the VLAN ID used by the virtual port.

### **vport WORD<1-32>**

Specifies the name of the virtual port.

### **WORD<1-128>**

Specifies the virtual service name.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## virtual-service WORD<1-128> change-user-pass WORD<1-20>

Changes the password for a VM user.

## Syntax

- **virtual-service WORD<1-128> change-user-pass WORD<1-20>**

## Command Parameters

WORD<1-20>

Specifies the username.

WORD<1-128>

Specifies the virtual service name.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

The password must be greater than, or equal to, 8 characters.

---

## virtual-service WORD<1-128> exec-command WORD<1-256>

Runs the **ls** command for the VM `config` directory from the VOSS CLI.

## Syntax

- **virtual-service WORD<1-128> exec-command WORD<1-256>**

## Command Parameters

*WORD<1-256>*

Specifies the VM command to run. To include spaces in the syntax, include the text string in quotation marks (").

*WORD<1-128>*

Specifies the virtual service name.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## virtual-service WORD<1-128> figw-cli WORD<1-256>

---

Runs a Fabric IPsec Gateway command from the VOSS CLI.

## Syntax

- **virtual-service WORD<1-128> figw-cli WORD<1-256>**

## Command Parameters

*WORD<1-256>*

Specifies the VM command to run. To include spaces in the syntax, include the text string in quotation marks (").

*WORD<1-128>*

Specifies the virtual service name.

## Default

None.

## Command Mode

Global Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## vlacp enable

---

Enable or disable the Virtual Link Aggregation Control Protocol (VLACP) globally to reset all port level settings on the chassis.

### Syntax

- **default vlapc enable**
- **default vlapc enable**
- **no vlapc enable**
- **vlacp enable**

### Command Parameters

**enable**

Enables the VLACP globally.

### Default

None

### Command Mode

Global Configuration

## vlan action

---

Perform a general VLAN action to initiate a specific function on a VLAN, such as clearing learned MAC addresses or ARP entries from the forwarding database.

### Syntax

- **vlan action <1-4059> { none | flushMacFdb | flushArp | flushIp | flushDynMemb | triggerRipUpdate | all }**

### Command Parameters

**all**

Sets action to all.

**flushArp**

Flush ARP tables for a VLAN.

**flushDynMemb**

Flush dynamic port members from the active port-members list on a policy-based VLAN. This command also removes the MAC addresses learned on those ports for the VLAN.

**fluship**

Flush IP Routing tables.

**flushMacFdb**

Flush the MAC FDB.

**none**

Sets action to none.

**triggerRipUpdate**

Sets action to triggerRipUpdate.

## Default

None

## Command Mode

Global Configuration

## vlan agetime

---

Configure the agetime for dynamic VLAN membership.

## Syntax

- **default vlan agetime <2-4059>**
- **vlan agetime <2-4059> <0-1000000>**

## Command Parameters

<0-1000000>

Specifies the agetime, in seconds.

<2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

## Default

The default is 600 seconds.

## Command Mode

Global Configuration

## vlan create

Create a VLAN by port, protocol, or SPBM. Optionally, you can choose to assign the VLAN a name and color. VLANs 4060-4094 are used internally. Create a VLAN with a value between 2 and 4059.

### Syntax

- `vlan create <2-4059> name WORD<0-64> type port-mstprstp <0-63>`
- `vlan create <2-4059> name WORD<0-64> type port-mstprstp <0-63> color <0-32>`
- `vlan create <2-4059> name WORD<0-64> type protocol-mstprstp <0-63> ipv6`
- `vlan create <2-4059> name WORD<0-64> type protocol-mstprstp <0-63> ipv6 color <0-32>`
- `vlan create <2-4059> name WORD<0-64> type spbm-bvlan`
- `vlan create <2-4059> name WORD<0-64> type spbm-bvlan color <0-32>`
- `vlan create <2-4059> type port-mstprstp <0-63>`
- `vlan create <2-4059> type port-mstprstp <0-63> color <0-32>`
- `vlan create <2-4059> type protocol-mstprstp <0-63> ipv6`
- `vlan create <2-4059> type protocol-mstprstp <0-63> ipv6 color <0-32>`
- `vlan create <2-4059> type spbm-bvlan`
- `vlan create <2-4059> type spbm-bvlan color <0-32>`
- `vlan create <2-4059> name WORD<0-64> type pvlan-mstprstp <0-63> secondary <2-4059>`
- `vlan create <2-4059> name WORD<0-64> type pvlan-mstprstp <0-63> secondary <2-4059> color <0-32>`
- `vlan create <2-4059> type pvlan-mstprstp <0-63> secondary <2-4059> color <0-32>`

### Command Parameters

`<2-4059>`

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

`color <0-32>`

Specifies the color of the VLAN.

`name WORD<0-64>`



Specifies the VLAN name in the range of 0-64. This parameter is optional.



#### Note

Do not use the name Mgmt when you specify a name for the VLAN that you create. The switch creates a management VLAN at boot up with the assigned name Mgmt.

The show command does not show the management VLAN.

#### **port-mstprstp <0-63>**

Specifies the VLAN type as created by port. <0-63> specifies the instance ID.

#### **protocol-mstprstp <0-63>**

Specifies the VLAN type as created by protocol. <0-63> specifies the instance ID.

#### **pvlan-mstprstp <0-63>**

Specifies the VLAN type as private for use in Etree deployments. <0-63> specifies the instance ID.

#### **spbm-bvlan**

Specifies the VLAN type as the backbone VLAN (B-VLAN) for Shortest Path Bridging MAC (SPBM).

#### **type ipsubnet-mstprstp <0-63> <A.B.C.D/X> [color <0-32]**

Creates a VLAN by IP subnet:

- <0-63> is the STP instance ID in the range of 0-63
- A.B.C.D/X is the subnet address or mask {a.b.c.d/x | a.b.c.d/x.x.x.x}
- color <0-32> is the color of the VLAN in the range of 0 to 32

#### **type port-mstprstp <0-63> [color <0-32>]**

Creates a VLAN by port: 0-63 is the STP instance ID from 0 to 63. color <0-32> is the color of the VLAN in the range of 0 to 32.

#### **type protocol-mstprstp <0-63> {appleTalk | declat | decOther | ip | ipv6 | ipx802dot2 | ipx802dot3 | ipxEthernet2 | ipxsnap | netBios | PPPoE | rarp | sna802dot2 | snaEthernet2 | vines | xns} [color <0-32>]**

Creates a VLAN by protocol:

- 0-63 is the STP instance ID
- appleTalk is the apple talk protocol
- declat is the declat protocol
- decOther is the decother protocol
- ip is the Ip version 4 protocol
- ipx802dot2 specifies the Novell Internetwork Packet Exchange (IPX) on IEEE 802.2 frames
- ipx802dot3 specifies the Novell Internetwork Packet Exchange (IPX) on Ethernet 802.3 frames
- ipxEthernet2 specifies the Novell IPX on Ethernet type 2 frames
- ipxsnap specifies the Novell IPX on Ethernet Standard Network Access Protocol (SNAP) frames
- netbios is the Netbios protocol

- PPPoE is the Point-to-Point Protocol Over Ethernet
- rarp is the Rarp protocol
- sna802dot2 is the Sna802dot2 protocol
- snaethernet2 is the Snaethernet2 protocol
- vines is the Vines protocol
- xns is the Xns protocol
- color <0-32> is the color of the VLAN in the range of 0 to 32

**type protocol-mstprstp <0-63> userDefined {0x0000 | <decimal value>} [color ] <0-32>] [encap {ethernet-ii | llc | snap}]**

Creates a VLAN using a user defined protocol.

- <0-63> is the STP instance ID in the range of 0-63
- {0x0000|<decimal value>} is the protocol ID in hexadecimal or decimal value
- color <0-32> is the color of the VLAN in the range of 0 to 32
- encap specifies the frame encapsulation header type

**type pvlan-mstprstp <0-63> secondary <2-4059> color <0-32>**

Creates a Private VLAN by port for a secondary VLAN ID. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998.

**type srcmac-mstprstp <0-63> [color<0-32> ]**

Creates a VLAN by source MAC address: 0-63 is the STP instance ID in the range of 0-63. color <0-32> is the color of the VLAN in the range of 0 to 32.

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

You cannot configure a VLAN name that uses all numbers, for example, 222.

## vlan delete

---

Delete a VLAN.

## Syntax

- **no vlan <2-4059>**
- **vlan delete <2-4059>**

## Command Parameters

<2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

## Default

None

## Command Mode

Global Configuration

## vlan i-sid

---

Map a customer VLAN (C-VLAN) to a service instance identifier (I-SID) to create a Layer 2 VSN. The C-VLAN cannot be a backbone VLAN (B-VLAN).

You can specify an I-SID name before or after you associate I-SID to VLAN. By default, the I-SID name is the word "ISID-" followed by its numeric value.

## Syntax

- **default vlan i-sid <1-4059>**
- **no vlan i-sid <1-4059>**
- **vlan i-sid <1-4059> <0-16777215> [force]**

## Command Parameters

<0-16777215>

Specifies the I-SID. You cannot use I-SID 0x00ffffff. The system reserves this I-SID to advertise the virtual BMAC in an SMLT dual-homing environment.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### force

Specifies the software must replace the existing VLAN-to-I-SID mapping, if one exists.

## Default

The default I-SID is 0.

## Command Mode

Global Configuration

## vlan mac-address-entry

---

Modify or flush the entries in the forwarding database (FDB).

## Syntax

- **vlan mac-address-entry <1-4059> flush**
- **vlan mac-address-entry <1-4059> sync**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### flush

Flushes the FDB.

### sync

Synchronizes the switch forwarding database with the forwarding database of the other aggregation switch.

## Default

None

## Command Mode

Global Configuration

## vlan mac-address-static

---

Configure the static members of a VLAN to set the VLAN static member parameters.

## Syntax

- **no vlan mac-address-static <1-4059> <0x00:0x00:0x00:0x00:0x00:0x00>**

- **vlan mac-address-static** <1-4059> <0x00:0x00:0x00:0x00:0x00:0x00> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<0x00:0x00:0x00:0x00:0x00:0x00>

Adds a static member to a VLAN bridge:

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Global Configuration

## vlan members

---

Add ports to a VLAN.

## Syntax

- **vlan members** <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **vlan members** <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} { portmember | static | notallowed }
- **vlan members add** <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **vlan members add** <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} { portmember | static | notallowed }

- **vlan members remove** <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}
- **vlan members remove** <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} { portmember | static | notallowed }

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**notallowed**

Selects the port type to not-allowed.

**portmember**

Select the port type to port member.

**static**

Selects the port type to static.

## Default

None

## Command Mode

Global Configuration

## vlan mlt

Add an MLT to a VLAN.

## Syntax

- **vlan mlt** <1-4059> <1-512>

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

<1-512>

Specifies the MLT ID.

## Default

None

## Command Mode

Global Configuration

## vlan name

---

Change the name of a VLAN.

## Syntax

- **vlan name <2-4059> WORD<0-64>**

## Command Parameters

<2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

<LINE>

New name for VLAN

## Default

None

## Command Mode

Global Configuration

## Usage Guidelines

You cannot configure a VLAN name that uses all numbers, for example, 222.

## vlan nodal-mep

---

Add nodal Maintenance Endpoints (MEPs) to the VLAN. The Nodal B-VLAN MEPs created on the CP and function as if they are connected to the virtual interface of the given B-VLAN. Because of this, they are supported for both port and MLT based B-VLANs. To support this behavior, a MAC entry is added to the forwarding database (FDB) and a new CFM data path table containing the B-VLAN and MP level are added to direct CFM frames to the CP as required.

### Syntax

- **no vlan nodal-mep <1-4059> WORD<0-22> WORD<0-22> <1-8191>**
- **vlan nodal-mep <1-4059> WORD<0-22> WORD<0-22> <1-8191>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

<1-8191>

Specifies the nodal Maintenance Endpoints (MEPs) to add to the VLAN.

WORD<0-22> WORD<0-22>

The first parameter, specifies the Maintenance-Domain (MD) name. The second parameter, specifies the Maintenance-Association (MA) name.

### Default

None

### Command Mode

Global Configuration

## vlan nodal-mip-level

---

Add a nodal Maintenance Intermediate Point level to the VLAN. The Nodal MIP is associated with a B-VLAN. VLAN and level are sufficient to specify the Nodal MIP entity. The Nodal MIP MAC address is the SPBM system ID for the node on which it resides. If the fastpath sends a message to the CP, the MIP responds if it is not the target and the MEP responds if it is the target.

### Syntax

- **no vlan nodal-mip-level <1-4059> WORD<0-15>**
- **vlan nodal-mip-level <1-4059> WORD<0-15>**



## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

WORD<0-15>

Adds the nodal Maintenance Intermediate Point (MIP) level.

## Default

None

## Command Mode

Global Configuration

## vlan ports

---

Modify VLAN port settings.

## Syntax

- **vlan ports {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} tagging tagAll**
- **vlan ports {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} tagging untagAll**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<LINE>

Port list

**disable**

Disable tagging on this port

**enable**

Enable tagging on this port

**filter-unregistered-frames {disable | enable}**

Enable/disable filtering of unregistered frames

**filter-untagged-frame {disable | enable}**

Enable/disable filtering of untagged frames

**name <LINE>**

Set VLAN port name

**priority <0-7>**

Set VLAN port priority

**pvid <1-4094>**

Change PVID

**tagAll**

Enable tagging on this port

**tagging {disable | enable | tagAll | tagPvidOnly | untagAll | untagPvidOnly}**

Enable/disable tagging

**tagPvidOnly**

Enable tagging of packets matching the

**untagAll**

Disable tagging on this port

**untagPvidOnly**

Disable tagging of packets matching the Pv

## Default

None

## Command Mode

Global Configuration

## vlan rmon

---

Enable RMON on this VLAN.

## Syntax

- **default vlan rmon <1-4059>**
- **no vlan rmon <1-4059>**
- **vlan rmon <1-4059>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

The default is disabled.

## Command Mode

Global Configuration

## vlan srcmac

---

Add MAC address for a VLAN.

## Syntax

- **default vlan srcmac <2-4059> 0x00:0x00:0x00:0x00:0x00:0x00**
- **no vlan srcmac <2-4059> 0x00:0x00:0x00:0x00:0x00:0x00**
- **vlan srcmac <2-4059> 0x00:0x00:0x00:0x00:0x00:0x00**

## Command Parameters

<0x00:0x00:0x00:0x00:0x00:0x00>

Specifies the source MAC address.

<0-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

## Default

None

## Command Mode

Global Configuration

## vlan static-mcastmac

---

Add VLAN static multicast MAC entries.

## Syntax

- `default vlan static-mcastmac <1-4059> [0x00:0x00:0x00:0x00:0x00:0x00] [mlt WORD<1-256>]`
- `default vlan static-mcastmac <1-4059> [0x00:0x00:0x00:0x00:0x00:0x00] [mlt WORD<1-256>]`
- `default vlan static-mcastmac <1-4059> ports{slot/port[/sub-port] [-slot/port[/sub-port]][,...]} [0x00:0x00:0x00:0x00:0x00:0x00]`
- `no vlan static-mcastmac <1-4059> 0x00:0x00:0x00:0x00:0x00:0x00`
- `no vlan static-mcastmac <1-4059> ports {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} [0x00:0x00:0x00:0x00:0x00:0x00]`
- `vlan static-mcastmac <1-4059> ports {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} [0x00:0x00:0x00:0x00:0x00:0x00]`
- `vlan static-mcastmac <1-4059>[0x00:0x00:0x00:0x00:0x00:0x00] [{slot/port[/sub-port] [-slot/port[/sub-port]][,...]]} [mlt WORD<1-256>]`

## Command Parameters

`{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**<1-256>**

Specifies the MLT ID.

**<1-4059>**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC address.

## Default

None

## Command Mode

Global Configuration

## vnid

Create a VNID instance.

## Syntax

- **no vnid <1-16777215> i-sid <1-16777215>**
- **vnid <1-16777215> i-sid <1-16777215>**

## Command Parameters

<1-16777215> i-sid <1-16777215>

Uses this VNID and I-SID information to create a VNID instance and enter VXLAN Configuration Mode. A VNID must not have the same value as an I-SID.



### Note

The command prompt changes to #vxlan to indicate that you are now in VXLAN Configuration mode for the VNID specified in vnid <1-16777215>.

## Default

None

## Command Mode

Global Configuration

---

## vnid mac-address-entry

Flush all the learned MAC addresses from the forwarding database of the selected VNID.

## Syntax

- **vnid mac-address-entry <1-16777215> flush**

## Command Parameters

<1-16777215> flush

Flush all the learned MAC addresses from the forwarding database of the selected VNID.

## Default

None

## Command Mode

Global Configuration

## vtep (configuration)

---

Configure the remote VTEP IP address.



### Note

The remote VTEP IP address cannot be a local, broadcast, or multicast IP address.

### Syntax

- **no vtep <1-500> ip <A.B.C.D> [name WORD<1-64>]**
- **vtep <1-500> ip <A.B.C.D> [name WORD<1-64>]**

### Command Parameters

<1-500> ip <A.B.C.D> [name WORD<1-64>]

Specifies an index value and an IP address that uniquely identifies this remote VTEP. Optionally, you can assign a specific name to this tunnel. By default, the switch assigns a name in this format: VTEP-<#ID>-<IP address>

### Default

None

### Command Mode

Global Configuration

## vtep source-ip

---

Configure the VTEP source IP address.

### Syntax

- **no vtep source-ip <A.B.C.D> [vrf WORD<1-16>]**
- **vtep source-ip <A.B.C.D> [vrf WORD<1-16>]**

### Command Parameters

<A.B.C.D> [vrf WORD<1-16>]

Specifies the VXLAN tunnel end point (VTEP) source IP address, which can be on the GRT or a VRF.

### Default

None

## Command Mode

Global Configuration

### web-server certificate

---

Configure the installed digital certificate to be used.

#### Syntax

- **web-server certificate {ca-name | cert-subject-name}**
- **no web-server certificate**
- **default web-server certificate**

#### Command Parameters

**ca-name WORD <1-45>**

Specifies the name of the Certificate Authority.

**cert-subject-name WORD <1-45>**

Specifies the subject identity label to be used. Certificates for this subject are already installed.

#### Default

None

## Command Mode

Global Configuration

### web-server def-display-rows

---

Configures the web server default display row width.

#### Syntax

- **web-server def-display-rows <10-100>**
- **default web-server def-display-rows**

#### Command Parameters

**<10-100>**

Specifies the default display row width.

#### Default

The default is 30.

## Command Mode

Global Configuration

### web-server enable

---

Enable the web management interface to provide management access to the switch using a web browser. You must enable the web interface before you can connect to the system using Enterprise Device Manager (EDM).

#### Syntax

- **web-server enable**
- **no web-server enable**
- **default web-server enable**

#### Default

The default is disabled.

## Command Mode

Global Configuration

### web-server help-tftp

---

Specifies the path to the TFTP server that stores the HTML Help files for the web server.

#### Syntax

- **web-server help-tftp WORD<0-256>**

#### Command Parameters

**WORD<0-256>**

Specifies the file name in the following format: a.b.c.d;/.

#### Default

None

## Command Mode

Global Configuration



---

## web-server http-port

---

Configures the web server HTTP port.

### Syntax

- **web-server http-port <80-49151>**
- **default web-server http-port**

### Command Parameters

<80-49151>

Specifies the web server HTTP port.

### Default

The default is 80.

### Command Mode

Global Configuration

### Usage Guidelines

To select another port for HTTP, you can discover the ports that TCP already use. Use the **show ip tcp connections** command to list the ports already in use, and then select a port that does not display in the command output.

---

## web-server inactivity-timeout

---

Configures the web-server login session inactivity timeout.

### Syntax

- **web-server inactivity-timeout <30-65535>**
- **default web-server inactivity-timeout**

### Command Parameters

<30-65535>

Specifies the inactivity timeout.

### Default

The default is 900 seconds (15 minutes).

## Command Mode

Global Configuration

### web-server password

---

Configures the web server password.

#### Syntax

- **web-server password min-password-len <1-32>**
- **web-server password ro WORD<1-20>**
- **web-server password rwa WORD<1-20>**
- **default web-server min-passwd-len**

#### Command Parameters

**min-password-len <1-32>**

Configures the minimum password length. By default, the minimum password length is 8 characters.

**ro WORD<1-20>**

Specifies the username and the password for the access level read-only.

**rwa WORD<1-20>**

Specifies the username and the password for the access level read-write-all.

#### Default

None

## Command Mode

Global Configuration Mode

### web-server read-only-user enable

---

Enables the web server read-only (RO) user.

#### Syntax

- **web-server read-only-user**
- **no web-server read-only-user**

#### Default

The default is enabled. After a software upgrade, the default is disabled.

## Command Mode

Global Configuration

## Usage Guidelines

**read-only-user enable** is available for demonstration purposes on some products. For more information, see [VOSS User Guide](#).

## web-server secure-only

---

Enables secure-only access to the web server.

## Syntax

- **web-server secure-only**
- **no web-server secure-only**
- **default web-server secure-only**

## Default

The default is enabled.

## Command Mode

Global Configuration

## Usage Guidelines

By default, the web server is configured with the secure-only option, which requires you to use https to access EDM. To access EDM using http, you must disable the secure-only option by using the **no web-server secure-only** command.

## web-server tls-min-ver

---

Configures the minimum version of the TLS protocol supported by the web-server.

## Syntax

- 
- **web-server tls-min-ver {tlsv10 | tlsv11 | tlsv12}**
- **default tls-min-ver**

## Command Parameters

<tlsv10|tlsv11|tlsv12>

Specifies the minimum version of the TLS protocol supported by the web-server.

## Default

The default is tlsv12.

## Command Mode

Global Configuration



# IS-IS Router Configuration

---

The following topics document commands available in IS-IS Router Configuration mode of the command line interface (CLI).

## accept (for the GRT)

---

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all routes from all Backbone Edge Bridges (BEBs) for the Global Routing Table (GRT).

### Syntax

- **accept backbone-route-map WORD<1-64>**
- **accept i-sid <1-16777215>**
- **accept i-sid <1-16777215> backbone-route-map WORD<1-64>**
- **accept i-sid <1-16777215> enable**
- **accept i-sid <1-16777215> route-map WORD<1-64>**
- **accept isid-list WORD<1-32>**
- **accept isid-list WORD<1-32> backbone-route-map WORD<1-64>**
- **accept isid-list WORD<1-32> enable**
- **accept isid-list WORD<1-32> route-map WORD<1-64>**
- **accept route-map WORD<1-64>**
- **accept route-map WORD<1-64> backbone-route-map WORD <1-64>**
- **no accept backbone-route-map**
- **no accept i-sid <1-16777215>**
- **no accept i-sid <1-16777215> backbone-route-map**
- **no accept i-sid <1-16777215> enable**
- **no accept i-sid <1-16777215> route-map**
- **no accept isid-list WORD<1-32>**
- **no accept isid-list WORD<1-32> backbone-route-map**
- **no accept isid-list WORD<1-32> enable**
- **no accept isid-list WORD<1-32> route-map**
- **no accept route-map**

## Command Parameters

**backbone-route-map WORD<1-64>**

Configures the backbone-route-map for DvR routes.

**enable**

Enables an IS-IS accept policy.

**i-sid <1-16777215>**

Specifies a service instance identifier (I-SID) number that represents a local or remote Layer 3 VSN for the IS-IS accept policy.

**isid-list WORD <1-32>**

Specifies a name for a list of I-SID numbers that represent local or remote Layer 3 VSN for the IS-IS accept policy.

**route-map WORD<1-64>**

Configures the IS-IS route policy by name.

## Default

None

## Command Mode

IS-IS Router Configuration

## accept adv-rtr (for the GRT)

Use an IS-IS accept policy instance to apply to a specific advertising advertising Backbone Edge Bridge (BEB) for the Global Routing Table (GRT).

## Syntax

- **accept adv-rtr <x.xx.xx>**
- **accept adv-rtr <x.xx.xx> backbone-route-map WORD<1-64>**
- **accept adv-rtr <x.xx.xx> enable**
- **accept adv-rtr <x.xx.xx> i-sid <1-16777215>**
- **accept adv-rtr <x.xx.xx> i-sid <1-16777215> backbone-route-map WORD<1-64>**
- **accept adv-rtr <x.xx.xx> i-sid <1-16777215> enable**
- **accept adv-rtr <x.xx.xx> i-sid <1-16777215> route-map WORD<1-64>**
- **accept adv-rtr <x.xx.xx> isid-list WORD<1-32>**
- **accept adv-rtr <x.xx.xx> isid-list WORD<1-32> backbone-route-map WORD<1-64>**
- **accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable**
- **accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map WORD<1-64>**

- **accept adv-rtr <x.xx.xx> route-map WORD<1-64>**
- **no accept adv-rtr <x.xx.xx>**
- **no accept adv-rtr <x.xx.xx> backbone-route-map**
- **no accept adv-rtr <x.xx.xx> enable**
- **no accept adv-rtr <x.xx.xx> i-sid <1-16777215>**
- **no accept adv-rtr <x.xx.xx> i-sid <1-16777215> backbone-route-map**
- **no accept adv-rtr <x.xx.xx> i-sid <1-16777215> enable**
- **no accept adv-rtr <x.xx.xx> i-sid <1-16777215> route-map**
- **no accept adv-rtr <x.xx.xx> isid-list WORD<1-32>**
- **no accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable**
- **no accept adv-rtr <x.xx.xx> route-map**

## Command Parameters

**<x.xx.xx>**

Specifies the Shortest Path Bridging MAC (SPBM) nickname at a level for each advertising BEB.

**adv-rtr <x.xx.xx>**

Specifies the Shortest Path Bridging MAC (SPBM) nickname for an advertising BEB for the IS-IS accept policy.

**backbone-route-map WORD<1-64>**

Configures the backbone-route-map for DVR routes.

**enable**

Enables an IS-IS accept policy.

**i-sid <0-16777215>**

Specifies a service instance identifier (I-SID) number that represents a local or remote Layer 3 VSN for the IS-IS accept policy.

**isid-list WORD <1-32>**

Specifies a name for a list of I-SID numbers that represent local or remote Layer 3 VSN for the IS-IS accept policy.

**route-map WORD<1-64>**

Configures the IS-IS route policy by name.

## Default

None

## Command Mode

IS-IS Router Configuration

---

## accept i-sid (for the GRT)

---

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to a specific Service Instance Identifier (I-SID) for the Global Routing Table (GRT).

### Syntax

- **accept i-sid <1-16777215>**
- **accept i-sid <1-16777215> backbone-route-map WORD<1-64>**
- **accept i-sid <1-16777215> enable**
- **accept i-sid <1-16777215> route-map WORD<1-64>**
- **no accept i-sid <1-16777215>**
- **no accept i-sid <1-16777215> backbone-route-map**
- **no accept i-sid <1-16777215> enable**
- **no accept i-sid <1-16777215> route-map**

### Command Parameters

**backbone-route-map WORD<1-64>**

Configures the backbone-route-map for DVR routes.

**enable**

Enables an IS-IS accept policy.

**i-sid <1-16777215>**

Specifies a service instance identifier (I-SID) number that represents a local or remote Layer 3 VSN for the IS-IS accept policy.

**route-map WORD<1-64>**

Configures the IS-IS route policy by name.

### Default

None

### Command Mode

IS-IS Router Configuration

---

## accept isid-list (for the GRT)

---

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to a specific list of Service Instance Identifiers (I-SIDs) for the Global Routing Table (GRT).



## Syntax

- **accept isid-list <1-16777215>**
- **accept isid-list <1-16777215> backbone-route-map WORD<1-64>**
- **accept isid-list <1-16777215> enable**
- **accept isid-list <1-16777215> route-map WORD<1-64>**
- **no accept isid-list <1-16777215>**
- **no accept isid-list <1-16777215> backbone-route-map**
- **no accept isid-list <1-16777215> enable**
- **no accept isid-list <1-16777215> route-map**

## Command Parameters

**backbone-route-map WORD<1-64>**

Configures the backbone-route-map for DvR routes.

**enable**

Enables an IS-IS accept policy.

**isid-list WORD <1-32>**

Specifies a name for a list of I-SID numbers that represent local or remote Layer 3 VSN for the IS-IS accept policy.

**route-map WORD<1-64>**

Configures the IS-IS route policy by name.

## Default

None

## Command Mode

IS-IS Router Configuration

## accept route-map

---

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply using a specific route-map for the Global Routing Table (GRT).

## Syntax

- **accept route-map WORD<1-64>**
- **no accept route-map**

## Command Parameters

**WORD<1-64>**

Configures the IS-IS route policy by name.

## Default

None

## Command Mode

IS-IS Router Configuration

---

## area-name (for IS-IS)

Configures the area name for the home area.

## Syntax

- **area-name WORD<0-255>**
- **no area-name**
- **default area-name**

## Command Parameters

**WORD<0-255>**

Specifies the area name.

## Default

The default value is area-manual-area, where manual-area represents the IS-IS manual-area value that you configure.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## area-vnode nick-name (for IS-IS)

Configures the IS-IS Multi-area SPB virtual node nick name.

## Syntax

- **area-vnode nick-name <x.xx.xx>**

- **default area-vnode nick-name**
- **no area-vnode nick-name**

## Command Parameters

<X.XX.XX>

Specifies the nickname for the Multi-area SPB virtual node. The value is 2.5 bytes.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## area-vnode sys-name (for IS-IS)

Configures the IS-IS Multi-area SPB virtual node system name.

## Syntax

- **area-vnode sys-name WORD<0-255>**
- **default area-vnode sys-name**
- **no area-vnode sys-name**

## Command Parameters

WORD<0-255>

Specifies the IS-IS Multi-area SPB virtual node system name.

## Default

None

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## area-vnode system-id (for IS-IS)

---

Configures the IS-IS Multi-area SPB virtual node system ID.

### Syntax

- **area-vnode system-id xxxx.xxxx.xxxx**
- **default area-vnode system-id**
- **no area-vnode system-id**

### Command Parameters

xxxx.xxxx.xxxx

Specifies the IS-IS Multi-area SPB virtual node system ID.

### Default

None

### Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## backbone

---

Configures a non-DvR BEB to join the DvR backbone so that it can receive redistributed DvR host routes from all DvR Controllers in the SPB network.

### Syntax

- **backbone enable**
- **no backbone enable**

### Command Parameters

enable

Configures a non- DvRBEB to join the DvR backbone.

## Default

none

## Command Mode

IS-IS Router Configuration

## csnp-interval

---

Configure the Complete Sequence Number Packets (CSNP) interval in seconds. This command is a system level parameter that applies to Level 1 CSNP generation on all interfaces.

## Syntax

- **csnp-interval <1-600>**
- **default csnp-interval**
- **no csnp-interval**

## Command Parameters

<1-600>

Configures the interval, in seconds.

## Default

The default CSNP interval is 10 seconds.

## Command Mode

IS-IS Router Configuration

## hello-padding

---

Pads hello packets to the full interface maximum transmission unit (MTU) to detect MTU mismatches.

## Syntax

- **hello-padding**
- **default hello-padding**
- **no hello-padding**

## Default

The default is enabled.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipsec encryption-key-length

---

Configure IPsec encryption key length for Fabric Extend tunnel.

### Syntax

- **ipsec encryption-key-length <128 | 256>**
- **default ipsec encryption-key-length**

### Command Parameters

<128 | 256>

Specifies the IPsec encryption key length, which is 128 bit or 256 bit.

### Default

The default IPsec encryption key length is 128 bit.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipsec tunnel-source-address

---

Configures the source IP address for IPsec tunnel.

### Syntax

- **ipsec tunnel-source-address {A.B.C.D}**
- **no ipsec tunnel-source-address**

## Command Parameters

{A.B.C.D}

Specifies the source IP address of IPsec tunnel.

## Default

None.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## ip-source-address

Configure the circuitless IP (CLIP) interface as the source address for SPBM IP Shortcuts. Assigns a source IP address for locally generated IP packets whose egress port is an SPBM NNI port.

The source-address value must be a locally configured loopback IP address. The IS-IS automatically advertises the source-address to other SPBM edge routers when you enable IP shortcuts. You must first configure a valid source-address before you enable IP shortcuts.

## Syntax

- **ip-source-address {A.B.C.D}**
- **no ip-source-address**

## Command Parameters

<A.B.C.D>

Specifies the circuitless IP (CLIP) interface as the source address for SPBM IP shortcuts.

## Default

None

## Command Mode

IS-IS Router Configuration

---

## ip-tunnel-source-address

---

Configure the IP tunnel source address.

### Syntax

- `ip-tunnel-source-address {A.B.C.D} [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] [vrf WORD<1-16>] [mtu <mtu_value>]`
- `ip-tunnel-source-address {A.B.C.D} port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} mtu <mtu_value>`
- `ip-tunnel-source-address {A.B.C.D} mtu <mtu_value>`
- `ip-tunnel-source-address {A.B.C.D} vrf WORD<1-16>`
- `no ip-tunnel-source-address`

### Command Parameters

**{A.B.C.D}**

Specifies the IS-IS IPv4 tunnel source address.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vrf WORD<1-16>**

Specifies the VRF name associated with the IP tunnel.

**mtu**

Specifies the Maximum Transmission Unit (MTU) size for each packet. Different hardware platforms support different MTU ranges. Use the CLI Help to see the available range for the switch.

### Default

None

### Command Mode

IS-IS Router Configuration

---

## ipv6 accept (IS-IS)

---

Configure an IPv6 Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all IPv6 routes from all Backbone Edge Bridges (BEBs).



## Syntax

- `ipv6 accept i-sid <1-16777215>`
- `ipv6 accept i-sid <1-16777215> enable`
- `ipv6 accept i-sid <1-16777215> route-map WORD<1-64>`
- `ipv6 accept isid-list WORD<1-32>`
- `ipv6 accept isid-list WORD<1-32> enable`
- `ipv6 accept isid-list WORD<1-32> route-map WORD<1-64>`
- `ipv6 accept route-map WORD<1-64>`
- `no ipv6 accept backbone-route-map`
- `no ipv6 accept i-sid <1-16777215>`
- `no ipv6 accept i-sid <1-16777215> enable`
- `no ipv6 accept i-sid <1-16777215> route-map`
- `no ipv6 accept isid-list WORD<1-32>`
- `no ipv6 accept isid-list WORD<1-32> enable`
- `no ipv6 accept isid-list WORD<1-32> route-map`
- `no ipv6 accept route-map`

## Command Parameters

**enable**

Enables an IPv6 IS-IS accept policy.

**i-sid <1-16777215>**

Specifies a service instance identifier (I-SID) number that represents a local or remote IPv6 Layer 3 VSN for the IPv6 IS-IS accept policy.

**isid-list WORD <1-32>**

Specifies a name for a list of I-SID numbers that represent local or remote IPv6 Layer 3 VSN for the IPv6 IS-IS accept policy.

**route-map WORD<1-64>**

Configures the IPv6 IS-IS route policy by name.

## Default

None

## Command Mode

IS-IS Router Configuration

## ipv6 accept adv-rtr (for IS-IS)

Use an IPv6 IS-IS accept policy instance to apply to a specific advertising Backbone Edge Bridge (BEB).

## Syntax

- `ipv6 accept adv-rtr <x.xx.xx>`
- `ipv6 accept adv-rtr <x.xx.xx> enable`
- `ipv6 accept adv-rtr <x.xx.xx> i-sid <1-16777215>`
- `ipv6 accept adv-rtr <x.xx.xx> i-sid <1-16777215> enable`
- `ipv6 accept adv-rtr <x.xx.xx> i-sid <1-16777215> route-map WORD<1-64>`
- `ipv6 accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `ipv6 accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `ipv6 accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map WORD<1-64>`
- `ipv6 accept adv-rtr <x.xx.xx> route-map WORD<1-64>`
- `no ipv6 accept adv-rtr <x.xx.xx>`
- `no ipv6 accept adv-rtr <x.xx.xx> enable`
- `no ipv6 accept adv-rtr <x.xx.xx> i-sid <1-16777215>`
- `no ipv6 accept adv-rtr <x.xx.xx> i-sid <1-16777215> enable`
- `no ipv6 accept adv-rtr <x.xx.xx> i-sid <1-16777215> route-map`
- `no ipv6 accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `no ipv6 accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `no ipv6 accept adv-rtr <x.xx.xx> route-map`

## Command Parameters

`<x.xx.xx>`

Specifies the Shortest Path Bridging MAC (SPBM) nickname at a level for each advertising BEB.

`enable`

Enables an IPv6 IS-IS accept policy for the specific advertising Backbone Edge Bridge (BEB).

`i-sid <0-16777215>`

Specifies a service instance identifier (I-SID) number that represents a local or remote IPv6 Layer 3 VSN for the IS-IS accept policy for the specific advertising Backbone Edge Bridge (BEB).

`isid-list WORD <1-32>`

Specifies a name for a list of I-SID numbers that represent local or remote IPv6 Layer 3 VSN for the IS-IS accept policy for the specific advertising Backbone Edge Bridge (BEB).

`route-map WORD<1-64>`

Configures the IS-IS route policy by name for the specific advertising Backbone Edge Bridge (BEB).

## Default

None

## Command Mode

IS-IS Router Configuration

## ipv6 redistribute (for GRT)

---

Ipv6 configurations.

### Syntax

- `default ipv6 redistribute {bgp | direct | ospf | rip |static} [enable]`
- `ipv6 redistribute bgp {enable | metric <0-65535> | metric-type [type1] [type2] | route-map WORD<1-64>}`
- `ipv6 redistribute direct {enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}`
- `ipv6 redistribute static {enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}`
- `no ipv6 redistribute {bgp | direct | ospf | rip |static} [enable]`

### Command Parameters

{bgp | direct | ospf | rip |static}

Specifies the type of IPv6 route to redistribute to the IS-IS routing domain.

{enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}

Enables redistribution.

### Default

None

## Command Mode

IS-IS Router Configuration

## ipv6 redistribute (for ISIS)

---

Enable redistribution to redistribute IPv6 routes into an ISIS routing domain.

### Syntax

- `default ipv6 redistribute {bgp | direct | ospf | rip |static} [enable]`
- `ipv6 redistribute direct {enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}`
- `ipv6 redistribute ospf {enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}`

- **ipv6 redistribute static {enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}**
- **no ipv6 redistribute {bgp | direct | ospf | rip |static} [enable]**

## Command Parameters

{bgp | direct | ospf | rip |static}

Specifies the type of IPv6 route to redistribute to the ISIS routing domain.

{enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}

Enables redistribution.

## Default

The default is disabled.

## Command Mode

IS-IS Router Configuration

## ipv6 redistribute bgp enable (For IS-IS)

---

Enable IPv6 BGP redistribute.

## Syntax

- **default ipv6 redistribute bgp enable**
- **ipv6 redistribute bgp enable**
- **no ipv6 redistribute bgp enable**

## Default

None

## Command Mode

IS-IS Router Configuration

## ipv6-source-address

---

Configure the circuitless IP (CLIP) interface as the source address for SPBM IPv6 Shortcuts. Assigns a source IPv6 address for locally generated IPv6 packets whose egress port is an SPBM NNI port.

The source-address value must be a locally configured loopback IPv6 address. The IS-IS automatically advertises the source-address to other SPBM edge routers when you enable IPv6 shortcuts. You must first configure a valid source-address before you enable IPv6 shortcuts.

## Syntax

- **ipv6-source-address WORD<0-46>**

## Command Parameters

WORD<0-46>

Enter isis ipv6 source address.

## Default

None

## Command Mode

IS-IS Router Configuration

---

## ipv6-source-address <ipv6-addr>

Assign a source IPv6 address for locally generated IPv6 packets that have an SPBM NNI port as an egress port.

The IPv6-source-address value must be a locally configured loopback IPv6 address. The IPv6 source address is automatically advertised by ISIS to other SPBM edge routers when IPv6 Shortcuts is enabled. IPv6 shortcuts cannot be enabled without first configuring a valid IPv6-source-address.

## Syntax

- **ipv6-source-address <ipv6-addr>**
- **no ipv6-source-address <ipv6-addr>**

## Default

None

## Command Mode

IS-IS Router Configuration

---

## is-type

Configure the router type globally. This release supports only Level 1 (L1) Intermediate-System-to-Intermediate-System (IS-IS).

## Syntax

- **default is-type**
- **is-type l1**
- **is-type l12**
- **no is-type**

## Command Parameters

**l1**

Configures the router type as Level 1 Intermediate-System-to-Intermediate-System (IS-IS).

**l12**

Configures the router type as Level 1 and Level 2 Intermediate-System-to-Intermediate-System (IS-IS). You cannot use this parameter in this release.

## Default

The default router type is Level 1 (l1).

## Command Mode

IS-IS Router Configuration

## manual-area (for IS-IS)

---

Configure an Intermediate-System-to-Intermediate-System (IS-IS) manual area, 1-13 bytes in the format <xx.xxx.xxx...xxx>. You must configure a manual area to use IS-IS. In this release, only one manual area is supported. Use the no format of this command to remove the area.

## Syntax

- **manual-area xx.xxxx.xxxx...xxx - 1...13 bytes**
- **no manual-area xx.xxxx.xxxx...xxx - 1...13 bytes**

## Command Parameters

**xx.xxxx.xxxx...xxx - 1...13 bytes**

Configures the manual area in a size up to 13 octets. The current release supports one area. For Intermediate-System-to-Intermediate-System (IS-IS) to operate, you must configure at least one area.

## Default

None

## Command Mode

IS-IS Router Configuration

## max-lsp-gen-interval

---

Configure the maximum level, in seconds, between generated Link State Packets (LSPs) by this Intermediate System.

### Syntax

- **default max-lsp-gen-interval**
- **max-lsp-gen-interval <30-900>**
- **no max-lsp-gen-interval**

### Command Parameters

<30-900>

Specifies the time interval at which the generated Link State Packet (LSP) is refreshed.

### Default

The default maximum interval value is 900.

## Command Mode

IS-IS Router Configuration

## metric

---

Configure the metric type that you can configure on an Intermediate-System-to-Intermediate-System (IS-IS) interface.

### Syntax

- **default metric**
- **metric { narrow | wide }**
- **no metric**

### Command Parameters

**narrow**

Configures the metric type as narrow. The switch only supports wide.

**wide**

Configures the metric type as wide. The switch only supports wide.

## Default

The default IS-IS metric type is wide.

## Command Mode

IS-IS Router Configuration

---

## multi-area dvr redistribute backbone

Configures the Multi-area SPB Distributed Virtual Routing backbone redistribution on the switch.

## Syntax

- **multi-area dvr redistribute backbone**
- **no multi-area dvr redistribute backbone**

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## multi-area ip redistribute routed-multicast

Configures the Multi-area SPB IPv4 multicast routing redistribution for home to remote direction, remote to home direction, or a specific route map policy.

## Syntax

- **multi-area ip redistribute routed-multicast**
- **multi-area ip redistribute routed-multicast [home-to-remote]**
- **multi-area ip redistribute routed-multicast [home-to-remote] [route-map WORD<1-64>]**
- **multi-area ip redistribute routed-multicast [home-to-remote] [enable]**
- **multi-area ip redistribute routed-multicast [remote-to-home]**
- **multi-area ip redistribute routed-multicast [remote-to-home] [route-map WORD<1-64>]**
- **multi-area ip redistribute routed-multicast [remote-to-home] [enable]**



## Command Parameters

### enable

Enables the Multi-area SPB IPv4 multicast routing redistribution.

### home-to-remote

Specifies the multicast routing redistribution configuration for home to remote direction.

### remote-to-home

Specifies the multicast routing redistribution configuration for remote to home direction.

### route-map WORD<1-64>

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## multi-area ip redistribute unicast

---

Configures the Multi-area SPB IPv4 unicast redistribution for home to remote direction, remote to home direction, or a specific route map policy.

## Syntax

- **multi-area ip redistribute unicast**
- **multi-area ip redistribute unicast [home-to-remote]**
- **multi-area ip redistribute unicast [home-to-remote] [route-map WORD<1-64>]**
- **multi-area ip redistribute unicast [home-to-remote] [enable]**
- **multi-area ip redistribute unicast [remote-to-home]**
- **multi-area ip redistribute unicast [remote-to-home] [route-map WORD<1-64>]**
- **multi-area ip redistribute unicast [remote-to-home] [enable]**

## Command Parameters

### enable

Enables the Multi-area SPB IPv4 unicast redistribution.

**home-to-remote**

Specifies the unicast redistribution configuration for home to remote direction.

**remote-to-home**

Specifies the unicast redistribution configuration for remote to home direction.

**route-map WORD<1-64>**

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## multi-area ipv6 redistribute unicast

---

Configures the Multi-area SPB IPv6 unicast redistribution for home to remote direction, remote to home direction, or a specific route map policy.

## Syntax

- **multi-area ipv6 redistribute unicast**
- **multi-area ipv6 redistribute unicast [home-to-remote]**
- **multi-area ipv6 redistribute unicast [home-to-remote] [route-map WORD<1-64>]**
- **multi-area ipv6 redistribute unicast [home-to-remote] [enable]**
- **multi-area ipv6 redistribute unicast [remote-to-home]**
- **multi-area ipv6 redistribute unicast [remote-to-home] [route-map WORD<1-64>]**
- **multi-area ipv6 redistribute unicast [remote-to-home] [enable]**

## Command Parameters

**enable**

Enables the Multi-area SPB IPv6 unicast redistribution.

**home-to-remote**

Specifies the unicast redistribution configuration for home to remote direction.

**remote-to-home**

Specifies the unicast redistribution configuration for remote to home direction.

**route-map WORD<1-64>**

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## multi-area l2 isid-list WORD<1-32>

Configures the Multi-area SPB layer 2 I-SID list that consists of specific I-SID values.

## Syntax

- **multi-area l2 isid-list WORD<1-32> WORD<1-1024>**
- **no multi-area l2 isid-list WORD<1-32> WORD<1-1024>**

## Command Parameters

**WORD<1-1024>**

Specifies the list of I-SID values.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## multi-area l2 redistribute i-sid deny-all except-isid-list

---

Configures the Multi-area SPB layer 2 I-SID redistribution to exclude all I-SID values specified in the I-SID list configured on the switch.

### Syntax

- **default multi-area l2 redistribute i-sid**
- **multi-area l2 redistribute i-sid deny-all except-isid-list WORD<1-32>**
- **no multi-area l2 redistribute i-sid deny-all except-isid-list**

### Command Parameters

WORD<1-32>

Specifies the name of the I-SID list.

### Default

The default is none.

### Command Mode

IS-IS Router Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## multi-area l2 redistribute i-sid permit-all except-isid-list

---

Configures the Multi-area SPB layer 2 I-SID redistribution to include all I-SID values specified in the I-SID list configured on the switch.

### Syntax

- **default multi-area l2 redistribute i-sid**
- **multi-area l2 redistribute i-sid permit-all except-isid-list WORD<1-32>**
- **no multi-area l2 redistribute i-sid permit-all except-isid-list**

### Command Parameters

WORD<1-32>

Specifies the name of the I-SID list.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

# multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215>

Configures the Multi-area SPB layer 2 multicast snooping I-SID redistribution for home to remote direction.

## Syntax

- `default multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215>`
- `default multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215> [enable]`
- `default multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215> [route-map]`
- `multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215>`
- `multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215> [enable]`
- `multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215> [route-map WORD<1-64>]`
- `no multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215>`
- `no multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215> [enable]`
- `no multi-area l2 redistribute snoop-multicast home-to-remote i-sid <1-16777215> [route-map]`

## Command Parameters

**enables**

Enables the Multi-area SPB layer 2 multicast snooping I-SID redistribution.

**route-map**

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

# multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32>

Configures the Multi-area SPB layer 2 multicast snooping I-SID list redistribution for home to remote direction.

## Syntax

- `default multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32>`
- `default multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32> [enable]`
- `default multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32> [route-map]`
- `multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32>`
- `multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32> [enable]`
- `multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32> [route-map WORD<1-64>]`
- `no multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32>`
- `no multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32> [enable]`
- `no multi-area l2 redistribute snoop-multicast home-to-remote isid-list WORD<1-32> [route-map]`

## Command Parameters

`enable`

Enables the Multi-area SPB layer 2 multicast snooping I-SID redistribution.

`route-map WORD<1-64>`

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## multi-area l2 redistribute snoop-multicast i-sid <1-16777215>

Configures the Multi-area SPB layer 2 multicast snooping I-SID redistribution.

## Syntax

- `default multi-area l2 redistribute snoop-multicast i-sid <1-16777215>`
- `default multi-area l2 redistribute snoop-multicast i-sid <1-16777215> [enable]`
- `default multi-area l2 redistribute snoop-multicast i-sid <1-16777215> [route-map]`
- `multi-area l2 redistribute snoop-multicast i-sid <1-16777215>`
- `multi-area l2 redistribute snoop-multicast i-sid <1-16777215> [enable]`
- `multi-area l2 redistribute snoop-multicast i-sid <1-16777215> [route-map WORD<1-64>]`
- `no multi-area l2 redistribute snoop-multicast i-sid <1-16777215>`
- `no multi-area l2 redistribute snoop-multicast i-sid <1-16777215> [enable]`
- `no multi-area l2 redistribute snoop-multicast i-sid <1-16777215> [route-map]`

## Command Parameters

**enable**

Enables Multi-area SPB layer 2 multicast snooping I-SID redistribution.

**route-map WORD<1-64>**

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## multi-area l2 redistribute snoop-multicast isid-list WORD<1-32>

Configures the Multi-area SPB layer 2 multicast snooping I-SID list redistribution.

## Syntax

- `default multi-area l2 redistribute snoop-multicast isid-list WORD<1-32>`
- `default multi-area l2 redistribute snoop-multicast isid-list WORD<1-32> [enable]`
- `default multi-area l2 redistribute snoop-multicast isid-list WORD<1-32> [route-map]`
- `multi-area l2 redistribute snoop-multicast isid-list WORD<1-32>`
- `multi-area l2 redistribute snoop-multicast isid-list WORD<1-32> [enable]`
- `multi-area l2 redistribute snoop-multicast isid-list WORD<1-32> [route-map WORD<1-64>]`
- `no multi-area l2 redistribute snoop-multicast isid-list WORD<1-32>`
- `no multi-area l2 redistribute snoop-multicast isid-list WORD<1-32> [enable]`
- `no multi-area l2 redistribute snoop-multicast isid-list WORD<1-32> [route-map]`

## Command Parameters

`enable`

Enables Multi-area SPB layer 2 multicast snooping I-SID list redistribution.

`route-map WORD<1-64>`

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration



## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215>

Configures the Multi-area SPB layer 2 multicast snooping I-SID redistribution for remote to home direction.

## Syntax

- `default multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215>`
- `default multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215> [enable]`
- `default multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215> [route-map]`
- `multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215>`
- `multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215> [enable]`
- `multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215> [route-map WORD<1-64>]`
- `no multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215>`
- `no multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215> [enable]`
- `no multi-area l2 redistribute snoop-multicast remote-to-home i-sid <1-16777215> [route-map]`

## Command Parameters

### enables

Enables the Multi-area SPB layer 2 multicast snooping I-SID redistribution.

### route-map

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32>

Configures the Multi-area SPB layer 2 multicast snooping I-SID list redistribution for remote to home direction.

## Syntax

- `default multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32>`
- `default multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32> [enable]`
- `default multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32> [route-map]`
- `multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32>`
- `multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32> [enable]`
- `multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32> [route-map WORD<1-64>]`
- `no multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32>`
- `no multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32> [enable]`
- `no multi-area l2 redistribute snoop-multicast remote-to-home isid-list WORD<1-32> [route-map]`

## Command Parameters

**enables**

Enables the Multi-area SPB layer 2 multicast snooping I-SID redistribution.

**route-map WORD<1-64>**

Specifies the name of the route map policy.

## Default

The default is none.

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## overload

---

Configure the overload condition. If the overload bit parameter is configured, the switch sets the overload bit in the Link State Packet (LSP). The setting affects Level 1 LSPs.

The overload parameter works in conjunction with the overload-on-startup parameter. When the overload-on-startup timer expires, the Shortest Path Bridging MAC (SPBM) node clears the overload bit and re-advertises its LSP.

When an LSP with an overload bit is received, the switch ignores the LSP in its SPF calculation. By default, overload is set to false. If overload is set to true, the switch cannot be a transit node, but it can still receive traffic destined to the switch.

## Syntax

- **default overload**
- **no overload**
- **overload**

## Default

The default is disabled.

## Command Mode

IS-IS Router Configuration

## overload-on-startup

---

Configure the Intermediate-System-to-Intermediate-System (IS-IS) overload-on-startup value in seconds.

## Syntax

- **default overload-on-startup**
- **no overload-on-startup**
- **overload-on-startup <15-3600>**

## Command Parameters

<15-3600>

Specifies the Intermediate-System-to-Intermediate-System (IS-IS) overload-on-startup value in seconds. The overload-on-startup value is used as a timer to control when to send out Link State Packets (LSPs) with the overload bit cleared after IS-IS startup.

## Default

The default overload-on-startup value is 20 seconds.

## Command Mode

IS-IS Router Configuration

## psnp-interval

---

Configure the Partial Sequence Number Packets (PSNP) interval in seconds. This command is a system level parameter that applies to Level 1 PSNP generation on all interfaces.

## Syntax

- **default psnp-interval**
- **psnp-interval <1-120>**

## Command Parameters

<1-120>

Configures the interval, in seconds. This is a system level parameter that applies for Level 1 Partial Sequence Number Packet (PSNP) generation on all interfaces. A longer interval reduces overhead, while a shorter interval speeds up convergence.

## Default

The default PSNP value is 2 seconds.

## Command Mode

IS-IS Router Configuration

## redistribute bgp (for IS-IS)

---

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

## Syntax

- **default redistribute bgp enable**
- **default redistribute bgp metric**

- **default redistribute bgp metric-type**
- **default redistribute bgp route-map**
- **default redistribute bgp subnets**
- **no redistribute bgp**
- **no redistribute bgp enable**
- **no redistribute bgp metric**
- **no redistribute bgp metric-type**
- **no redistribute bgp route-map**
- **no redistribute bgp subnets**
- **redistribute bgp**
- **redistribute bgp enable**
- **redistribute bgp metric <0-65535>**
- **redistribute bgp metric-type external**
- **redistribute bgp metric-type internal**
- **redistribute bgp route-map WORD<0-64>**
- **redistribute bgp subnets allow**
- **redistribute bgp subnets suppress**

## Command Parameters

### **enable**

Enables the redistribution of the BGP into the Shortest Path Bridging MAC (SPBM) network. The prefix "default" before the command sets the isis redistribute bgp enable to default.

### **enable**

Enables the redistribution of the specified protocol into the Shortest Path Bridging MAC (SPBM) network.

### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### **metric-type external**

Configures the type of route to import into the BGP. The prefix "default" before the command sets the isis redistribute metric-type to default. The default is internal.

### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type internal**

Configures the type of route to import into the BGP. The prefix "default" before the command sets the isis redistribute metric-type to default. The default is internal.

### **metric-type internal**

Configures the type of route to import into the protocol. The default is internal.

### **route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

**subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The prefix "default" before the command sets the isis redistribute subnets to default. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The prefix "default" before the command sets the isis redistribute subnets to default. The default is allow.

## Default

By default, route redistribution is disabled.

## Command Mode

IS-IS Router Configuration

## redistribute direct (for IS-IS)

---

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

## Syntax

- **default redistribute direct enable**
- **default redistribute direct metric**
- **default redistribute direct metric-type**
- **default redistribute direct route-map**
- **default redistribute direct subnets**
- **no redistribute direct**
- **no redistribute direct enable**
- **no redistribute direct metric**
- **no redistribute direct metric-type**
- **no redistribute direct route-map**

- **no redistribute direct subnets**
- **redistribute direct**
- **redistribute direct enable**
- **redistribute direct metric <0-65535>**
- **redistribute direct metric-type external**
- **redistribute direct metric-type internal**
- **redistribute direct route-map WORD<0-64>**
- **redistribute direct subnets allow**
- **redistribute direct subnets suppress**

## Command Parameters

### **enable**

Enables route redistribution of the direct protocol. The prefix "default" before the command sets the isis redistribute direct enable to default.

### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type internal**

Configures the type of route to import into the direct protocol. The prefix "default" before the command sets the isis redistribute metric-type to default. The default is internal.

### **route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

### **subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

### **subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

## Default

By default, route redistribution is disabled.

## Command Mode

IS-IS Router Configuration

---

## redistribute ospf (for IS-IS)

---

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

### Syntax

- **default redistribute ospf enable**
- **default redistribute ospf metric**
- **default redistribute ospf metric-type**
- **default redistribute ospf route-map**
- **default redistribute ospf subnets**
- **no redistribute ospf**
- **no redistribute ospf enable**
- **no redistribute ospf metric**
- **no redistribute ospf metric-type**
- **no redistribute ospf route-map**
- **no redistribute ospf subnets**
- **redistribute ospf**
- **redistribute ospf enable**
- **redistribute ospf metric <0-65535>**
- **redistribute ospf metric-type external**
- **redistribute ospf metric-type internal**
- **redistribute ospf route-map WORD<0-64>**
- **redistribute ospf subnets allow**
- **redistribute ospf subnets suppress**

### Command Parameters

#### **enable**

Enables the redistribution of the OSPF protocol into the Shortest Path Bridging MAC (SPBM) network.

#### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

#### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

#### **metric-type internal**

Configures the type of route to import into the protocol. The default is internal.

#### **route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

#### **subnets allow**



Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

#### **subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

## Default

By default, route redistribution is disabled.

## Command Mode

IS-IS Router Configuration

## redistribute rip (for IS-IS)

---

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

## Syntax

- **default redistribute rip enable**
- **default redistribute rip metric**
- **default redistribute rip metric-type**
- **default redistribute rip route-map**
- **default redistribute rip subnets**
- **no redistribute rip**
- **no redistribute rip enable**
- **no redistribute rip metric**
- **no redistribute rip metric-type**
- **no redistribute rip route-map**
- **no redistribute rip subnets**
- **redistribute rip**
- **redistribute rip enable**
- **redistribute rip metric <0-65535>**
- **redistribute rip metric-type external**
- **redistribute rip metric-type internal**
- **redistribute rip route-map WORD<0-64>**
- **redistribute rip subnets allow**
- **redistribute rip subnets suppress**

## Command Parameters

### **enable**

Enables route redistribution.

### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type internal**

Configures the type of route to import into the protocol.

### **route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

### **subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

### **subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

## Default

By default, route redistribution is disabled.

## Command Mode

IS-IS Router Configuration

## redistribute static (for IS-IS)

---

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

## Syntax

- **default redistribute static enable**
- **default redistribute static metric**
- **default redistribute static metric-type**
- **default redistribute static route-map**
- **default redistribute static subnets**
- **no redistribute static**
- **no redistribute static enable**

- **no redistribute static metric**
- **no redistribute static metric-type**
- **no redistribute static route-map**
- **no redistribute static subnets**
- **redistribute static**
- **redistribute static enable**
- **redistribute static metric <0-65535>**
- **redistribute static metric-type external**
- **redistribute static metric-type internal**
- **redistribute static route-map WORD<0-64>**
- **redistribute static subnets allow**
- **redistribute static subnets suppress**

## Command Parameters

### **enable**

Enables route redistribution.

### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type internal**

Configures the type of route to import into the protocol. The default is internal.

### **route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

### **subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

### **subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

## Default

By default, route redistribution is disabled.

## Command Mode

IS-IS Router Configuration

---

## retransmit-lsp-interval

---

Configure the minimum time between retransmission of a Link State Packet (LSP). This defines how fast the switch resends the same LSP. This is a system level parameter that applies for Level 1 retransmission of LSPs.

### Syntax

- **default retransmit-lsp-interval**
- **no retransmit-lsp-interval**
- **retransmit-lsp-interval <1-300>**

### Command Parameters

<1-300>

Specifies the minimum time between retransmission of a Link State Packet (LSP). This defines how fast the switch resends the same LSP. This is a system level parameter that applies for Level 1 retransmission of LSPs.

### Default

The default is 5 seconds.

### Command Mode

IS-IS Router Configuration

---

## spbm <1-100>

---

Create the Shortest Path Bridging MAC (SPBM) instance globally. This release supports only one instance. Use the no form of the command to delete the instance globally.

### Syntax

- **no spbm <1-100>**
- **spbm <1-100>**

### Command Parameters

<1-100>

Specifies the Shortest Path Bridging MAC (SPBM) instance ID. Creates the SPBM instance. In this release only one SPBM instance is supported.

### Default

None

## Command Mode

IS-IS Router Configuration

### spbm <1-100> b-vid

---

Add the backbone VLAN (B-VLAN) to the Shortest Path Bridging MAC (SPBM) instance, globally. You can configure a maximum of two B-VLANs. If you add only one B-VLAN to the SPBM instance, it becomes the primary B-VLAN. If you configure two B-VLANs, you must configure one as the primary B-VLAN. Use the no format to remove a B-VLAN from the global SPBM instance.

## Syntax

- **no spbm <1-100> b-vid List of VLAN Ids {vlan-id[-vlan-id][,...]}**
- **no spbm <1-100> b-vid List of VLAN Ids {vlan-id[-vlan-id][,...]} primary <1-4059>**
- **spbm <1-100> b-vid List of VLAN Ids {vlan-id[-vlan-id][,...]}**
- **spbm <1-100> b-vid List of VLAN Ids {vlan-id[-vlan-id][,...]} primary <1-4059>**

## Command Parameters

{vlan-id[-vlan-id][,...]}

Specifies the VLANs to add to the Shortest Path Bridging MAC (SPBM) instance as Backbone VLANs (B-VLANs). Sets the IS-IS SPBM instance data VLANs.

<1-100>

Specifies the Shortest Path Bridging MAC (SPBM) instance ID.

**primary <1-4059>**

Specifies the primary B-VLAN by VLAN ID.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

IS-IS Router Configuration

### spbm <1-100> ip

---

Configure Shortest Path Bridging MAC (SPBM) IP shortcuts.

## Syntax

- **default spbm <1-100> ip enable**
- **no spbm <1-100> ip enable**
- **spbm <1-100> ip enable**

## Command Parameters

<1-100>

Specifies the Shortest Path Bridging MAC (SPBM) instance ID.

**ip enable**

Enables Shortest Path Bridging MAC (SPBM) IP shortcuts.

## Default

The default is disabled.

## Command Mode

IS-IS Router Configuration

---

## spbm <1-100> ipv6

Configure Shortest Path Bridging MAC (SPBM) IPv6 shortcuts.

## Syntax

- **default spbm <1-100> ipv6 enable**
- **no spbm <1-100> ipv6 enable**
- **spbm <1-100> ipv6 enable**

## Command Parameters

<1-100>

Specifies the Shortest Path Bridging MAC (SPBM) instance ID.

**enable**

Enables Shortest Path Bridging MAC (SPBM) IPv6 shortcuts.

## Default

The default is disabled.

## Command Mode

IS-IS Router Configuration

## spbm <1-100> lsdb-trap

---

Enable a trap when the Shortest Path Bridging MAC (SPBM) Link State Database (LSDB) changes.

### Syntax

- **default spbm <1-100> lsdb-trap enable**
- **no spbm <1-100> lsdb-trap enable**
- **spbm <1-100> lsdb-trap enable**

### Command Parameters

<1-100>

Specifies the Shortest Path Bridging MAC (SPBM) instance ID.

**enable**

Enables a trap when the Shortest Path Bridging MAC (SPBM) Link State Database (LSDB) changes.

### Default

The default is disabled.

### Command Mode

IS-IS Router Configuration

## spbm <1-100> multicast

---

Enables SPBM multicast globally.

### Syntax

- **default spbm <1-100> multicast enable**
- **no spbm <1-100> multicast enable**
- **spbm <1-100> multicast enable**

### Command Parameters

<1-100>

Specifies the Shortest Path Bridging MAC (SPBM) instance ID.

**enable**

Enables SPBM multicast globally.

## Default

The default is disabled.

## Command Mode

IS-IS Router Configuration

## spbm <1-100> multicast fwd-cache-timeout

---

Configures the timeout value for the Global Router.

## Syntax

- **default spbm <1-100> multicast fwd-cache-timeout**
- **no spbm <1-100> multicast fwd-cache-timeout**
- **spbm <1-100> multicast fwd-cache-timeout <10-86400>**

## Command Parameters

<10-86400>

fwd-cache-timeout value in seconds.

<1-100>

Specifies the Shortest Path Bridging MAC (SPBM) instance ID. Creates the SPBM instance. In this release only one SPBM instance is supported.

## Default

The default is 210 seconds.

## Command Mode

IS-IS Router Configuration

## spbm <1-100> multicast spb-pim-gw controller

---

Configures SPB-PIM gateway controller.

## Syntax

- **default spbm <1-100> multicast spb-pim-gw controller enable**
- **no spbm <1-100> multicast spb-pim-gw controller enable**
- **spbm <1-100> multicast spb-pim-gw controller enable**



## Command Parameters

### **enable**

Enables the SPB-PIM Gateway Controller.

## Default

The default is disabled.

## Command Mode

IS-IS Router Configuration

---

## spbm <1-100> nick-name (for IS-IS)

Configure a global nick-name for the Shortest Path Bridging MAC (SPBM) instance. The system uses the nick-name to calculate the multicast address for the node.

## Syntax

- **default spbm <1-100> nick-name**
- **no spbm <1-100> nick-name**
- **spbm <1-100> nick-name x.xx.xx - 2.5 bytes**

## Command Parameters

### **<1-100>**

Specifies the SPBM instance ID.

### **nick-name x.xx.xx - 2.5 bytes**

Specifies the system nick-name (2.5 bytes in the format <x.xx.xx>).

## Default

By default, no nickname exists.

## Command Mode

IS-IS Router Configuration

---

## spbm <1-100> smlt-peer-system-id

Configure the system ID of the interswitch trunk (IST) peer, so that if it goes down, the local peer can take over forwarding for the failed peer. You must configure this command to use Shortest Path Bridging MAC (SPBM) in a Split MultiLink Trunking (SMLT) environment. The device with the lower system ID is the primary device.

## Syntax

- **spbm <1-100> smlt-peer-system-id xxxx.xxxx.xxxx - 6 bytes**

## Command Parameters

### <1-100>

Specifies the SPBM instance ID. SMLT peer system ID is part of the required configuration. You must configure the SMLT peer system ID as the nodal MAC of the peer device. In the Intermediate-System-to-Intermediate-System (IS-IS) network, the nodal MAC of devices should be eight apart from each other.

### xxxx.xxxx.xxxx - 6 bytes

Specifies the nodal MAC of the peer device as the system ID. Nodal MACs of devices in the Intermediate-System-to-Intermediate-System (IS-IS) network must be 8 apart from each other.

Split MultiLink Trunking (SMLT) peer system ID is part of the required configuration. If SMLT virtual Backbone MAC (B-MAC) is not configured, it is derived from the configured SMLT peer system ID and the nodal MAC of the device (IS-IS system ID).

SMLT split Backbone Edge Bridge (BEB) is also derived from the SMLT peer system ID and nodal MAC of the device.

The device with the lower system ID is primary, the device with the higher system ID is secondary.

## Default

None

## Command Mode

IS-IS Router Configuration

## spbm <1-100> smlt-virtual-bmac

---

Configure the virtual Backbone MAC (B-MAC) address, which is shared and advertised by both peers. Configuration of this command is optional.

## Syntax

- **spbm <1-100> smlt-virtual-bmac 0x00:0x00:0x00:0x00:0x00:0x00**

## Command Parameters

### <1-100>

Specifies the SPBM instance ID.

0x00:0x00:0x00:0x00:0x00:0x00

Specifies the virtual MAC address. SMLT virtual B-MAC is the optional configuration. If SMLT virtual B-MAC is not configured, the system derives SMLT virtual B-MAC from the configured SMLT peer system ID and the nodal MAC of the device (IS-IS system ID).

The system compares the nodal MAC of the device with the SMLT peer system ID configured and takes the small one, plus 0x01, as the SMLT virtual B-MAC. The system also derives SMLT split BEB from the SMLT peer system ID and nodal MAC of the device.

The device with the lower system ID is primary, the device with the higher system ID is secondary.

## Default

None

## Command Mode

IS-IS Router Configuration

## spbm <1-100> stp-multi-homing

---

Sets the MSTP-Fabric Connect Multi Homing support on the switch.

## Syntax

- **default spbm <1-100> stp-multi-homing enable**
- **no spbm <1-100> stp-multi-homing enable**
- **spbm <1-100> stp-multi-homing enable**

## Command Parameters

**enable**

Enables MSTP-Fabric Connect Multi Homing on the specific SPBM instance.

## Default

Disabled

## Command Mode

IS-IS Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information, see [VOSS User Guide](#).

---

## spf-delay

---

Configure the delay, in milliseconds, to pace successive Shortest Path First (SPF) runs. The timer prevents more than two SPF runs from being scheduled back-to-back. The mechanism for pacing SPF allows two back-to-back SPF runs.

### Syntax

- **default spf-delay**
- **no spf-delay**
- **spf-delay <0-5000>**

### Command Parameters

<0-5000>

Configures the delay, in milliseconds.

### Default

The default is 100 milliseconds.

### Command Mode

IS-IS Router Configuration

---

## sys-name

---

Configure the name for the system.

### Syntax

- **default sys-name**
- **no sys-name**
- **sys-name WORD<0-255>**

### Command Parameters

WORD<0-255>

Specifies the system name.

### Default

By default, the system name is the host name at the system level.

## Command Mode

IS-IS Router Configuration

## system-id (for IS-IS)

---

Configure a system ID. You must configure a system ID before you enable IS-IS. You cannot delete the system ID but you can change it if you first disable IS-IS.

## Syntax

- **default system-id**
- **no system-id**
- **system-id xxxx.xxxx.xxxx - 6 bytes**
- **system-id xxxx.xxxx.xxxx - 6 bytes**

## Command Parameters

xxxx.xxxx.xxxx - 6 bytes

Specifies the system ID in 6 octets.

## Default

The default system ID is the node Backbone MAC.

## Command Mode

IS-IS Router Configuration



# IS-IS Router Remote Configuration

---

The following topics document commands available in IS-IS Router Remote Configuration mode of the command line interface (CLI).

## area-name (for remote IS-IS)

---

Configures the area name for the remote area.

### Syntax

- **area-name WORD<0-255>**
- **no area-name**
- **default area-name**

### Command Parameters

**WORD<0-255>**

Specifies the area name.

### Default

The default value is area-manual-area, where manual-area represents the remote IS-IS manual-area value that you configure.

### Command Mode

IS-IS Router Remote Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## area-vnode nick-name (for remote IS-IS)

---

Configures the remote IS-IS Multi-area SPB virtual node nick name.

## Syntax

- **area-vnode nick-name <x.xx.xx>**
- **default area-vnode nick-name**
- **no area-vnode nick-name**

## Command Parameters

<x.xx.xx>

Specifies the nickname for the Multi-area SPB virtual node. The value is 2.5 bytes.

## Default

The default is none.

## Command Mode

IS-IS Router Remote Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## area-vnode system-id (for remote IS-IS)

---

Configures the remote IS-IS Multi-area SPB virtual node system ID.

## Syntax

- **area-vnode system-id xxxx.xxxx.xxxx**
- **default area-vnode system-id**
- **no area-vnode system-id**

## Command Parameters

xxxx.xxxx.xxxx

Specifies the IS-IS Multi-area SPB virtual node system ID.

## Default

None

## Command Mode

IS-IS Router Remote Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## area-vnode sys-name (for remote IS-IS)

---

Configures the remote IS-IS Multi-area SPB virtual node system name.

## Syntax

- **area-vnode sys-name WORD<0-255>**
- **default area-vnode sys-name**
- **no area-vnode sys-name**

## Command Parameters

WORD<0-255>

Specifies the remote IS-IS Multi-area SPB virtual node system name.

## Default

None

## Command Mode

IS-IS Router Remote Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## manual-area (for remote IS-IS)

---

Configure a remote Intermediate-System-to-Intermediate-System (IS-IS) manual area, 1-13 bytes in the format <xx.xxx.xxx...xxxx>. You must configure a manual area to use the remote IS-IS.

## Syntax

- **manual-area xx.xxxx.xxxx...xxxx**
- **no manual-area xx.xxxx.xxxx...xxxx**



## Command Parameters

`XX.XXXX.XXXX...XXXX`

Configures the manual area in a size up to 13 octets. For a remote Intermediate-System-to-Intermediate-System (IS-IS) to operate, you must configure at least one area.

## Default

The default is none.

## Command Mode

IS-IS Router Remote Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## spbm <1-100> nick-name (for remote IS-IS)

---

Configures a nick-name for the remote Shortest Path Bridging MAC (SPBM) instance. The system uses the nick-name to calculate the multicast address for the nodes.

## Syntax

- **default spbm <1-100> nick-name**
- **no spbm <1-100> nick-name**
- **spbm <1-100> nick-name x.xx.xx**

## Command Parameters

`<1-100>`

Specifies the SPBM instance ID.

`nick-name x.xx.xx`

Specifies the system nick-name (2.5 bytes in the format <x.xx.xx>).

## Default

By default, no nickname exists.

## Command Mode

IS-IS Router Remote Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## system-id (for remote IS-IS)

---

Configures a system ID. You must configure a system ID before you enable remote IS-IS. You cannot delete the system ID but you can change it if you first disable remote IS-IS.

## Syntax

- **default system-id**
- **no system-id**
- **system-id *xxxx.xxxx.xxxx***

## Command Parameters

*xxxx.xxxx.xxxx*

Specifies the system ID in 6 octets.

## Default

None

## Command Mode

IS-IS Router Remote Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).



# Logical Interface Configuration

---

The following topics document commands available in Logical Interface Configuration mode of the command line interface (CLI).

## auth-key

---

Configure the IPsec authentication key on a logical device.

### Syntax

- **auth-key WORD<1-32>**
- **no auth-key**

### Command Parameters

**WORD<1-32>**

Configures the authentication key value.

### Default

None

### Command Mode

Logical Interface Configuration

## bfd enable

---

Enable Bidirectional Forwarding Detection (BFD) on a logical interface.

### Syntax

- **bfd enable**
- **no bfd enable**

### Default

None

## Command Mode

Logical Interface Configuration

## egress-shaping-rate

---

Configures the egress shaping rate on a logical interface.

### Syntax

- **default egress-shaping-rate**
- **egress-shaping-rate <1-1000>**
- **no egress-shaping-rate**

### Command Parameters

<1-1000>

The shaper bandwidth in Mbps.

### Default

The default value is 0. Egress Tunnel Shaping is disabled.

## Command Mode

Logical Interface Configuration

## ipsec

---

Enable IPsec on a logical interface.

### Syntax

- **ipsec**
- **no ipsec**
- **default ipsec**

### Default

None

## Command Mode

Logical Interface Configuration

---

## ipsec auth-method

---

Configure the IPsec authentication method for the tunnel.

### Syntax

- **default ipsec auth-method**
- **ipsec auth-method <pre-share | rsa-sig>**
- **ipsec auth-method rsa-sig [cert-subject-name WORD<1-45>]**

### Command Parameters

**<pre-share | rsa-sig>**

Specifies the IPsec authentication method as either a pre-shared key or RSA signature for digital certificates.

**cert-subject-name WORD<1-45>**

Specifies the digital certificate subject name to be used as the identity certificate. If a subject name is not specified, the default certificate subject name is Global.

### Default

The default is a pre-shared key.

### Command Mode

Logical Interface Configuration

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## ipsec compression

---

IPsec compression reduces the size of the IP datagram to improve the communication performance between hosts connected behind Backbone Edge Bridges (BEB).

### Syntax

- **default ipsec compression**
- **ipsec compression**
- **no ipsec compression**

## Default

The default is disabled.

## Command Mode

Logical Interface Configuration

## Usage Guidelines



### Tip

As a best practice, use IPsec compression only for Fabric Extend tunnels where latency is greater than 70ms.

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipsec esp

---

Configure the Encapsulating Security Payload (ESP) cipher suite for IPsec.

## Syntax

- **default ipsec esp**
- **ipsec esp [<aes128gcm16-sha256 | aes256-sha256 | aes256gcm16-sha256 >]**

## Command Parameters

<aes128gcm16-sha256>

Specifies the AES cipher with a 128-bit encryption key and GCM block mode.

<aes256-sha256>

Specifies the AES cipher with a 256-bit encryption key and CBC block mode (for QAT performance mode).

< aes256gcm16-sha256>

Specifies the AES cipher with a 256-bit encryption key and GCM block mode.

## Default

The default is aes128gcm16-sha256.

## Command Mode

Logical Interface Configuration

## Usage Guidelines

This command only applies to XA1400 Series.

## ipsec fragment-before-encrypt

---

Configures IPsec fragmentation of the packets to occur before encryption and IPsec encapsulation.

### Syntax

- **ipsec fragment-before-encrypt**
- **no ipsec fragment-before-encrypt**

### Default

The default is disabled.

### Command Mode

Logical Interface Configuration

## Usage Guidelines

This command only applies to XA1400 Series.

## ipsec remote-nat-ip

---

Configures the Network Address Translation Traversal (NAT-T) Responder device public IP address.

### Syntax

- **ipsec remote-nat-ip {A.B.C.D}**
- **no ipsec remote-nat-ip**

### Command Parameters

{A.B.C.D}

Specifies the IP address of the Responder device in an IPsec NAT-T connection.

### Default

None.

### Command Mode

Logical Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipsec responder-only

---

Configure one side of an IPsec Network Address Translation Traversal (NAT-T) connection as a Responder device. By default, both sides of an IPsec NAT-T connection are initiators.

### Syntax

- **ipsec responder-only**
- **no ipsec responder-only**

### Default

The default is initiator.

### Command Mode

Logical Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipsec tunnel-dest-ip

---

Configures the destination IP address for IPsec tunnel.

### Syntax

- **ipsec tunnel-dest-ip {A.B.C.D}**
- **no ipsec tunnel-dest-ip**

### Command Parameters

{A.B.C.D}

Specifies the destination IP address of the IPsec tunnel.

### Default

None.



## Command Mode

Logical Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipsec tunnel-source-address type

---

Configure a specific IPsec source IP address for each IPsec tunnel.

## Syntax

- **ipsec tunnel-source-address type dhcp**
- **ipsec tunnel-source-address type static {A.B.C.D}**
- **no ipsec tunnel-source-address**

## Command Parameters

**dhcp**

Dynamically obtains the source IP address for the IPsec tunnel from DHCP.

**static {A.B.C.D}**

Specifies the manually configured source IP address of the IPsec tunnel. The IP address must be on the same VRF as the source IP address for IP tunnel.

## Default

The default is no configured address.

## Command Mode

Logical Interface Configuration

## Usage Guidelines

This command only applies to XA1400 Series.

## isis enable

---

Create an IS-IS circuit and interface on the selected logical interface.

## Syntax

- **default isis enable**
- **isis**
- **isis enable**
- **no isis**
- **no isis enable**

## Default

None

## Command Mode

Logical Interface Configuration

## isis hello-auth

---

Specify the authentication type used for IS-IS hello packets on the logical interface. The type can be one of the following: none, hmac-md5, or hmac-sha-256.

## Syntax

- **default isis hello-auth**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 }**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 } key WORD<1-16>**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 } key WORD<1-16> key-id <1-255>**
- **no isis hello-auth**

## Command Parameters

**key WORD<1-16>**

Specifies the authentication key (password) used by the receiving router to verify the packet.

**key-id <1-255>**

Specifies the optional key ID.

**type { none | simple | hmac-md5 | hmac-sha-256 }**

Specifies the authentication type used for IS-IS hello packets on the interface. The type can be one of the following: none, simple, hmac-md5, or hmac-sha-256. The default type is none. Use the no or default options to set the hello-auth type to none.

- If simple is selected, you can also specify a key value. Simple password authentication uses a text password in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet.

- If `hmac-md5` is selected, you can also specify a key value and key-id. MD5 authentication creates an encoded checksum in the transmitted packet. The receiving router uses an authentication key (password) to verify the MD5 checksum of the packet.
- If `hmac-sha-256` is selected, you can also specify a key value and key-id. With SHA-256 authentication, the switch adds an HMAC-SHA256 digest to each Hello packet. The switch that receives the Hello packet computes the digest of the packet and compares it with the received digest. If the digests match, the packet is accepted. If the digests do not match, the receiving switch discards the packet.

## Default

The default is no authentication type (none).

## Command Mode

Logical Interface Configuration

## isis l1-dr-priority

---

Configure the Level 1 IS-IS designated router priority to the specified value.

## Syntax

- **default isis l1-dr-priority**
- **isis l1-dr-priority <0-127>**
- **no isis l1-dr-priority**

## Command Parameters

<0-127>

Configures the Level 1 IS-IS designated router priority to the specified value.

## Default

The default Level 1 designated router priority value is 64.

## Command Mode

Logical Interface Configuration

## isis l1-hello-interval

---

Configure the hello interval to change how often hello packets are sent out from an interface level.

## Syntax

- **default isis l1-hello-interval**
- **isis l1-hello-interval <1-600>**
- **no isis l1-hello-interval**

## Command Parameters

<1-600>

Configures the Level 1 hello interval.

## Default

The default Level 1 hello interval value is 9 seconds.

## Command Mode

Logical Interface Configuration

---

## isis l1-hello-multiplier

Configure the hello multiplier to specify how many hellos the switch must miss before it considers the adjacency with a neighboring switch down.

## Syntax

- **default isis l1-hello-multiplier**
- **isis l1-hello-multiplier <1-600>**
- **no isis l1-hello-multiplier**

## Command Parameters

<1-600>

Configures the Level 1 hello multiplier.

## Default

The default Level 1 hello-multiplier value is 3.

## Command Mode

Logical Interface Configuration

---

## isis spbm

Enable the SPBM instance on the logical interface.

## Syntax

- **default isis spbm <1-100> interface-type**
- **default isis spbm <1-100> ll-metric**
- **isis spbm <1-100>**
- **isis spbm <1-100> interface-type { broadcast | pt-pt }**
- **isis spbm <1-100> ll-metric <1-16777215>**
- **no isis spbm <1-100>**
- **no isis spbm <1-100> interface-type**
- **no isis spbm <1-100> ll-metric**

## Command Parameters

**<1-100>**

Specifies the SPBM instance ID.

**interface-type { broadcast | pt-pt }**

Configures the SPBM instance interface type.

**ll-metric <1-16777215>**

Configures the cost for the SPBM instance.

## Default

None

## Command Mode

Logical Interface Configuration



# Loopback Interface Configuration

---

The following topics document commands available in Loopback Interface Configuration mode of the command line interface (CLI).

## ip address (loopback)

---

Configure a circuitless IP interface (CLIP) when you want to provide a virtual interface that is not associated with a physical port. You can use a CLIP interface to provide uninterrupted connectivity to your switch.

### Syntax

- **ip address <1-256> {A.B.C.D/X}**
- **ip address <1-256> {A.B.C.D/X} vrf WORD<1-16>**
- **ip address <1-256> {A.B.C.D} {A.B.C.D}**
- **ip address {A.B.C.D/X}**
- **ip address {A.B.C.D/X} vrf WORD<1-16>**
- **ip address {A.B.C.D} {A.B.C.D}**
- **no ip address <1-256> {A.B.C.D}**
- **no ip address <1-256> {A.B.C.D} vrf WORD<1-16>**
- **no ip address {A.B.C.D}**
- **no ip address {A.B.C.D} vrf WORD<1-16>**

### Command Parameters

[vrf WORD<1-16>]

Specifies an associated VRF by name.

{A.B.C.D/X}

Specifies the IP address and subnet mask.

{A.B.C.D}

Specifies the IP address.

<1-256>

Specifies the interface identification number for the circuitless IP (CLIP).

## Default

None

## Command Mode

Loopback Interface Configuration

## ip area (loopback)

---

Designate an area for the circuitless IP (CLIP) interface.

## Syntax

- `default ip area`
- `default ip area <1-256>`
- `default ip area vrf WORD<1-16>`
- `ip area <1-256> {A.B.C.D}`
- `ip area <1-256> {A.B.C.D} vrf WORD<1-16>`
- `ip area {A.B.C.D}`
- `ip area {A.B.C.D} vrf WORD<1-16>`
- `no ip area`
- `no ip area <1-256>`
- `no ip area vrf WORD<1-16>`

## Command Parameters

`{A.B.C.D}`

Specifies the IP address of the OSPF area that is associated with the CLIP.

`<1-256>`

Specifies the interface identification number for the CLIP.

`vrf WORD<1-16>`

Specifies an associated VRF by name.

## Default

None

## Command Mode

Loopback Interface Configuration

## ip bfd (for a loopback)

---

Enable and configure Bidirectional Forwarding Detection (BFD) on a loopback interface.

## Syntax

- `default ip bfd enable`
- `default ip bfd interval`
- `default ip bfd min-rx`
- `default ip bfd multiplier`
- `ip bfd enable`
- `ip bfd interval <100-65335>`
- `ip bfd min-rx <100-65335>`
- `ip bfd multiplier <1-20>`
- `ip bfd loopback <1-256>`
- `no ip bfd enable`
- `no ip bfd loopback`

## Command Parameters

### enable

Enable BFD on a loopback.

### interval

Specifies the transmit interval in milliseconds. The default is 200 ms. The minimum value for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure the remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.



#### Note

For XA1400 Series, the default is 1000 ms.

### min\_rx

Specifies the receive interval in milliseconds. The default is 200 ms. The minimum value for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure the remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.



#### Note

For XA1400 Series, the default is 1000 ms.

### multiplier

Specifies the multiplier used to calculate the amount of time BFD waits before it declares a receive timeout. The default is 3. If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

## Default

The default is disabled.



## Command Mode

Loopback Interface Configuration

## Usage Guidelines

This command is not supported on all hardware platforms. For information about feature support, see [VOSS User Guide](#).

## ip dhcp-relay (for loopback)

---

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command `no ip dhcp-relay` disables DHCP Relay but does not delete the DHCP entry.

## Syntax

- `default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}`
- `default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} disable`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} enable`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode { bootp | bootp_dhcp | dhcp }`
- `no ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}`
- `no ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} enable`

## Command Parameters

`{A.B.C.D} {A.B.C.D}`

The first IP address is the IP address of the dhcp-relay agent, while the second one is the IP address of the server.

`<bootp|dhcp|bootp_dhcp>`

Configures DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

## Default

None

## Command Mode

Loopback Interface Configuration

## ip ipsec enable (for a loopback interface)

---

Enable Internet Protocol Security (IPsec) for IPv4 on a loopback interface.

## Syntax

- `default ip ipsec enable`
- `ip ipsec enable`
- `no ip ipsec enable`

## Default

The default is disabled.

## Command Mode

Loopback Interface Configuration

## ip ipsec policy (for a loopback interface)

---

Link an Internet Protocol Security (IPsec) IPv4 policy to a loopback interface.

## Syntax

- `default ip ipsec policy WORD<1-32>`
- `ip ipsec policy WORD<1-32>`
- `ip ipsec policy WORD<1-32> dir both`
- `ip ipsec policy WORD<1-32> dir in`
- `ip ipsec policy WORD<1-32> dir out`
- `no ip ipsec policy WORD<1-32> dir both`
- `no ip ipsec policy WORD<1-32> dir in`
- `no ip ipsec policy WORD<1-32> dir out`

## Command Parameters

`dir <both|in|out>`

Specifies the direction to which IPsec applies. Both specifies both ingress and egress traffic, in specifies ingress traffic, and out specifies egress traffic. By default, the direction is both.

`WORD<1-32>`

Specifies the IPsec policy name.

## Default

None

## Command Mode

Loopback Interface Configuration

---

## ip ospf (loopback)

---

Enable OSPF for the circuitless IP (CLIP) interface.

### Syntax

- `default ip ospf`
- `default ip ospf <1-256>`
- `default ip ospf vrf WORD<1-16>`
- `ip ospf`
- `ip ospf <1-256>`
- `ip ospf vrf WORD<1-16>`
- `no ip ospf`
- `no ip ospf <1-256>`
- `no ip ospf vrf WORD<1-16>`

### Command Parameters

`<1-256>`

Specifies the interface identification number for the CLIP.

`vrf WORD<1-16>`

Specifies an associated VRF by name.

### Default

The default is disabled.

### Command Mode

Loopback Interface Configuration

---

## ip pim (loopback)

---

Enable PIM for the circuitless IP (CLIP) interface.

### Syntax

- `default ip pim`
- `default ip pim <1-256>`
- `default ip pim <1-256> bsr-candidate vrf WORD<1-16>`
- `default ip pim bsr-candidate`
- `default ip pim bsr-candidate vrf WORD<1-16>`
- `default ip pim vrf WORD<1-16>`

- **ip pim**
- **ip pim <1-256>**
- **ip pim <1-256> bsr-candidate preference <0-255> vrf WORD<1-16>**
- **ip pim bsr-candidate preference <0-255>**
- **ip pim bsr-candidate preference <0-255> vrf WORD<1-16>**
- **ip pim vrf WORD<1-16>**
- **no ip pim**
- **no ip pim <1-256>**
- **no ip pim <1-256> bsr-candidate vrf WORD<1-16>**
- **no ip pim bsr-candidate**
- **no ip pim bsr-candidate vrf WORD<1-16>**
- **no ip pim vrf WORD<1-16>**

## Command Parameters

**<0-255>**

Specifies the preference value.

**<1-256>**

Specifies the interface ID.

**bsr-candidate preference <0-255>**

Enables the CLIP interface as a candidate bootstrap router and configure a preference value. The C-BSR with the highest BSR preference and address is the preferred Bootstrap Router (BSR).

**vrf WORD<1-16>**

Specifies the VRF name.

## Default

The default is -1, which indicates that the current interface is not a C-BSR.

## Command Mode

Loopback Interface Configuration

## ipv6 interface address (loopback)

---

Create an IPv6 loopback interface address.

## Syntax

- **ipv6 interface address WORD<0-255>**
- **no ipv6 interface address WORD<0-255>**

## Command Parameters

WORD<0-255>

Assigns an IPv6 address to the Loopback Interface.

## Default

None

## Command Mode

Loopback Interface Configuration

---

## ipv6 ipsec enable (for a loopback interface)

Enable Internet Protocol Security (IPsec) for IPv6 on a loopback interface.

## Syntax

- **default ipv6 ipsec enable**
- **ipv6 ipsec enable**
- **no ipv6 ipsec enable**

## Default

The default is disabled.

## Command Mode

Loopback Interface Configuration

---

## ipv6 ipsec policy (for a loopback interface)

Link an Internet Protocol Security (IPsec) IPv6 policy to a loopback interface.

## Syntax

- **default ipv6 ipsec policy WORD<1-32>**
- **ipv6 ipsec policy WORD<1-32>**
- **ipv6 ipsec policy WORD<1-32> dir both**
- **ipv6 ipsec policy WORD<1-32> dir in**
- **ipv6 ipsec policy WORD<1-32> dir out**
- **no ipv6 ipsec policy WORD<1-32> dir both**
- **no ipv6 ipsec policy WORD<1-32> dir in**
- **no ipv6 ipsec policy WORD<1-32> dir out**

## Command Parameters

**dir <both|in|out>**

Specifies the direction to which IPsec applies. Both specifies both ingress and egress traffic, in specifies ingress traffic, and out specifies egress traffic. By default, the direction is both.

**WORD<1-32>**

Specifies the IPsec policy name.

## Default

None

## Command Mode

Loopback Interface Configuration

## ipv6 ospf

---

Creates an Open Shortest Path First Version 3 (OSPFv3) instance on a loopback interface for a specific area from the associated Virtual Router Forwarding (VRF) list and enables the OSPFv3 circuitless IP (CLIP) instance.

## Syntax

- **ipv6 ospf <1-256> area {A.B.C.D}**
- **ipv6 ospf <1-256> enable**
- **no ipv6 ospf <1-256>**
- **no ipv6 ospf <1-256> enable**

## Command Parameters

**<1-256>**

Specifies the interface identification for the CLIP.

**area {A.B.C.D}**

Specifies the OSPFv3 identification number for the area, typically formatted as an IP address.

**enable**

Enables the OSPFv3 CLIP instance.

## Default

The default is none.

## Command Mode

Loopback Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis enable

---

Create an IS-IS circuit and interface on the selected logical interface.

### Syntax

- **default isis enable**
- **isis**
- **isis enable**
- **no isis**
- **no isis enable**

### Default

None

### Command Mode

Logical Interface Configuration

## migrate-to-mgmt (for a loopback interface)

---

Before upgrading to VOSS Release 8.1.60 or later, you can use this command to designate an existing loopback interface for use as a Segmented Management Instance. Save the configuration. During the upgrade this migration configuration moves the selected interface from the VOSS routing stack to the management stack for use with management applications.

After upgrading to VOSS Release 8.1.60 or later, you can use this command to move an existing Segmented Management Instance CLIP interface to a different VRF. Save the configuration. During a reboot the migration configuration moves the selected interface to the management stack for use with management applications.



#### Note

Do not migrate an interface used for routing purposes, such as where you configured Layer 3 routing protocols. The selected interface routing configuration is reset during a migration.

### Syntax

- **migrate-to-mgmt**
- **no migrate-to-mgmt**

## Default

None

## Command Mode

Loopback Interface Configuration





# Management Instance Configuration

---

The following topics document commands available in Management Instance Configuration mode of the command line interface (CLI).

## convert (for a Management CLIP)

---

Converts existing configuration for Management Instance CLIP attributes.

### Syntax

- **convert ip** <A.B.C.D A.B.C.D | A.B.C.D/X> [**rollback** <0-3600>]
- **convert vrf** WORD <0-16> [**rollback** <0-3600>]

### Command Parameters

<A.B.C.D A.B.C.D | A.B.C.D/X>

Specifies the IP address and subnet mask.

<0-3600>

Specifies the time in seconds between when the command is issued and when the command changes will be undone. The default is 120 seconds. To disable the rollback, enter 0.

WORD<0-16>

Specifies the vrf name.

### Default

None

### Command Mode

Management Instance Configuration

### Usage Guidelines

This command is not supported on VSP 8600 Series.

---

## convert (for a Management OOB)

---

Converts existing configuration for Management Instance OOB attributes.

### Syntax

- **convert ip** <A.B.C.D A.B.C.D | A.B.C.D/X> [rollback <0-3600>]
- **convert gateway** <A.B.C.D> [rollback <0-3600>]

### Command Parameters

<A.B.C.D A.B.C.D | A.B.C.D/X>

Specifies the IP address and subnet mask.

<0-3600>

Specifies the time in seconds between when the command is issued and when the command changes will be undone. The default is 120 seconds. To disable the rollback, enter 0.

<A.B.C.D>

Specifies the gateway IP address.

### Default

None

### Command Mode

Management Instance Configuration

### Usage Guidelines

This command is not supported on VSP 8600 Series.

---

## convert (for a Management VLAN)

---

Converts existing configuration for Management Instance VLAN attributes.

### Syntax

- **convert vlan** <2-4059> [rollback <0-3600>]
- **convert ip** <A.B.C.D A.B.C.D | A.B.C.D/X> [rollback <0-3600>]
- **convert gateway** <A.B.C.D> [rollback <0-3600>]
- **convert i-sid** <1-16777215> [rollback <0-3600>]

- **convert vlan <2-4059> [ports-tagged {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] [rollback <0-3600>]**
- **convert vlan <2-4059> [ports-untagged {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] [rollback <0-3600>]**

## Command Parameters

**<2-4059>**

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

**<A.B.C.D A.B.C.D | A.B.C.D/X>**

Specifies the IP address and subnet mask.

**<A.B.C.D>**

Specifies the gateway IP address.

**<1-16777215>**

Specifies the service instance identifier (I-SID).

**<0-3600>**

Specifies the time in seconds between when the command is issued and when the command changes will be undone. The default is 120 seconds. To disable the rollback, enter 0.

**{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Management Instance Configuration

## Usage Guidelines

This command is not supported on VSP 8600 Series.

## enable (for a Management Instance)

Enables a Segmented Management Instance.

## Syntax

- **default enable**
- **enable**
- **no enable**

## Default

The default is disabled.

## Command Mode

Management Instance Configuration

---

## ip address (for a Management Instance)

Adds an IPv4 address to a Segmented Management Instance.

## Syntax

- **ip address {A.B.C.D/X}**
- **ip address {A.B.C.D} {A.B.C.D}**
- **no ip address**

## Command Parameters

{A.B.C.D/X}

Specifies the address and mask.

{A.B.C.D} {A.B.C.D}

Specifies the address and mask.

## Default

None

## Command Mode

Management Instance Configuration

---

## ip route (for a Management Instance)

Configures an IPv4 static route for a Management Instance.

## Syntax

- **default ip route** {A.B.C.D/X | <A.B.C.D> <A.B.C.D>} **next-hop** {A.B.C.D} [weight]
- **ip route** {A.B.C.D/X | <A.B.C.D> <A.B.C.D>} **next-hop** {A.B.C.D} [weight <1-65535>]
- **no ip route** {A.B.C.D/X | <A.B.C.D> <A.B.C.D>} **next-hop** {A.B.C.D} [weight]

## Command Parameters

**{A.B.C.D/X}**

Specifies the address and mask.

**{A.B.C.D} {A.B.C.D}**

Specifies the address and mask.

**next-hop {A.B.C.D}**

Specifies the next hop address for the static route. Use an IP in the same subnet as the management VLAN IP address.

**weight <1-65535>**

Specifies the static route cost. The default is 200.

## Default

None

## Command Mode

Management Instance Configuration

## Usage Guidelines

For the Management Instance CLIP, you do not need to configure a default or static route. This interface type uses all routing information learned by protocols attached to the VRF. For more information about how to associate a VRF with the CLIP interface, see [mgmt clip](#) on page 496.

For the Management Instance OOB and VLAN, you must configure a default or static route to reach the next-hop gateway; no routing protocol information is used to access off-link networks.

## ipv6 address (for a Management Instance)

---

Adds an IPv6 address to a Segmented Management Instance.

## Syntax

- **ipv6 address** WORD<0-255>
- **no ipv6 address**

## Command Parameters

**WORD<0-255>**

Specifies the address and prefix length.

## Default

None

## Command Mode

Management Instance Configuration

---

## ipv6 route (for a Management Instance)

Configures an IPv6 static route for a Management Instance.

## Syntax

- **default ipv6 route WORD<0-255> next-hop WORD<0-255> [weight]**
- **ipv6 route WORD<0-255> [next-hop WORD<0-255>] [weight <1-65535>]**
- **no ipv6 route WORD<0-255> next-hop WORD<0-255> [weight]**

## Command Parameters

**next-hop WORD<0-255>**

Specifies the next hop address for the static route. Use an IP in the same subnet as the management VLAN IP address.

**weight <1-65535>**

Specifies the static route cost. The default is 200.

**WORD<0-255>**

Specifies the address and prefix length.

## Default

None

## Command Mode

Management Instance Configuration

## Usage Guidelines

For the Management Instance CLIP, you do not need to configure a default or static route. This interface type uses all routing information learned by protocols attached to the VRF. For more information about how to associate a VRF with the CLIP interface, see [mgmt clip](#) on page 496.

For the Management Instance OOB and VLAN, you must configure a default or static route to reach the next-hop gateway; no routing protocol information is used to access off-link networks.

## force-topology-ip (for a Management Instance)

---

Specifies the default topology IP address for a Segmented Management Instance.

### Syntax

- **default force-topology-ip**
- **force-topology-ip**
- **no force-topology-ip**

### Default

None

### Command Mode

Management Instance Configuration

### Usage Guidelines

This command is not supported on VSP 8600 Series.

## mac-offset (for a Management VLAN Instance)

---

Specifies the MAC-offset for a Management VLAN instance.

### Syntax

- **mgmt vlan mac-offset <mac-offset>**

### Command Parameters

**mac-offset** *<MAC-offset>*

Specifies a number by which to offset the MAC address from the chassis MAC address. This ensures that each IP address has a different MAC address. If you omit this variable, a unique MAC offset is automatically generated. Different hardware platforms support different ranges. To see which range is available on the switch, use the CLI command completion Help.

### Default

None

## Command Mode

Global Configuration

## Usage Guidelines

The commands are not supported on VSP 8600 Series. For more information about feature support, see [VOSS Feature Support Matrix](#).

## **propagate-to-routing (for a Management VLAN Instance)**

---

Propagates the management VLAN IP address and static routes from the management VLAN interface to the VOSS routing stack.

## Syntax

- **propagate-to-routing [vrf WORD<0-16>]**

## Command Parameters

**vrf WORD<0-16>**

Specifies the VRF name.

## Default

The default is none.

## Command Mode

Management Instance Configuration

## Usage Guidelines

This command only applies to XA1400 Series.

## **rmon**

---

Enables RMON for a Segmented Management Instance.

## Syntax

- **default rmon**
- **no rmon**
- **rmon**



## Default

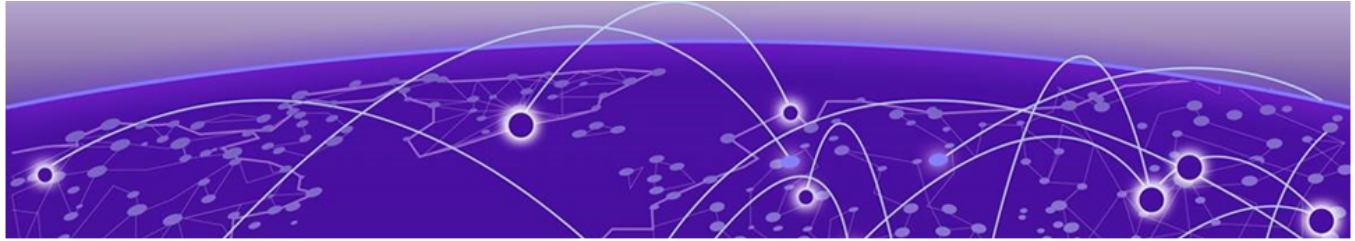
The default is disabled.

## Command Mode

Management Instance Configuration

## Usage Guidelines

This command is not supported on VSP 8600 Series.



# mgmtEthernet Interface Configuration

---

The following topics document commands available in mgmtEthernet Interface Configuration mode of the command line interface (CLI).

## auto-negotiate (for the management port)

---

Configure auto-negotiation for the Ethernet management port.



### Note

This command does not apply to all hardware platforms.

## Syntax

- **auto-negotiate enable**
- **default auto-negotiate enable**
- **no auto-negotiate enable**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default varies depending on the platform:

- 5420 Series- enabled
- 5520 Series - enabled
- VSP 4900 Series - enabled
- VSP 7200 Series - disabled
- VSP 7400 Series - enabled
- VSP 8200 Series - enabled
- VSP 8400 Series - enabled
- VSP 8600 Series - enabled

## Command Mode

mgmtEthernet Interface Configuration

### duplex (for the management port)

---

Configure the duplex mode for the Ethernet management port.



#### Note

This command does not apply to all hardware platforms.

## Syntax

- **default duplex** [**port** {**slot/port**[/**sub-port**] [**-slot/port**[/**sub-port**]] [,...]]
- **duplex** [**port** {**slot/port**[/**sub-port**] [**-slot/port**[/**sub-port**]] [,...]] <**half|full**>

## Command Parameters

<**half|full**>

Specifies half- or full-duplex mode. 1 and 10 Gb/s ports must use full-duplex mode.

**port** {*slot/port*[/*sub-port*] [*-slot/port*[/*sub-port*]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

The default is half-duplex mode.

## Command Mode

mgmtEthernet Interface Configuration

### ip address (for the management port)

---

Configure the IP address for the Ethernet management port.



#### Note

This command does not apply to all hardware platforms.

## Syntax

- **ip address {A.B.C.D A.B.C.D|A.B.C.D/X}**
- **ip address port {slot/port} {A.B.C.D/X}**
- **ip address port {slot/port} {A.B.C.D} {A.B.C.D}**
- **no ip address {A.B.C.D}**

## Command Parameters

{A.B.C.D A.B.C.D|A.B.C.D/X}

Assigns an IP address and mask for the management port.



### Important

You cannot assign an address of 0.0.0.0/0. You can specify the mask in either dotted decimal notation or as a decimal number.

## Default

None

## Command Mode

mgmtEthernet Interface Configuration

## ip ipsec enable (for a management interface)

---

Enable Internet Protocol Security (IPsec) for IPv4 on a management interface.

## Syntax

- **default ip ipsec enable**
- **ip ipsec enable**
- **no ip ipsec enable**

## Default

The default is disabled.

## Command Mode

mgmtEthernet Interface Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## ip ipsec policy (for a management interface)

---

Link an Internet Protocol Security (IPsec) IPv4 policy to a management interface.

### Syntax

- `default ip ipsec policy WORD<1-32>`
- `ip ipsec policy WORD<1-32>`
- `ip ipsec policy WORD<1-32> dir both`
- `ip ipsec policy WORD<1-32> dir in`
- `ip ipsec policy WORD<1-32> dir out`
- `no ip ipsec policy WORD<1-32> dir both`
- `no ip ipsec policy WORD<1-32> dir in`
- `no ip ipsec policy WORD<1-32> dir out`

### Command Parameters

`dir <both|in|out>`

Specifies the direction to which IPsec applies. Both specifies both ingress and egress traffic, in specifies ingress traffic, and out specifies egress traffic. By default, the direction is both.

`WORD<1-32>`

Specifies the IPsec policy name.

### Default

None

### Command Mode

mgmtEthernet Interface Configuration

### Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## ipv6 interface address (for the management port)

---

Configure the IPv6 address for the Ethernet management port.



#### Note

This command does not apply to all hardware platforms.

## Syntax

- **ipv6 interface address WORD<0-255> eui <1-3>**
- **no ipv6 interface address WORD<0-255>**

## Command Parameters

WORD<0-255> eui <1-3>

Assigns an IPv6 address, prefix length, and extended unique identifier to the to the management port.

## Default

None

## Command Mode

mgmtEthernet Interface Configuration

## ipv6 interface enable (for the management port)

---

Enable IPv6 route advertisement on the Ethernet management port.



### Note

This command does not apply to all hardware platforms.

## Syntax

- **default ipv6 interface enable**
- **ipv6 interface enable**
- **no ipv6 interface enable**

## Default

The default is disabled.

## Command Mode

mgmtEthernet Interface Configuration

## ipv6 interface hop-limit (for the management port)

---

Configure the maximum number of hops before packets drop.



### Note

This command does not apply to all hardware platforms.

## Syntax

- **default ipv6 interface hop-limit**
- **ipv6 interface hop-limit <1-255>**

## Command Parameters

<1-255>

Configures the maximum hops.

## Default

The default is 30 hops.

## Command Mode

mgmtEthernet Interface Configuration

## ipv6 interface link-local (for the management port)

---

Create a link-local address for the Ethernet management port.



### Note

This command does not apply to all hardware platforms.

## Syntax

- **ipv6 interface link-local WORD<0-19>**

## Command Parameters

WORD<0-19>

Specifies the link-local address for the management port.

## Default

None

## Command Mode

mgmtEthernet Interface Configuration

---

## ipv6 interface mtu (for the management port)

---

Configure the maximum transmission unit for the Ethernet management port.



### Note

This command does not apply to all hardware platforms.

### Syntax

- **default ipv6 interface mtu**
- **ipv6 interface mtu <1280-1500>**

### Command Parameters

<1280-1500>

Configures the maximum transmission unit for the interface.

### Default

The default is 1500.

### Command Mode

mgmtEthernet Interface Configuration

---

## ipv6 interface name (for the management port)

---

Configure an interface description for the Ethernet management port.



### Note

This command does not apply to all hardware platforms.

### Syntax

- **ipv6 interface name WORD<0-255>**

### Command Parameters

WORD<0-255>

Assigns a descriptive name to the management port.

### Default

None



## Command Mode

mgmtEthernet Interface Configuration

### ipv6 interface process-redirect (for the management port)

---

Configure process-redirect messages to honor or ignore redirect messages for the management port. Redirect messages are visible only when Stateless Address Autoconfiguration is configured on switches capable of routing IPv6 traffic.

#### Syntax

- **ipv6 interface process-redirect**

#### Default

None

## Command Mode

mgmtEthernet Interface Configuration

### ipv6 interface reachable-time (for the management port)

---

Configure the time a neighbor is considered reachable after receiving a reachability confirmation.



#### Note

This command does not apply to all hardware platforms.

#### Syntax

- **default ipv6 interface reachable-time**
- **ipv6 interface reachable-time <0-3600000>**

#### Command Parameters

<0-3600000>

Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.

#### Default

The default is 30000.

## Command Mode

mgmtEthernet Interface Configuration

---

## ipv6 interface retransmit-timer (for the management port)

---

Configure the time, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.



### Note

This command does not apply to all hardware platforms.

### Syntax

- **default ipv6 interface retransmit-timer**
- **ipv6 interface retransmit-timer <0-3600000>**

### Command Parameters

<0-3600000>

Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

### Default

The default is 1000.

### Command Mode

mgmtEthernet Interface Configuration

---

## ipv6 ipsec enable (for a management interface)

---

Enable Internet Protocol Security (IPsec) for IPv6 on a management interface.

### Syntax

- **default ipv6 ipsec enable**
- **ipv6 ipsec enable**
- **no ipv6 ipsec enable**

### Default

The default is disabled.

### Command Mode

mgmtEthernet Interface Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## ipv6 ipsec policy (for a management interface)

Link an Internet Protocol Security (IPsec) IPv6 policy to a management interface.

## Syntax

- **default ipv6 ipsec policy WORD<1-32>**
- **ipv6 ipsec policy WORD<1-32>**
- **ipv6 ipsec policy WORD<1-32> dir both**
- **ipv6 ipsec policy WORD<1-32> dir in**
- **ipv6 ipsec policy WORD<1-32> dir out**
- **no ipv6 ipsec policy WORD<1-32> dir both**
- **no ipv6 ipsec policy WORD<1-32> dir in**
- **no ipv6 ipsec policy WORD<1-32> dir out**

## Command Parameters

**dir <both|in|out>**

Specifies the direction to which IPsec applies.

- Both specifies both ingress and egress traffic
- in specifies ingress traffic
- out specifies egress traffic

By default, the direction is both.

**WORD<1-32>**

Specifies the IPsec policy name.

## Default

None

## Command Mode

mgmtEthernet Interface Configuration

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

---

## ipv6 nd dad-ns (for the management port)

---

Configure the number of neighbor solicitation messages from duplicate address detection.



### Note

This command does not apply to all hardware platforms.

### Syntax

- **default ipv6 nd dad-ns**
- **ipv6 nd dad-ns <0-600>**

### Command Parameters

<0-600>

Configures the number of neighbor solicitation messages from duplicate address detection.

- A value of 0 disables duplicate address detection on the specified interface
- A value of 1 configures a single transmission without follow-up transmissions

### Default

The default is 1.

### Command Mode

mgmtEthernet Interface Configuration

---

## shutdown (for the management port)

---

Disable the Ethernet management port.



### Note

This command does not apply to all hardware platforms.

### Syntax

- **default shutdown**
- **no shutdown**
- **shutdown**

### Default

The default is enabled.

## Command Mode

mgmtEthernet Interface Configuration

## speed (for the management port)

---

Configure the speed for the Ethernet management (mgmt) port.



### Note

This command does not apply to all hardware platforms.

## Syntax

- **default speed**
- **speed <10|100>**

## Command Parameters

<10|100>

Configures the connection speed for ports to 10 or 100 Mb/s.

## Default

None

## Command Mode

mgmtEthernet Interface Configuration



# MKA Profile Configuration

---

The following topics document commands available in MKA Profile Configuration mode of the command line interface (CLI).

## confidentiality-offset

---

Configure the confidentiality offset to specify the number of unencrypted bytes that precede MACsec encryption. Valid values are 30 and 50. Configuring the offset to 30 enables an IPv4 header and TCP/UDP header to remain unencrypted, while configuring the offset to 50 enables an IPv6 header and TCP/UDP header to remain unencrypted.

### Syntax

- **confidentiality-offset <30 | 50>**
- **default confidentiality-offset**
- **no confidentiality-offset**

### Command Parameters

<30 | 50>

Specifies the bytes after the Ethernet header from which data encryption begins.

### Default

The default is no confidentiality offset.

### Command Mode

MKA Profile Configuration mode

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## include-sci

---

Configure SCI tagging for a MACsec-enabled switch.

## Syntax

- **include-sci enable**
- **default include-sci enable**
- **no include-sci**

## Default

The default is enabled.

## Command Mode

MKA Profile Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## replay-protect

---

Configure a replay protect window that accepts out of sequence frames.

## Syntax

- **default replay-protect enable**
- **no replay-protect enable**
- **replay-protect enable window-size <5-500>**

## Command Parameters

### enable

Enables replay protect for the specified MKA profile.

### window-size

Specifies the maximum acceptable difference in packet numbers between out of order packets. If a packet number differs from the number of the previously received packet by more than the specified window size, the packet is dropped.

## Default

The default is disabled.

## Command Mode

mka profile

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).





# MLT Interface Configuration

---

The following topics document commands available in MLT Interface Configuration mode of the command line interface (CLI).

## default svlan-porttype

---

Set svlan port type to default.

### Syntax

- **default svlan-porttype**

### Default

None

### Command Mode

MLT Interface Configuration

## end-point tracking (for an MLT/SMLT)

---

Create and enable Endpoint Tracking on and MLT and SMLT interfaces. Creating and enabling Endpoint Tracking on interfaces can be accomplished using a one-step or two-step process; you can create and enable at the same time, or create but leave disabled, and then enable at a later time.

Use the no operator with **endpoint-tracking** to delete, and the no operator with **endpoint-tracking enable** to disable.

### Syntax

- **endpoint-tracking**
- **endpoint-tracking enable**
- **no endpoint-tracking**
- **no endpoint-tracking enable**

### Command Parameters

enable

Creates and enables Endpoint Tracking, or enables Endpoint Tracking previously created on an MLT or SMLT.

## Default

Disabled

## Command Mode

MLT Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## fa authentication-key (for an MLT)

Configure the Fabric Attach authentication key.

## Syntax

- **default fa authentication-key**
- **fa authentication-key WORD<0-32>**

## Command Parameters

WORD<0-32>

Configures the authentication key on the MLT.

## Default

None

## Command Mode

MLT Interface Configuration

---

## fa enable (for an MLT)

Enable Fabric Attach on an MLT.

## Syntax

- **fa enable**
- **no fa enable**

## Default

None

## Command Mode

MLT Interface Configuration

## fa management (for an MLT)

---

Configure Fabric Attach management on an MLT.

## Syntax

- **default fa management i-sid**
- **fa management i-sid <1-16777215> <c-vid>**
- **no fa management i-sid**

## Command Parameters

*<c-vid>*

Specifies the customer VLAN ID. Different hardware platforms support different customer VLAN ID ranges. Use the CLI Help to see the available range for the switch.

**i-sid <1-16777215>**

Specifies the management I-SID.

## Default

None

## Command Mode

MLT Interface Configuration

## fa message-authentication (for an MLT)

---

Configure Fabric Attach message authentication on an MLT.

## Syntax

- **default no fa message-authentication**
- **fa message-authentication**
- **no fa message-authentication**

## Default

None

## Command Mode

MLT Interface Configuration

## flex-uni (for an MLT)

---

Configure Switched UNI on an MLT.

## Syntax

- **flex-uni enable**
- **default flex-uni enable**
- **no flex-uni enable**

## Command Parameters

**enable**

Enables Switched UNI on an MLT.

## Default

The default is disabled.

## Command Mode

MLT Interface Configuration

## ip dhcp-relay (for an MLT)

---

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command `no ip dhcp-relay` disables DHCP Relay but does not delete the DHCP entry.

## Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}**
- **default ip dhcp-relay broadcast**
- **default ip dhcp-relay circuitId**
- **default ip dhcp-relay fwd-path {A.B.C.D}**
- **default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode**
- **default ip dhcp-relay fwd-path {A.B.C.D} mode**
- **default ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>**
- **default ip dhcp-relay max-hop**

- `default ip dhcp-relay min-sec`
- `default ip dhcp-relay mode`
- `default ip dhcp-relay remoteId`
- `default ip dhcp-relay trusted`
- `ip dhcp-relay broadcast`
- `ip dhcp-relay circuitId`
- `ip dhcp-relay fwd-path {A.B.C.D}`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} disable`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} enable`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode { bootp | bootp_dhcp | dhcp }`
- `ip dhcp-relay fwd-path {A.B.C.D} disable`
- `ip dhcp-relay fwd-path {A.B.C.D} enable`
- `ip dhcp-relay fwd-path {A.B.C.D} mode bootp`
- `ip dhcp-relay fwd-path {A.B.C.D} mode bootp_dhcp`
- `ip dhcp-relay fwd-path {A.B.C.D} mode dhcp`
- `ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `ip dhcp-relay max-hop <1-16>`
- `ip dhcp-relay min-sec <0-65535>`
- `ip dhcp-relay mode { bootp | dhcp | bootp_dhcp }`
- `ip dhcp-relay remoteId`
- `ip dhcp-relay trusted`
- `no ip dhcp-relay`
- `no ip dhcp-relay broadcast`
- `no ip dhcp-relay circuitId`
- `no ip dhcp-relay fwd-path {A.B.C.D}`
- `no ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}`
- `no ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} enable`
- `no ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `no ip dhcp-relay remoteId`
- `no ip dhcp-relay trusted`

## Command Parameters

{A.B.C.D}

Creates a forwarding path to the DHCP server with a mode and a state. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface.

**Tip**

If the relay is a Virtual Router configured on this interface, you must set the vrid.

**{A.B.C.D} {A.B.C.D}**

The first IP address is the IP address of the dhcp-relay agent, while the second one is the IP address of the server.

**<bootp|dhcp|bootp\_dhcp>**

Configures DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

**broadcast**

Enables the device to send the server reply as a broadcast to the end station. After you disable this variable, the device sends the server reply as a unicast to the end station.

**circuitId**

Enables the device to insert the Option 82 Circuit ID into the packets sent to the server (enables DHCP Option 82).

**max-hop <1-16>**

Configures the maximum number of hops before a BootP/DHCP packet is discarded (1-16). The default is 4.

**min-sec <0-65535>**

Configures the minimum seconds count for DHCP. If the secs field in the BootP/DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped (0- 65535). The default is 0 seconds.

**mode <bootp|dhcp|bootp\_dhcp>**

Configures DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

**remotId**

Enables the device to insert the Option 82 Remote ID into the packets sent to the server (enables DHCP Option 82).

**trusted**

Configures the circuit as trusted in an Option 82 context.

## Default

None

## Command Mode

MLT Interface Configuration

---

## ip dhcp-snooping (for MLT)

---

Sets the trust factor associated with an MLT for DHCP Snooping feature.

### Syntax

- **default ip dhcp-snooping**
- **ip dhcp-snooping <trusted|untrusted>**
- **no ip dhcp-snooping**

### Command Parameters

#### trusted

Sets the trust factor as trusted on the MLT for DHCP Snooping.

#### untrusted

Sets the trust factor as untrusted on the MLT for DHCP Snooping.

### Default

The default is untrusted.

### Command Mode

MLT Interface Configuration

---

## i-sid (for an mlt)

---

Create Switched UNI (S-UNI) service instance identifiers (I-SID).

### Syntax

- **i-sid <1-16777215> elan**

### Command Parameters

#### <1-16777215>

Specifies the service instance identifiers (I-SID) number.

#### elan

Create an Elan based service.

### Default

None

## Command Mode

MLT Interface Configuration

## isis (on an MLT)

---

Create an Intermediate-System-to-Intermediate-System (IS-IS) circuit and interface on the selected MultiLink Trunking (MLT) instance.

### Syntax

- **default isis enable**
- **isis**
- **isis enable**
- **no isis**
- **no isis enable**

### Command Parameters

**enable**

Enables the Intermediate-System-to-Intermediate-System (IS-IS) circuit and interface on the selected MLT.

### Default

None

## Command Mode

MLT Interface Configuration

## isis hello-auth (on an MLT)

---

Configure the authentication type used for Intermediate-System-to-Intermediate-System (IS-IS) hello packets on the interface.

### Syntax

- **default isis hello-auth**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 }**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 } key WORD<1-16>**
- **isis hello-auth type { none | simple | hmac-md5 | hmac-sha-256 } key WORD<1-16> key-id <1-255>**
- **no isis hello-auth**



## Command Parameters

**key WORD<1-16>**

Specifies the authentication key (password) used by the receiving router to verify the packet.

**key-id <1-255>**

Specifies the optional key ID.

**type { none | simple | hmac-md5 | hmac-sha-256 }**

Specifies the authentication type used for IS-IS hello packets on the interface. The type can be one of the following: none, simple, hmac-md5, or hmac-sha-256.

- If simple is selected, you can also specify a key value. Simple password authentication uses a text password in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet.
- If hmac-md5 is selected, you can also specify a key value and key-id. MD5 authentication creates an encoded checksum in the transmitted packet. The receiving router uses an authentication key (password) to verify the MD5 checksum of the packet.
- If hmac-sha-256 is selected, you can also specify a key value and key-id. With SHA-256 authentication, the switch adds an HMAC-SHA256 digest to each Hello packet. The switch that receives the Hello packet computes the digest of the packet and compares it with the received digest. If the digests match, the packet is accepted. If the digests do not match, the receiving switch discards the packet.

The default type is none. Use the no or default options to set the hello-auth type to none.

## Default

The default is no authentication type (none).

## Command Mode

MLT Interface Configuration

## isis l1-dr-priority (on an MLT)

---

Configure the Level 1 Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

## Syntax

- **isis l1-dr-priority <0-127>**
- **no isis l1-dr-priority**

## Command Parameters

**<0-127>**

Configures the Level 1 Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

## Default

The default Level 1 designated router priority value is 64.

## Command Mode

MLT Interface Configuration

---

## isis l1-hello-interval (on an MLT)

Configure the hello interval to change how often hello packets are sent out from an interface level.

## Syntax

- **isis l1-hello-interval <1-600>**
- **no isis l1-hello-interval**

## Command Parameters

<1-600>

Configures the Level 1 hello interval.

## Default

The default Level 1 hello interval value is 9 seconds.

## Command Mode

MLT Interface Configuration

---

## isis l1-hello-multiplier (on an MLT)

Configure the hello multiplier to specify how many hellos the switch must miss before it considers the adjacency with a neighboring switch down.

## Syntax

- **isis l1-hello-multiplier <1-600>**
- **no isis l1-hello-multiplier**

## Command Parameters

<1-600>

Configures the Level 1 hello multiplier.

## Default

The default Level 1 hello-multiplier value is 3 seconds.

## Command Mode

MLT Interface Configuration

## isis spbm (on an MLT)

---

Configure Shortest Path Bridging MAC (SPBM) on an Intermediate-System-to-Intermediate-System (IS-IS) interface on a MultiLink Trunking (MLT) instance.

## Syntax

- **default isis spbm <1-100> interface-type**
- **default isis spbm <1-100> ll-metric**
- **isis spbm <1-100>**
- **isis spbm <1-100> interface-type { broadcast | pt-pt }**
- **isis spbm <1-100> ll-metric <1-16777215>**
- **no isis spbm <1-100>**
- **no isis spbm <1-100> interface-type**
- **no isis spbm <1-100> ll-metric**

## Command Parameters

**<1-100>**

Specifies the Shortest Path Bridging MAC (SPBM) instance ID.

**interface-type { broadcast | pt-pt }**

Configures the Shortest Path Bridging MAC (SPBM) instance interface type.

**ll-metric <1-16777215>**

Configures the cost for the Shortest Path Bridging MAC (SPBM) instance.

## Default

None

## Command Mode

MLT Interface Configuration

## lacp (on an MLT)

---

Configure a MultiLink Trunking (MLT) with Link Aggregation Control Protocol (LACP) to use the dynamic link aggregation function.

## Syntax

- **default lacp**
- **default lacp key**
- **default lacp system-priority**
- **lacp enable**
- **lacp enable key <0-512> system-priority <0-65535>**
- **lacp key <0-512>**
- **lacp system-priority <0-65535>**
- **no lacp**
- **no lacp enable**

## Command Parameters

### enable

Enables Link Aggregation Control Protocol (LACP) on the MLT interface. The default is disabled.

### key <0-512>

Sets the Link Aggregation Control Protocol (LACP) aggregator key for a specific MLT. <0-512> specifies the Link Aggregation Control Protocol (LACP) actor admin key. The default key value is 0

### system-priority <0-65535>

Sets the Link Aggregation Control Protocol (LACP) system priority for a specific MLT. <0-65535> specifies the system priority. The default system-priority is 32768.

## Default

None

## Command Mode

MLT Interface Configuration

## mef-uni enable (for an mlt)

---

Enable mef-union port (s).

## Syntax

- **default mef-uni enable**
- **mef-uni enable**
- **no mef-uni enable**

## Default

The default is enabled.

## Command Mode

MLT Interface Configuration

## virtual-ist (on an MLT)

---

Virtual interswitch trunk (VIST) improves upon the Layer 2 and Layer 3 resiliency by using a virtualized IST channel through the SPBM cloud.

## Syntax

- **virtual-ist enable**

## Command Parameters

**enable**

Enables vIST on the specified MLT ID.

## Default

None

## Command Mode

MLT Interface Configuration



# OSPF Router Configuration

---

The following topics document commands available in OSPF Router Configuration mode of the command line interface (CLI).

## accept adv-rtr (for OSPF)

---

Use a route policy to define how the switch Redistribute external routes from a specified source into an OSPF domain. The policy defines which route types the switch accepts and Redistribute.

### Syntax

- `accept adv-rtr {A.B.C.D}`
- `accept adv-rtr {A.B.C.D} enable`
- `accept adv-rtr {A.B.C.D} metric-type { type1 | type2 | any }`
- `accept adv-rtr {A.B.C.D} route-map WORD<0-64>`
- `default accept adv-rtr {A.B.C.D}`
- `default accept adv-rtr {A.B.C.D} enable`
- `default accept adv-rtr {A.B.C.D} metric-type`
- `default accept adv-rtr {A.B.C.D} route-map`
- `no accept adv-rtr {A.B.C.D}`
- `no accept adv-rtr {A.B.C.D} enable`

### Command Parameters

**{A.B.C.D}**

Specifies the IP address.

**enable**

Enables an OSPF accept entry for a specified advertising router.

**metric-type <type1|type2|any>**

Indicates the OSPF external type. This parameter describes which types of OSPF external routes match this entry. any means match all external routes. type1 means match external type 1 only. type2 means match external type 2 only.

**route-map WORD<0-64>**

Specifies the name of the route policy to use for filtering external routes advertised by the specified advertising router before accepting into the routing table.

## Default

None

## Command Mode

OSPF Router Configuration

## area

---

Import information from other areas to learn their OSPF relationships and create normal, stubby, or not-so-stubby areas (NSSA). Place stubby or NSSAs at the edge of an OSPF routing domain.

## Syntax

- **area {A.B.C.D}**
- **area {A.B.C.D} default-cost <0-16777215>**
- **area {A.B.C.D} import external**
- **area {A.B.C.D} import noexternal**
- **area {A.B.C.D} import nssa**
- **area {A.B.C.D} import-summaries enable**
- **area {A.B.C.D} stub**
- **default area {A.B.C.D}**
- **default area {A.B.C.D} default-cost**
- **default area {A.B.C.D} import**
- **default area {A.B.C.D} import-summaries enable**
- **default area {A.B.C.D} stub**
- **no area {A.B.C.D}**
- **no area {A.B.C.D} import-summaries enable**

## Command Parameters

### **default-cost <0-16777215>**

Stub area default metric for this stub area, which is the cost from 0 to 16 777 215. This is the metric value applied at the indicated type of service.

### **import <external|noexternal|nssa>**

Specifies the type of area: external - Stub and NSSA (not so stubby area) are both false. noexternal-Configures the area as stub area. nssa - Configures the area as NSSA.

### **import-summaries enable**

Configures the area support to import summary advertisements into a stub area. This parameter must be used only if the area is a stub area.

### **stub**

Configures the import external option for this area as stub. A stub area has only one exit point (router interface) from the area.

## Default

None

## Command Mode

OSPF Router Configuration

## area range

---

Use aggregate area ranges to reduce the number of link-state advertisements that are required within the area. You can also control advertisements.

## Syntax

- **area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-metric <0-65535>**
- **area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-mode { summarize | suppress | no-summarize }**
- **default area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink }**
- **default area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-metric**
- **default area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-mode**
- **no area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink }**

## Command Parameters

**<A.B.C.D> <A.B.C.D/X>**

<A.B.C.D> identifies an OSPF area and <A.B.C.D/X> is the IP address and subnet mask of the range, respectively.

**<summary-link|nssaextlink>**

Specifies the LSA type. If you configure the range as type nssaextlink then you cannot configure the advertise-metric.

**advertise-metric <0-65535>**

Changes the advertised metric cost of the OSPF area range.

**advertise-mode <summarize|suppress|nosummarize**

Changes the advertisement mode of the range.



## Default

None

## Command Mode

OSPF Router Configuration

## area virtual-link

---

Use manual virtual interfaces to provide a backup link for vital OSPF traffic with a minimum of resource use.

## Syntax

- **area virtual-link {A.B.C.D} {A.B.C.D}**
- **area virtual-link {A.B.C.D} {A.B.C.D} authentication-key WORD<0-8>**
- **area virtual-link {A.B.C.D} {A.B.C.D} authentication-type message-digest**
- **area virtual-link {A.B.C.D} {A.B.C.D} authentication-type none**
- **area virtual-link {A.B.C.D} {A.B.C.D} authentication-type sha 1**
- **area virtual-link {A.B.C.D} {A.B.C.D} authentication-type sha 2**
- **area virtual-link {A.B.C.D} {A.B.C.D} authentication-type simple**
- **area virtual-link {A.B.C.D} {A.B.C.D} dead-interval <0-2147483647>**
- **area virtual-link {A.B.C.D} {A.B.C.D} hello-interval <1-65535>**
- **area virtual-link {A.B.C.D} {A.B.C.D} primary-digest-key <1-255>**
- **area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval <0-3600>**
- **area virtual-link {A.B.C.D} {A.B.C.D} transit-delay <0-3600>**
- **area virtual-link digest-key {A.B.C.D} {A.B.C.D} <1-255> key WORD<0-16>**
- **default area virtual-link {A.B.C.D} {A.B.C.D}**
- **default area virtual-link {A.B.C.D} {A.B.C.D} authentication-type**
- **default area virtual-link {A.B.C.D} {A.B.C.D} dead-interval**
- **default area virtual-link {A.B.C.D} {A.B.C.D} hello-interval**
- **default area virtual-link {A.B.C.D} {A.B.C.D} primary-digest-key**
- **default area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval**
- **default area virtual-link {A.B.C.D} {A.B.C.D} transit-delay**
- **default area virtual-link digest-key {A.B.C.D} {A.B.C.D} <1-255>**
- **no area virtual-link {A.B.C.D} {A.B.C.D}**
- **no area virtual-link digest-key {A.B.C.D} {A.B.C.D} <1-255>**

## Command Parameters

**<1-255>**

Specifies the key ID.

**<A.B.C.D> <A.B.C.D>**

Creates a virtual interface area identifier. <A.B.C.D> <A.B.C.D> specify the area ID and the virtual interface ID, respectively.

**authentication-key WORD<0-8>**

Configures the authentication key of up to eight characters.

**authentication-type <none|simple|message-digest|sha 1|sha 2>**

Configures the authentication type for the OSPF area. authentication-type is: none, simple password, MD5 authentication, SHA 1, or SHA 2. If simple, all OSPF updates received by the interface must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key. The default is none.

**dead-interval <0-2147483647>**

Configures the dead interval, in seconds, for the virtual interface, the number of seconds that a router Hello packets are not seen before its neighbors declare the router down. This value must be at least four times the Hello interval value. The default is 60.

**digest-key**

Creates a digest-key.

**hello-interval <1-65535>**

Configures the Hello interval, in seconds, on the virtual interface for the length of time (in seconds) between the Hello packets that the router sends on the interface. The default is 10.

**key WORD<0-16>**

Specifies the digest key range.

**primary-digest-key <1-255>**

Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the message digest key.

**retransmit-interval <0-3600>**

Configures the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions. The range is from 0 to 3600.

**transit-delay <0-3600>**

Configures the transit delay for the virtual interface, the estimated number of seconds required to transmit a link-state update over the interface. The range is from 0 to 3600.

## Default

None

## Command Mode

OSPF Router Configuration

---

## as-boundary-router enable

---

Configure the router as an autonomous system boundary router (ASBR).

### Syntax

- **as-boundary-router enable**
- **default as-boundary-router**
- **default as-boundary-router enable**
- **no as-boundary-router**
- **no as-boundary-router enable**

### Default

The default is disabled.

### Command Mode

OSPF Router Configuration

---

## auto-vlink

---

Use automatic virtual links to provide an automatic, dynamic backup link for vital OSPF traffic. Automatic virtual links require more system resources than manually configured virtual links.

### Syntax

- **auto-vlink**
- **default auto-vlink**
- **no auto-vlink**

### Default

None

### Command Mode

OSPF Router Configuration

---

## bad-lsa-ignore enable

---

Configures the switch to accept bad LSAs, for example, with a hole in the mask. If you use the no operator with this command, the switch ignores bad LSAs.

## Syntax

- `bad-lsa-ignore enable`
- `default bad-lsa-ignore`
- `default bad-lsa-ignore enable`
- `no bad-lsa-ignore`
- `no bad-lsa-ignore enable`

## Default

The default is disabled.

## Command Mode

OSPF Router Configuration

## default-cost

---

Configures the default OSPF metrics.

## Syntax

- `default default-cost`
- `default default-cost ethernet`
- `default default-cost fast-ethernet`
- `default default-cost forty-gig-ethernet`
- `default default-cost gig-ethernet`
- `default default-cost hundred-gig-ethernet`
- `default default-cost ten-gig-ethernet`
- `default default-cost twentyfive-gig-ethernet`
- `default default-cost vlan`
- `default-cost ethernet <1-65535>`
- `default-cost fast-ethernet <1-65535>`
- `default-cost forty-gig-ethernet <1-65535>`
- `default-cost gig-ethernet <1-65535>`
- `default-cost hundred-gig-ethernet <1-65535>`
- `default-cost ten-gig-ethernet <1-65535>`
- `default-cost twentyfive-gig-ethernet <1-65535>`
- `default-cost vlan <1-65535>`

## Command Parameters

`ethernet <1-65535>`

Configures the OSPF default metrics for 10 Mb/s Ethernet. The default is 100.

**fast-ethernet <1-65535>**

Configures the OSPF default metrics for 100 Mb/s (Fast) Ethernet. The default is 10.

**forty-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 40 Gigabit Ethernet. The default is 1.

**gig-ethernet <1-65535>**

Configures the OSPF default metrics for Gigabit Ethernet. The default is 1.

**hundred-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 100 Gigabit Ethernet. The default is 1.

**ten-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 10 Gigabit Ethernet. The default is 1.

**twentyfive-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 25 Gigabit Ethernet. On a channelized 100 Gbps port, the default-cost for each 25 Gbps channel is 1

## Default

None

## Command Mode

OSPF Router Configuration

## helper-mode-disable

---

Disable helper mode.

## Syntax

- **default helper-mode-disable**
- **helper-mode-disable**
- **no helper-mode-disable**

## Default

The default is enabled when OSPF is configured.

## Command Mode

OSPF Router Configuration

## host-route

---

Use host routes when the switch resides in a network that uses routing protocols other than OSPF.

## Syntax

- **default host-route {A.B.C.D}**
- **default host-route {A.B.C.D} metric**
- **host-route {A.B.C.D}**
- **host-route {A.B.C.D} metric <0-65535>**
- **no host-route {A.B.C.D}**

## Command Parameters

**<A.B.C.D>**

Specifies the IP address of the host router in a.b.c.d format.

**metric <0-65535>**

Configures the metric (cost) for the host route.

## Default

None

## Command Mode

OSPF Router Configuration

## ip area virtual-link ipsec

---

Create the Internet Protocol Security (IPsec) policy under the OSPF virtual link.

## Syntax

- **ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec**
- **no ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec**

## Command Parameters

**{A.B.C.D} {A.B.C.D}**

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

## Default

None

## Command Mode

OSPF Router Configuration

---

## ip area virtual-link ipsec action

---

Configure the action of the Internet Protocol Security (IPsec) policy under the OSPF virtual link.

### Syntax

- **default ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec action**
- **ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec action drop**
- **ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec action permit**
- **no ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec action**

### Command Parameters

{A.B.C.D} {A.B.C.D}

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

action <drop|permit>

Specifies the action of the IPsec policy under the OSPF virtual link to permit or drop traffic. The default is permit.

### Default

The default is permit.

### Command Mode

OSPF Router Configuration

---

## ip area virtual-link ipsec direction

---

Configure the direction of the Internet Protocol Security (IPsec) policy under the OSPF virtual link.

### Syntax

- **default ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction**
- **ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction both**
- **ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction in**
- **ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction out**
- **no ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction**

### Command Parameters

{A.B.C.D} {A.B.C.D}

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

<both|in|out>

Specifies the direction of the traffic of the IPsec policy under the OSPF virtual link.

## Default

None

## Command Mode

OSPF Router Configuration

---

## ip area virtual-link ipsec enable

Enable the Internet Protocol Security (IPsec) policy created under the OSPF virtual link.

## Syntax

- **default ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec enable**
- **ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec enable**
- **no ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec enable**

## Command Parameters

{A.B.C.D} {A.B.C.D}

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

## Default

The default is disabled.

## Command Mode

OSPF Router Configuration

---

## ip area virtual-link ipsec security-association

Link the Internet Protocol Security (IPsec) security association to the OSPF virtual link.

## Syntax

- **default ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec security-association WORD<0-32>**
- **ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec security-association WORD<0-32>**



- **no ip area virtual-link {A.B.C.D} {A.B.C.D} ipsec security-association WORD<0-32>**

## Command Parameters

**{A.B.C.D} {A.B.C.D}**

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

**WORD<0-32>**

Specifies the name of the security association.

## Default

None

## Command Mode

OSPF Router Configuration

## ipv6 area

---

Create and configure an OSPFv3 IPv6 area.

## Syntax

- **default ipv6 area {A.B.C.D}**
- **default ipv6 area {A.B.C.D} default-cost**
- **default ipv6 area {A.B.C.D} import**
- **default ipv6 area {A.B.C.D} import-summaries enable**
- **ipv6 area {A.B.C.D}**
- **ipv6 area {A.B.C.D} default-cost <0-16777215>**
- **ipv6 area {A.B.C.D} import external**
- **ipv6 area {A.B.C.D} import noexternal**
- **ipv6 area {A.B.C.D} import nssa**
- **ipv6 area {A.B.C.D} import-summaries enable**
- **ipv6 area {A.B.C.D} translator-role <1-2>**
- **ipv6 area {A.B.C.D} type nssa**
- **ipv6 area {A.B.C.D} type stub**
- **no ipv6 area {A.B.C.D}**
- **no ipv6 area {A.B.C.D} import-summaries enable**

## Command Parameters

**{A.B.C.D}**

Specifies the area address.

**default-cost <0-16777215>**

Specifies the stub metric for the area. The default-cost default is 10.

**import <external|noexternal|nssa>**

Configures the area support for importing advertisements. The default is external.

**import-summaries enable**

Configures the area support for importing summary advertisements into a stub area. Use this entry only for a stub area. The default is enabled.

**translator-role {1|2}**

Indicates a Not-So-Stubby-Area (NSSA) border router ability to perform translation of type-7 LSAs into type-5 LSAs. Configure this value to 2 to make it a candidate. You can configure this parameter only when you first create the area. The default translator-role is 1.

**type {nssa|stub}**

Configures the type of area. A Not-So-Stubby-Area (NSSA) prevents flooding of normal route advertisements into the area by replacing them with a default route. A stub area uses only one exit point (router interface) out of the area. You can configure this parameter only when you first create the area. By default, the area is neither a stub area or NSSA (Not-So-Stubby Area).

## Default

None

## Command Mode

OSPF Router Configuration

## ipv6 area range

---

Create and configure an area address range on the OSPF router to reduce the number of ABR advertisements into other OSPF areas.

## Syntax

- **default ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link [advertise-metric]**
- **default ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink [advertise-metric]**
- **ipv6 area range {A.B.C.D} WORD<0-255> advertise-mode advertise**
- **ipv6 area range {A.B.C.D} WORD<0-255> advertise-mode not-advertise**
- **ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-metric <0-65535>**

- `ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-mode advertise`
- `ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-mode not-advertise`
- `ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-metric <0-65535>`
- `ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-mode advertise`
- `ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-mode not-advertise`
- `no ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link`
- `no ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink`

## Command Parameters

`{A.B.C.D}`

Specifies the area address.

`advertise-metric <0-65535>`

Specifies the advertise metric value and LSA type. The default advertise-metric is 0.

`advertise-mode <advertise|not-advertise>`

Configures if the area advertises into other OSPF areas. The default advertise-mode is advertise.

`inter-area-prefix-link`

Configures the area to use this LSA type.

`nssa-extlink`

Configures the area to use this LSA type.

`WORD<0-255>`

Specifies the IPv6 address and prefix.

## Default

None

## Command Mode

OSPF Router Configuration

## ipv6 area virtual-link

Configure an OSPF virtual interface to the ABR if a remote OSPF ABR uses no connection to the backbone area but needs to be part of the same routing domain in which the switch resides.

## Syntax

- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D}**
- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} dead-interval**
- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} hello-interval**
- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval**
- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} transit-delay**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D}**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} dead-interval <1-65535>**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} hello-interval <1-65535>**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval <1-1800>**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} transit-delay <1-1800>**
- **no ipv6 area virtual-link {A.B.C.D} {A.B.C.D}**

## Command Parameters

**{A.B.C.D} {A.B.C.D}**

Specifies the area address and the virtual link address.

**dead-interval <1-65535>**

Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default dead-interval is 60.

**hello-interval <1-65535>**

Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default hello interval is 10.

**retransmit-interval <1-1800>**

Specifies the retransmit interval, in seconds, for link-state advertisements. The default retransmit-interval is 5.

**transit-delay <1-1800>**

Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default transit-delay is 1.

## Default

The default is disabled.

## Command Mode

OSPF Router Configuration

## ipv6 area virtual-link ipsec

Create the Internet Protocol Security (IPsec) policy under the OSPF virtual link.

## Syntax

- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec**
- **no ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec**

## Command Parameters

{A.B.C.D} {A.B.C.D}

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

## Default

None

## Command Mode

OSPF Router Configuration

---

## ipv6 area virtual-link ipsec action

Configure the action of the Internet Protocol Security (IPsec) policy under the OSPF virtual link.

## Syntax

- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec action**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec action drop**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec action permit**
- **no ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec action**

## Command Parameters

{A.B.C.D} {A.B.C.D}

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

**action <drop|permit>**

Specifies the action of the IPsec policy under the OSPF virtual link to permit or drop traffic. The default is permit.

## Default

The default is permit.

## Command Mode

OSPF Router Configuration

---

## ipv6 area virtual-link ipsec direction

---

Configure the direction of the Internet Protocol Security (IPsec) policy under the OSPF virtual link.

### Syntax

- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction both**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction in**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction out**
- **no ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec direction**

### Command Parameters

{A.B.C.D} {A.B.C.D}

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

<both|in|out>

Specifies the direction of the traffic of the IPsec policy under the OSPF virtual link.

### Default

None

### Command Mode

OSPF Router Configuration

---

## ipv6 area virtual-link ipsec enable

---

Enable the Internet Protocol Security (IPsec) policy created under the OSPF virtual link.

### Syntax

- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec enable**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec enable**
- **no ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec enable**

### Command Parameters

{A.B.C.D} {A.B.C.D}

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

## Default

The default is disabled.

## Command Mode

OSPF Router Configuration

---

## ipv6 area virtual-link ipsec security-association

---

Link the Internet Protocol Security (IPsec) security association to the OSPF virtual link.

## Syntax

- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec security-association WORD<0-32>**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec security-association WORD<0-32>**
- **no ipv6 area virtual-link {A.B.C.D} {A.B.C.D} ipsec security-association WORD<0-32>**

## Command Parameters

**{A.B.C.D} {A.B.C.D}**

The first IP address specifies the area IP address, and the second IP address specifies the virtual-link IP address.

**WORD<0-32>**

Specifies the name of the security association.

## Default

None

## Command Mode

OSPF Router Configuration

---

## ipv6 as-boundary-router

---

Enable or disable the boundary-router on the router interface.

## Syntax

- **default ipv6 as-boundary-router [enable]**
- **ipv6 as-boundary-router**

- **ipv6 as-boundary-router enable**
- **no ipv6 as-boundary-router [enable]**

## Command Parameters

**enable**

Enables the boundary-router.

## Default

The default is disabled.

## Command Mode

OSPF Router Configuration

## ipv6 redistribute (for OSPF)

---

Enable redistribution to redistribute IPv6 routes into an OSPFv3 routing domain.

## Syntax

- **default ipv6 redistribute {bgp | direct | ospf | rip |static} [enable]**
- **ipv6 redistribute direct {enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}**
- **ipv6 redistribute isis {enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}**
- **ipv6 redistribute static {enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}**
- **no ipv6 redistribute {bgp | direct | ospf | rip |static} [enable]**

## Command Parameters

**{bgp | direct | ospf | rip |static}**

Specifies the type of IPv6 route to redistribute to the OSPFv3 routing domain.

**{enable | metric <0-65535> | metric-type [type1][type2] | route-map WORD<1-64>}**

Enables redistribution.

## Default

The default is disabled.

## Command Mode

OSPF Router Configuration



---

## ipv6 redistribute bgp enable (For OSPF)

---

Enable IPv6 BGP redistribute.

### Syntax

- **ipv6 redistribute bgp enable**
- **no ipv6 redistribute bgp enable**

### Default

None

### Command Mode

OSPF Router Configuration

---

## ipv6 router-id

---

Configure the OSPF router ID.

### Syntax

- **default ipv6 router-id**
- **ipv6 router-id {A.B.C.D}**

### Command Parameters

{A.B.C.D}

Specifies the address for the router ID.

### Default

None

### Command Mode

OSPF Router Configuration

---

## ipv6 tunnel (for OSPF)

---

Configure OSPF parameters for an IPv6 tunnel.

## Syntax

- **default ipv6 tunnel <1-2000>**
- **default ipv6 tunnel <1-2000> dead-interval**
- **default ipv6 tunnel <1-2000> hello-interval**
- **default ipv6 tunnel <1-2000> metric**
- **default ipv6 tunnel <1-2000> poll-interval**
- **default ipv6 tunnel <1-2000> priority**
- **default ipv6 tunnel <1-2000> retransmit-interval**
- **default ipv6 tunnel <1-2000> transmit-delay**
- **ipv6 tunnel <1-2000> area {A.B.C.D}**
- **ipv6 tunnel <1-2000> dead-interval <1-65535>**
- **ipv6 tunnel <1-2000> enable**
- **ipv6 tunnel <1-2000> hello-interval <1-65535>**
- **ipv6 tunnel <1-2000> metric <0-65535>**
- **ipv6 tunnel <1-2000> poll-interval <0-65535>**
- **ipv6 tunnel <1-2000> priority <0-255>**
- **ipv6 tunnel <1-2000> retransmit-interval <1-1800>**
- **ipv6 tunnel <1-2000> transmit-delay <1-1800>**
- **no ipv6 tunnel <1-2000>**
- **no ipv6 tunnel <1-2000> enable**

## Command Parameters

**{A.B.C.D}**

Specifies the area address.

**<1-2000>**

Specifies the tunnel ID.

**dead-interval <1-65535>**

Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default dead-interval is 40.

**hello-interval <1-65535>**

Specifies the hello interval, in seconds, for hello packets sent between switches for an interface in an OSPF area. The default hello-interval is 10.

**metric <0-65535>**

Configures the OSPF metric for the tunnel. The switch advertises the metric in router link advertisements. The default metric is 100.

**poll-interval <0-65535>**

Configures the polling interval, in seconds, for the OSPF tunnel. The default pollinterval is 120.

**priority <0-255>**

Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The default priority is 1.

**retransmit-interval <1-1800>**

Specifies the retransmit interval, in seconds, for link-state advertisements. The default retransmit-interval is 5.

**transmit-delay <1-1800>**

Specifies the transmit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default transmit-delay is 1.

## Default

None

## Command Mode

OSPF Router Configuration

## neighbor (for OSPF)

---

Configure NBMA neighbors so that the interface can participate in Designated Router election. All OSPF neighbors that you manually configure are NBMA neighbors.

## Syntax

- **default neighbor {A.B.C.D}**
- **neighbor {A.B.C.D} priority <0-255>**
- **network {A.B.C.D}**
- **no neighbor {A.B.C.D}**

## Command Parameters

**<A.B.C.D>**

Identifies an OSPF area in IP address format A.B.C.D.

**priority <0-255>**

Changes the priority level of the neighbor.

## Default

None

## Command Mode

OSPF Router Configuration

---

## network (for OSPF)

---

Enable OSPF on a network.

### Syntax

- **default network {A.B.C.D}**
- **network {A.B.C.D}**
- **network {A.B.C.D} area {A.B.C.D}**
- **no network {A.B.C.D}**

### Command Parameters

{A.B.C.D}

Specifies the IP address of the network.

area {A.B.C.D}

Specifies the OSPF area.

### Default

None

### Command Mode

OSPF Router Configuration

---

## redistribute (for OSPF)

---

Redistribute learned routes into OSPF.

### Syntax

- **default redistribute { bgp | direct | isis | ospf | rip | static }**
- **default redistribute { bgp | direct | isis | ospf | rip | static } enable**
- **default redistribute { bgp | direct | isis | ospf | rip | static } enable vrf-src WORD<1-16>**
- **default redistribute { bgp | direct | isis | ospf | rip | static } metric**
- **default redistribute { bgp | direct | isis | ospf | rip | static } route-map**
- **default redistribute { bgp | direct | isis | ospf | rip | static } vrf-src WORD<1-16>**
- **default redistribute { bgp | direct | isis | ospf | rip | static } metric-type**

- `default redistribute { bgp| direct | isis | ospf | rip | static } subnets`
- `no redistribute { bgp| direct | isis | ospf | rip | static }`
- `no redistribute { bgp| direct | isis | ospf | rip | static } route-map`
- `no redistribute { bgp| direct | isis | ospf | rip | static } vrf-src WORD<1-16>`
- `no redistribute { bgp| direct | isis | ospf | rip | static } enable`
- `no redistribute { bgp| direct | isis | ospf | rip | static } enable vrf-src WORD<1-16>`
- `redistribute { bgp| direct | isis | ospf | rip | static }`
- `redistribute { bgp| direct | isis | ospf | rip | static } metric-type { type1 | type2 } vrf-src WORD<1-16>`
- `redistribute { bgp| direct | isis | ospf | rip | static } enable`
- `redistribute { bgp| direct | isis | ospf | rip | static } metric <0-65535>`
- `redistribute { bgp| direct | isis | ospf | rip | static } metric vrf-src WORD<1-16>`
- `redistribute { bgp| direct | isis | ospf | rip | static } metric-type { type1 | type2 }`
- `redistribute { bgp| direct | isis | ospf | rip | static } route-map WORD<0-64>`
- `redistribute { bgp| direct | isis | ospf | rip | static } subnets { allow | suppress }`
- `redistribute { bgp| direct | isis | ospf | rip | static } vrf-src WORD<1-16>`

## Command Parameters

`{ bgp| direct | isis | ospf | rip | static }`

Specifies the protocol type. The possible values are bgp, direct, isis, ospf, rip, or static.

`enable`

Enables route redistribution of Intermediate-System-to-Intermediate-System (IS-IS) learned IP routes into OSPF.

`metric <0-65535>`

Configures the metric (cost) to apply to redistributed routes. The default is 1.

`metric-type { type1 | type2 }`

Configures the type of route to import into the OSPF protocol.

`route-map WORD<0-64>`

Configures the route policy to apply to redistributed routes.

`subnets { allow | suppress }`

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**vrf-src WORD<1-16>**

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

By default, route redistribution is disabled.

## Command Mode

OSPF Router Configuration

---

## rfc1583-compatibility enable

Controls the preference rules used when the router chooses among multiple autonomous system external (ASE) LSAs which advertise the same destination. If enabled, the preference rule is the same as that specified by RFC1583. If disabled, the preference rule is as described in RFC2328, which can prevent routing loops when ASE LSAs for the same destination originate from different areas.

## Syntax

- **default rfc1583-compatibility**
- **default rfc1583-compatibility enable**
- **no rfc1583-compatibility**
- **no rfc1583-compatibility enable**
- **rfc1583-compatibility enable**

## Default

The default is disabled.

## Command Mode

OSPF Router Configuration

---

## router-id (for OSPF)

Configure OSPF parameters on the switch to control how OSPF behaves on the system. The switch uses global parameters to communicate with other OSPF routers. Globally configure OSPF before you configure OSPF for an interface, port, or VLAN.

## Syntax

- **default router-id**
- **no router-id**
- **router-id {A.B.C.D}**

## Command Parameters

**router-id <A.B.C.D>**

Configures the OSPF router ID IP address, where A.B.C.D is the IP address.

## Default

None

## Command Mode

OSPF Router Configuration

---

## show ip ospf

Display OSPF configuration information to ensure accuracy.

## Syntax

- **show ip ospf**
- **show ip ospf vrf WORD <1-16>**
- **show ip ospf vrfids WORD <0-512>**

## Command Parameters

**vrf WORD <1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

OSPF Router Configuration

---

## timers basic holddown (for OSPF)

---

Configures the OSPF hold-down timer value, the length of time (in seconds) that OSPF continues to advertise a network after determining that it is unreachable.

### Syntax

- **default timers basic**
- **default timers basic holddown**
- **timers basic holddown <3-60>**

### Command Parameters

<3-60>

Configures the holddown timer value.

### Default

The default is 120 seconds.

### Command Mode

OSPF Router Configuration

---

## trap

---

Enable OSPF traps.

### Syntax

- **default trap**
- **default trap enable**
- **no trap**
- **no trap enable**
- **trap enable**

### Command Parameters

enable

Enables OSPF traps.

### Default

The default value is disable.



## Command Mode

OSPF Router Configuration



# OVSDB Configuration

---

The following topics document commands available in OVSDB Configuration mode of the command line interface (CLI).

## controller

---

Configures the Network Virtualization Controller for OVSDB.

### Syntax

- **controller** <1-100> **ip address** <A.B.C.D> **protocol** **ssl**
- **controller** <1-100> **ip address** <A.B.C.D> **protocol** **ssl** **port** <1-65535>
- **controller** <1-100> **ip address** <A.B.C.D> **protocol** **tcp**
- **controller** <1-100> **ip address** <A.B.C.D> **protocol** **tcp** **port** <1-65535>
- **no controller** <1-100>

### Command Parameters

**<1-100>**

Specifies the OVSDB controller ID.

**ip address** <A.B.C.D>

Specifies an IPv4 address for the OVSDB controller.

**port** <1-65535>

Specifies a port number for the OVSDB controller.

**protocol** **ssl**

Specifies SSL communications protocol for the OVSDB controller.

**protocol** **tcp**

Specifies TCP communications protocol for the OVSDB controller.

### Default

None

### Command Mode

OVSDB Configuration

---

## install-cert-file

---

Specifies the certificate file path and file name for OVSDB.

### Syntax

- **install-cert-file WORD<1-128>**
- **no install-cert-file**

### Command Parameters

WORD <1-128>

Specifies the path and file name of the OVSDB certificate.

### Default

None

### Command Mode

OVSDB Configuration

---

## managed-interface i-sids

---

Configure an I-SID as the management interface for OVSDB.

### Syntax

- **managed-interface i-sids WORD <1-1024>**

### Command Parameters

WORD <1-1024>

Specifies the I-SIDs to create an OVSDB managed interface.

### Default

None

### Command Mode

OVSDB Configuration

---

## private-key

---

Specifies the path and filename of the private key for OVSDB.

## Syntax

- **no private-key**
- **private key WORD <1-128>**

## Command Parameters

**WORD <1-128>**

Specifies the path and file name of the OVSDB private key.

## Default

None

## Command Mode

OVSDB Configuration

---

## replication

Configures OVSDB replication.

## Syntax

- **default replication**
- **no replication**
- **replication peer-ip <A.B.C.D> local-ip <A.B.C.D>**

## Command Parameters

**local-ip <A.B.C.D>**

Specifies an IPv4 address for the primary local OVSDB controller.

**peer-ip <A.B.C.D>**

Specifies an IPv4 address for the secondary peer OVSDB controller.

## Default

None

## Command Mode

OVSDB Configuration



# Privileged EXEC

---

The following topics document commands available in Privileged EXEC mode of the command line interface (CLI).

## !(command number)

---

Executes a previously used command that displays it in the output of the show history command. Specify the number that displays it before the command in the show history output. You must be in the correct mode to reuse the command.

### Syntax

- **!(command number)**

### Default

None

### Command Mode

Privileged EXEC

## attribute

---

Modify MS-DOS file attributes to enable file transfer.

### Syntax

- **attribute WORD<1-1536> + | - | R**
- **attribute WORD<1-99> + | - | R**

### Command Parameters

**+ | - | R**

Set or remove read-only permission.

**WORD<1-99>**

Specifies the file name.

## Default

None

## Command Mode

Privileged EXEC

# backup

---

Use this command to backup all files, including the directory of the internal flash, to the USB flash or to create a backup zip.

## Syntax

- **backup configure WORD<1-99>**
- **backup intflash**

## Command Parameters

### configure WORD<1-99>

Copies all configuration files and packages them into a single .zip file. License files are not backed up.

### intflash

Copies all files from the internal flash to the USB drive at /usb/intflash. You must disable logging to the compact flash you want to restore before you can use the backup. The system verifies that the USB flash device has enough available space to perform the backup operation. If the USB flash device does not have enough available space, the system displays an error message. The backup command uses the following filepath on the USB flash device: /usb/intflash/intflashbackup\_yyyymmddhhmmss.tgz.



### Note

This command does not apply to all hardware platforms. On some platforms, the USB port cannot be used for file transfer. For more information, see your hardware documentation.

## Default

None

## Command Mode

Privileged EXEC

---

## boot

---

Restart the switch to implement configuration changes or recover from a system failure. When you restart the system, you can specify an optional configuration file to use to load the device. If no config file is specified, the run-time CLI uses the configuration file specified by the boot config choice command. The image booted is that specified by the software activate command.

### Syntax

- **boot**
- **boot [config WORD<1-99>] [-y]**
- **boot config WORD<1-99>**
- **boot -y**

### Command Parameters

**-y**

Suppresses the confirmation message before the switch restarts. If you omit this parameter, you must confirm the action before the switch restarts.

**config WORD<1-99>**

Specifies the software configuration device and file name in the following format:/intflash/<file>. The filename, including the directory structure, can include up to 99 characters.

### Default

None

### Command Mode

Privileged EXEC

---

## cd

---

Change current file system directory path.

### Syntax

- **cd WORD<1-99>**

### Command Parameters

**<1-99>**

Specifies the directory location.

## Default

None

## Command Mode

Privileged EXEC

---

## clear alarm

Clear the alarm database to remove old information after a condition is resolved or to reset statistics.

## Syntax

- **clear alarm database**
- **clear alarm database alarm-id WORD<0-100>**
- **clear alarm statistics**

## Command Parameters

### database

Clears the alarm database.

### database alarm-id WORD<0-100>

Specifies an alarm ID to clear.

### statistics

Clears the alarm database statistics.

## Default

None

## Command Mode

Privileged EXEC

---

## clear app-telemetry counter

Clear the Application Telemetry status counters.

## Syntax

- **clear app-telemetry counter**
- **clear app-telemetry counter id <number>**
- **clear app-telemetry counter name <rule>**



## Command Parameters

**id** <1-2000>

Clears the counters for the specified rule number.

**name** WORD<1-32>

Clears the counters for the specified rule name.

## Default

None

## Command Mode

Privileged EXEC

## clear dvr host-entries

---

Clears Distributed Virtual Routing (DvR) host entries.

## Syntax

- **clear dvr host-entries**
- **clear dvr host-entries ipv4 {A.B.C.D}**
- **clear dvr host-entries ipv4 {A.B.C.D} l3isid <0-16777215>**
- **clear dvr host-entries l2isid <0-16777215>**
- **clear dvr host-entries l3isid <0-16777215>**
- **clear dvr host-entries l3isid <0-16777215> ipv4 {A.B.C.D}**

## Command Parameters

**ipv4** {A.B.C.D}

Specifies the IPv4 address.

**l2isid** <0-16777215>

DvR host entries for the specific layer 2 I-SID.

**l3isid** <0-16777215>

DvR host entries for the specific layer 3 I-SID.

## Default

None

## Command Mode

Privileged EXEC

## clear eapol non-eap

---

Clears the Non-EAP session that is learned on the switch.

### Syntax

- **clear eapol non-eap**
- **clear eapol non-eap {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **clear eapol non-eap {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} 0x00:0x00:0x00:0x00:0x00:0x00**
- **clear eapol non-eap 0x00:0x00:0x00:0x00:0x00:0x00**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Specifies the port list on which the Non-EAP MAC is learnt.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC-Address on the Non-EAP session.

### Default

None

### Command Mode

Privileged EXEC

## clear energy-saver eee stats

---

Clear Energy Efficient Ethernet (EEE) statistics for all ports, or for a specific port.

### Syntax

- **clear energy-saver eee stats**
- **clear energy-saver eee stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## clear fa statistics

---

Clears the Fabric Attach statistics information on the switch.

## Syntax

- **clear fa statistics**
- **clear fa statistics summary**
- **clear fa statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

### summary

Displays the summary of the Fabric Attach statistics information.

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

---

## clear filter acl

---

Clear Access Control List (ACL) statistics if you no longer require previous statistics or log information.

### Syntax

- **clear filter acl log**
- **clear filter acl statistics <acl-id>**
- **clear filter acl statistics <acl-id> <ace-id>**
- **clear filter acl statistics <acl-id> qos**
- **clear filter acl statistics <acl-id> security**
- **clear filter acl statistics all**
- **clear filter acl statistics default**
- **clear filter acl statistics default <acl-id>**
- **clear filter acl statistics global**
- **clear filter acl statistics global <acl-id>**

### Command Parameters

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

**all**

Clears all statistics for all access control entries.

**default** *<acl-id>*

Clears traffic statistics for an access control entry (ACE).

**global** *<acl-id>*

Clears global statistics for an access control entry (ACE).

**qos**

Clears access control list (ACL) statistics for QoS access control entries (ACEs).

**security**

Clears access control list (ACL) statistics for Security ACEs.

### Default

None

## Command Mode

Privileged EXEC

## clear ip arp interface

---

Clear the ARP timers.

### Syntax

- **clear ip arp interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **clear ip arp interface vlan <1-4059>**

### Command Parameters

**gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

## Command Mode

Privileged EXEC

## clear ip bfd stats

---

Clear local and remote Bidirectional Forwarding Detection (BFD) statistics for IPv4 interfaces.

### Syntax

- **clear ip bfd stats**
- **clear ip bfd stats vrf WORD<1-16>**
- **clear ip bfd stats vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF instance by VRF name.

**vrfids WORD<0-512>**

Specifies a VRF or range of VRFs by ID.

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## clear ip dhcp-relay

Clear dhcp-relay counter.

## Syntax

- **clear ip dhcp-relay counters**
- **clear ip dhcp-relay counters interface gigabitethernet {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]**
- **clear ip dhcp-relay counters interface vlan <1-4059>**
- **clear ip dhcp-relay counters vrf WORD<1-16>**
- **clear ip dhcp-relay counters vrfid <0-511>**

## Command Parameters

*{slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### counters

Clear dhcp-relay counters/statistics. No interface specified, it will clear all interface on GlobalRouter.

**vlan <1-4059>**

Clear Ip dhcp-relay statistics by vlan.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags,

the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Clear vrf Ip dhcp-relay statistics.

**vrfid <0-511>**

Enter Vrf Id.

## Default

None

## Command Mode

Privileged EXEC

## clear ip dhcp-relay counters

---

Clear the Ip Dhcp Relay counter.

## Syntax

- **clear ip dhcp-relay counters interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **clear ip dhcp-relay counters vrf WORD<1-16>**
- **clear ip dhcp-relay counters vrfid <0-511>**

## Command Parameters

**<0-511>**

Specifies the VRF ID.

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Clear IP routes on the Interface Gigabit Ethernet.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**WORD<1-16>**

Specifies the VRF name.

## Default

None

## Command Mode

Privileged EXEC

## clear ip dhcp-snooping binding

---

Clears entries from the DHCP Snooping binding table.

### Syntax

- **clear ip dhcp-snooping binding dynamic**
- **clear ip dhcp-snooping binding static**

### Command Parameters

**dynamic**

Clears dynamic entries from the DHCP Snooping binding table.

**static**

Clears static entries from the DHCP Snooping binding table.

### Default

None

## Command Mode

Privileged EXEC

## clear ip mroute stats

---

Clear IP multicast route statistics.

### Syntax

- **clear ip mroute stats**

### Default

None

## Command Mode

Privileged EXEC



---

## clear ip msdp peer

---

Clears the peer connection to clear the TCP connection to the specified MSDP peer and resets all MSDP message counters.

### Syntax

- **clear ip msdp peer {A.B.C.D} vrf WORD<0-16>**
- **clear ip msdp peer {A.B.C.D} vrfids WORD<0-512>**

### Command Parameters

**{A.B.C.D}**

Specifies the MSDP peer IP address.

**vrf WORD<0-16>**

Specifies the VRF name.

**vrfids WORD<0-512>**

Specifies the VRF ID.

### Default

None

### Command Mode

Privileged EXEC

---

## clear ip msdp sa-cache

---

Clears the MSDP foreign cache entries.

### Syntax

- **clear ip msdp sa-cache vrf WORD<0-16>**
- **clear ip msdp sa-cache vrfids WORD<0-512>**

### Command Parameters

**group <prefix/len>**

Specifies the group IP address of the SA cache entry.

**peer {A.B.C.D}**

Specifies the peer address.

**RP {A.B.C.D}**

Specifies the RP address of the SA cache entry.

**source <prefix/len>**

Specifies the source IP address of the SA cache entry.

**vrf WORD<0-16>**

Specifies the VRF name.

**vrfids WORD<0-512>**

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

---

## clear ip msdp sa-cache peer

Clears the MSDP cache for a specific peer.

## Syntax

- **clear ip msdp sa-cache peer {A.B.C.D} vrf WORD<0-16>**
- **clear ip msdp sa-cache peer {A.B.C.D} vrfids WORD<0-512>**

## Default

None

## Command Mode

Privileged EXEC

---

## clear ip msdp statistics

Clear IP MSDP statistics counters.

## Syntax

- **clear ip msdp statistics**
- **clear ip msdp statistics {A.B.C.D}**
- **clear ip msdp statistics {A.B.C.D} vrf WORD<0-16>**
- **clear ip msdp statistics {A.B.C.D} vrfids WORD<0-512>**
- **clear ip msdp statistics vrf WORD<0-16>**
- **clear ip msdp statistics vrfids WORD<0-512>**

## Command Parameters

{A.B.C.D}

Specifies the peer address.

vrf WORD<0-16>

Specifies the VRF name.

vrfids WORD<0-512>

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

## clear ip ospf stats

---

Clear IP OSPF statistics.

## Syntax

- **clear ip ospf stats vrf <WORD<1-16>**
- **clear ip ospf stats vrfid <0-511>**

## Command Parameters

vrf WORD<1-16>

Specifies the VRF name.

vrfid <0-511>

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

## clear ip route

---

Clear the routing table.

## Syntax

- **clear ip route gigabitethernet {slot/port[/sub-port]}**
- **clear ip route vlan <1-4059>**

## Command Parameters

**gigabitethernet** {*slot/port[/sub-port]*}

Clear IP routes on the Interface Gigabit Ethernet.

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Clear IP routes on the Interface Vlan.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## clear ip vrrp

---

Clear the Virtual Router Redundancy Protocol (VRRP) configuration.

## Syntax

- **clear ip vrrp gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} vrid <1-255>**
- **clear ip vrrp vlan <1-4059> vrid <1-255>**

## Command Parameters

**gigabitethernet** {*slot/port[/sub-port] [-slot/port[/sub-port]] [,...]*}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrid** <1-255>

Specifies the ID of the virtual router.

## Default

None

## Command Mode

Privileged EXEC

## clear ipsec stats all

---

Clear the Internet Protocol Security (IPsec) system statistics counters.

## Syntax

- **clear ipsec stats all**

## Default

None

## Command Mode

Privileged EXEC

## clear ipv6 bfd stats

---

Clear local and remote Bidirectional Forwarding Detection (BFD) statistics for IPv6 interfaces.



### Note

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Syntax

- **clear ipv6 bfd stats**
- **clear ipv6 bfd stats vrf WORD<1-16>**

- **clear ipv6 bfd stats vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF instance by VRF name.

**vrfids WORD<0-512>**

Specifies a VRF or range of VRFs by ID.

## Command Mode

Privileged EXEC

## clear ipv6 dcache

---

Clear the destination cache.

## Syntax

- **clear ipv6 dcache [vrf WORD<1-16> | vrfids WORD<0-512>]**
- **clear ipv6 dcache gigabitethernet {slot/port[/sub-port]} [vrf WORD<1-16> | vrfids WORD<0-512>]**
- **clear ipv6 dcache mgmtethernet mgmt**
- **clear ipv6 dcache tunnel <1-2000>**
- **clear ipv6 dcache vlan <1-4059> [vrf WORD<1-16> | vrfids WORD<0-512>]**

## Command Parameters

**gigabitethernet {slot/port[/sub-port]}**

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mgmtethernet mgmt**

Identifies a management port.

**tunnel <1-2000>**

Specifies the tunnel ID.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Clears the interface information for a particular VRF name.

**vrfids WORD<0-512>**

Clears the interface information for the particular VRF ids

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

The *mgmtethernet mgmt* parameter only applies to VSP 8600 Series.

## clear ipv6 fhs snooping

---

Clears all Security Binding Table (SBT) entries or a particular dynamic SBT entry.

## Syntax

- **clear ipv6 fhs snooping**
- **clear ipv6 fhs snooping vlan <1-4059>**
- **clear ipv6 fhs snooping vlan <1-4059> ipv6-address WORD<0-46>**

## Command Parameters

**ipv6-address WORD<0-46>**

Clears a specific snooping entry based on its IPv6 address.

**vlan <1-4059>**

Clears snooping entries by VLAN.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

---

## clear ipv6 fhs statistics all

---

Clears the IPv6 ND inspection statistics along with RA guard statistics and DHCPv6 Guard statistics.

### Syntax

- **clear ipv6 fhs statistics all**
- **clear ipv6 fhs statistics all {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

Privileged EXEC

---

## clear ipv6 fhs statistics dhcp-guard

---

Clears the DHCP-guard statistics.

### Syntax

- **clear ipv6 fhs statistics dhcp-guard**
- **clear ipv6 fhs statistics dhcp-guard {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



## Default

None

## Command Mode

Privileged EXEC

## clear ipv6 fhs statistics nd-inspection

---

Clear the Neighbor Discovery inspection statistics on either a single port or a set of ports or all ports.

## Syntax

- **clear ipv6 fhs statistics nd-inspection**
- **clear ipv6 fhs statistics nd-inspection {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## clear ipv6 fhs statistics ra-guard

---

Clears the RA Guard statistics.

## Syntax

- **clear ipv6 fhs statistics ra-guard**
- **clear ipv6 fhs statistics ra-guard {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

---

## clear ipv6 mroute stats

Clear IPv6 multicast route statistics.

## Syntax

- **clear ipv6 mroute stats**

## Default

None

## Command Mode

Privileged EXEC

---

## clear ipv6 neighbor-cache

Clear the neighbor cache.

## Syntax

- **clear ipv6 neighbor-cache [vrf WORD<1-16> | vrfids WORD<0-512>]**
- **clear ipv6 neighbor-cache gigabitEthernet {slot/port[/sub-port]} [vrf WORD<1-16> | vrfids WORD<0-512>]**
- **clear ipv6 neighbor-cache mgmtethernet mgmt**
- **clear ipv6 neighbor-cache vlan <1-4059> [vrf WORD<1-16> | vrfids WORD<0-512>]**

## Command Parameters

**gigabitethernet** {*slot/port[/sub-port]*}

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mgmtethernet mgmt**

Identifies a management port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Clears the interface information for a particular VRF name.

**vrfids WORD<0-512>**

Clears the interface information for the particular VRF ids

## Default

The default is disabled.

## Command Mode

Privileged EXEC

## Usage Guidelines

The *mgmtethernet mgmt* parameter only applies to VSP 8600 Series.

## clear ipv6 ospf stats

---

Clear the IPv6 OSPF statistics.

## Syntax

- **clear ipv6 ospf stats [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **clear ipv6 ospf stats vrf WORD<1-16>**
- **clear ipv6 ospf stats vrfids WORD<0-512>**

## Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

Privileged EXEC

## clear ipv6 rip

---

Clear Routing Information Protocol next generation (RIPng) information for IPv6 interface.

## Syntax

- **clear ipv6 rip stats**
- **clear ipv6 rip stats gigabitethernet {slot/port[/sub-port]}**
- **clear ipv6 rip stats vlan <1-4059>**

## Command Parameters

### stats

Clears RIPng statistics for IPv6 interface.

### gigabitethernet {slot/port[/sub-port]}

Clears IPv6 RIPng statistics for brouter.

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### vlan <1-4059>

Clears IPv6 RIPng statistics for VLAN.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## clear ipv6 route static

---

Clear IPv6 static routes.

### Syntax

- `clear ipv6 route static [vrf WORD<1-16> | vrfids WORD<0-512>]`

### Command Parameters

`vrf WORD<1-16>`

Clears the interface information for a particular VRF name.

`vrfids WORD<0-512>`

Clears the interface information for the particular VRF ids

### Default

None

### Command Mode

Privileged EXEC

## clear ipv6 statistics

---

Use this command to clear IPv6 statistics.

### Syntax

- `clear ipv6 statistics all [vrf WORD<1-16> | vrfids WORD<0-512>]`
- `clear ipv6 statistics interface [vrf WORD<1-16> | vrfids WORD<0-512>]`
- `clear ipv6 statistics interface general [vrf WORD<1-16> | vrfids WORD<0-512>]`
- `clear ipv6 statistics interface general gigabitethernet {slot/port[/sub-port]} [vrf WORD<1-16> | vrfids WORD<0-512>]`
- `clear ipv6 statistics interface general loopback <1-256>`
- `clear ipv6 statistics interface general mgmtethernet mgmt`
- `clear ipv6 statistics interface general tunnel <1-2000>`
- `clear ipv6 statistics interface general vlan <1-4059>`
- `clear ipv6 statistics interface icmp`
- `clear ipv6 statistics interface icmp gigabitethernet {slot/port[/sub-port]}`
- `clear ipv6 statistics interface icmp loopback <1-256>`
- `clear ipv6 statistics interface icmp mgmtethernet mgmt`

- **clear ipv6 statistics interface icmp tunnel <1-2000>**
- **clear ipv6 statistics interface icmp vlan <1-4059>**
- **clear ipv6 statistics tcp [vrf WORD<1-16> | vrfids WORD<0-512>]**
- **clear ipv6 statistics udp [vrf WORD<1-16> | vrfids WORD<0-512>]**

## Command Parameters

### all

Clears all statistics.

### general

Clears general statistics.

### gigabitEthernet {slot/port[/sub-port]}

Clears statistics for a brouter interface.

Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### icmp

Clears Internet Control Message Protocol (ICMP) statistics.

### loopback <1-256>

Identifies a loopback interface.

### mgmtethernet mgmt

Clears statistics for a management port.

### tcp

Clears TCP statistics.

### tunnel <1-2000>

Clears statistics for a tunnel.

### udp

Clears UDP statistics.

### vlan <1-4059>

Clears statistics for a tunnel.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### vrf WORD<1-16>

Clears the interface information for a particular VRF name.

### vrfids WORD<0-512>

Clears the interface information for the particular VRF ids

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

The *mgmtethernet mgmt* parameter only applies to VSP 8600 Series.

## clear ipv6 vrrp

---

Clears the IPv6 VRRP configuration.

## Syntax

- **clear ipv6 vrrp gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} vrid <1-255>**
- **clear ipv6 vrrp vlan <1-4059> vrid <1-255>**

## Command Parameters

**gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrid** <1-255>

Specifies the ID of the virtual router.

## Default

None

## Command Mode

Privileged EXEC

---

## clear isis lsdb

---

Clear the Intermediate-System-to-Intermediate-System (IS-IS) Link State Database (LSDB). The command clears learned Link State Packets (LSPs) only. The command does not clear local generated LSPs. As soon as the platform clears the LSDB the LSP synchronization process starts immediately and the LSDB synchronizes with its neighbors.

### Syntax

- **clear isis lsdb**

### Default

None

### Command Mode

Privileged EXEC

---

## clear isis stats

---

Clear Intermediate-System-to-Intermediate-System (IS-IS) statistics.

### Syntax

- **clear isis stats**
- **clear isis stats error-counters**
- **clear isis stats packet-counters**

### Command Parameters

#### **error-counters**

Clears the IS-IS stats error-counters.

#### **packet-counters**

Clears the IS-IS stats packet-counters.

### Default

None

### Command Mode

Privileged EXEC



## clear khi

---

Clear the key health indicators for CPP port statistics or management instance statistics information.

### Syntax

- **clear khi cpp port-statistics**
- **clear khi mgmt statistics**

### Command Parameters

#### **cpp port-statistics**

Clears statistics for control packets that go to the control processor.

#### **mgmt statistics**

Clears statistics for control packets that go to the segmented management instance.

### Default

None

### Command Mode

Privileged EXEC

### Usage Guidelines

The *mgmt statistics* parameter is not supported on VSP 8600 Series.

## clear lacp

---

Clear link aggregation information and statistics.

### Syntax

- **clear lacp link-aggregate <1-512>**
- **clear lacp stats**
- **clear lacp stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

#### **link-aggregate <1-512>**

Specifies the MLT ID.

#### **port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**stats**

Clears lacp stats.

## Default

None

## Command Mode

Privileged EXEC

---

## clear link-debounce stats

Clear Link Debounce statistics on all ports.

## Syntax

- **clear link-debounce stats**

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## clear link-debounce stats port

Clear Link Debounce statistics on specific ports.

## Syntax

- **clear link-debounce stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## clear lldp

---

Clear Link Layer Discovery Protocol (LLDP) information.

## Syntax

- **clear lldp stats**
- **clear lldp stats summary**
- **clear lldp stats {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

### stats

Clears LLDP statistics.

### summary

Clears LLDP global statistics.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## clear logging

---

Clear the log file.

## Syntax

- **clear logging**

## Default

None

## Command Mode

Privileged EXEC

## clear mac-address-table

---

Clear the entries in the MAC address table.

## Syntax

- **clear mac-address-table port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} address WORD<17-17>**
- **clear mac-address-table port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} address WORD<17-17> interface vlan <1-4059>**

## Command Parameters

**address WORD<17-17>**

Specifies the MAC address.

**interface vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## clear mgmt statistics

---

Reset the statistics counters for a Segmented Management Instance.

## Syntax

- **clear mgmt statistics**

## Command Parameters

None

## Default

None

## Command Mode

Privileged EXEC

## clear mlt

---

Clear interswitch trunking (IST) statistics.

## Syntax

- **clear mlt ist stats**

## Default

None

## Command Mode

Privileged EXEC

## clear qos

---

Clear quality of service (QoS) information.

### Syntax

- **clear qos cosq-stats**
- **clear qos cosq-stats cpu-port**
- **clear qos cosq-stats interface**
- **clear qos cosq-stats interface {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **clear qos statistics policy**
- **clear qos statistics policy <1-16000>**
- **clear qos statistics policy slot {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

<1-16000>

Specifies a policy ID.

**cosq-stats**

Clear qos cos queue statistics

**cosq-stats cpu-port**

Clear Qos Cosq Stats on cpu port.

**cosq-stats interface**

Clear Qos Cosq Stats on port.

**cosq-stats interface {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Clear Qos Cosq Stats on port for the specified gigabit address.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

## Command Mode

Privileged EXEC

---

## clear qos cosq-stats

---

Clear qos cos queue statistics.

### Syntax

- **clear qos cosq-stats**
- **clear qos cosq-stats cpu-port**
- **clear qos cosq-stats interface**
- **clear qos cosq-stats interface {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **clear qos cosq-stats logical-intf**
- **clear qos cosq-stats logical intf isis <1-255>**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**isis <1-255>**

Clears the statistics for the specified logical interface.

### Default

None

### Command Mode

Privileged EXEC

---

## clear radius statistics

---

Clear server statistics.

### Syntax

- **clear radius statistics**

### Default

None

## Command Mode

Privileged EXEC

## clear sflow statistics

---

Clear sFlow statistics.

### Syntax

- **clear sflow statistics**
- **clear sflow statistics collector <1-2>**

### Command Parameters

**collector <1-2>**

Clear the sFlow statistics for the specified collector.

### Default

None

## Command Mode

Privileged EXEC

## clear slpp

---

Clear SLPP Information.

### Syntax

- **clear slpp stats**
- **clear slpp stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

**stats**

Clear SLPP Stats.

**stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Clear SLPP Stats for the specified port.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



## Default

None

## Command Mode

Privileged EXEC

## clear slpp stats

---

Clear slpp statistics.

## Syntax

- **clear slpp stats**

## Default

None

## Command Mode

Privileged EXEC

## Clear spoof-detect

---

Clear blocked MAC addresses by spoof detect.

## Syntax

- **clear spoof-detect blocked-mac 0x00:0x00:0x00:0x00:0x00:0x00**

## Command Parameters

**blocked-mac 0x00:0x00:0x00:0x00:0x00:0x00**

Clears blocked MAC addresses by spoof detect.

## Default

None

## Command Mode

Privileged EXEC

## clear ssh

---

Clear the SSH session.

## Syntax

- **clear ssh <0-7>**

## Command Parameters

<0-7>

Specifies the session ID.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to VSP 8600 Series.

## clear telnet

---

Close open Telnet sessions.

## Syntax

- **clear telnet <0-7>**

## Command Parameters

<0-7>

Specifies the Telnet session ID to close.

## Default

None

## Command Mode

Privileged EXEC

## clear trace

---

Clear the trace file.

## Syntax

- **clear trace**

## Default

None

## Command Mode

Privileged EXEC

---

## clear virtual-ist stats

Clear stats for vIST.

## Syntax

- **clear virtual-ist stats**

## Default

None

## Command Mode

Privileged EXEC

---

## clear vlacp

Clears Virtual Link Aggregation Control Protocol (VLACP) information on the switch.

## Syntax

- **clear vlacp flap-stats**
- **clear vlacp flap-stats port**{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **clear vlacp stats**
- **clear vlacp stats port**{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

## Command Parameters

**flap-stats port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Clears the VLACP Flap Detect and Damping statistics for the VLACP ports.

**stats port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Clears the VLACP information for the specific port.

## Default

None.

## Command Mode

Privileged EXEC

## configure

---

Log on to Global Configuration mode.

## Syntax

- **configure**
- **configure network**
- **configure network address {A.B.C.D}**
- **configure network address {A.B.C.D} filename WORD<1-239>**
- **configure network filename WORD<1-239>**
- **configure network filename WORD<1-239> address {A.B.C.D}**
- **configure terminal**

## Command Parameters

### network

Configures the device from a TFTP network host.

### network address {A.B.C.D} filename WORD<1-239>

Specifies an address of the TFTP server.

### network filename WORD<1-239> address {A.B.C.D}

Specifies the filename of the configuration file.

### terminal

Configures the device from a terminal.

## Default

None

## Command Mode

Privileged EXEC

---

## copy

---

Copy files as part of an upgrade procedure to back up files or to move files to another location.

### Syntax

- **copy clilog WORD<1-255>**
- **copy running-config startup-config**
- **copy WORD<1-255> WORD<1-255>**
- **copy WORD<1-255> WORD<1-255> -y**

### Command Parameters

**clilog WORD<1-255>**

Copies the log file to a specific location. You can specify the name and location for the log file in one of the following formats: a.b.c.d:<file>, /intflash/<file>, and /usb/<file>.

**running-config startup-config**

Copies running and start-up configuration.

**WORD<1-255> WORD<1-255>**

Source filename, a.b.c.d:<file> | /intflash/<file> | /usb/<file>.

**-y**

Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action before the switch copies the file.

### Default

None

### Command Mode

Privileged EXEC

---

## cp

---

Use this command to copy files.

### Syntax

- **cp WORD<1-255> WORD<1-255>**
- **cp WORD<1-255> WORD<1-255> -y**

### Command Parameters

**WORD <1-255> WORD <1-255>**

The first WORD<1-255> specifies the file to copy. The second WORD<1-255> uses one of the following formats: /intflash/ <file> . Word<1-255> is a string of 1-255 characters.

**-y**

Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action before the switch copies the file.

## Default

None

## Command Mode

Privileged EXEC

## delete

---

Use this command to delete files.

## Syntax

- **delete WORD<1-255>**
- **delete WORD<1-255> -y**

## Command Parameters

**WORD<1-255>**

Specifies the name and location of the file to delete in the following formats: /intflash/<file>, and /usb/<file>. WORD<1-255> is a string of 1-255 characters.

**WORD<1-255> -y**

Remove file or directory, with wildcard pattern.

**-y**

Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action before the switch deletes the file.

## Default

None

## Command Mode

Privileged EXEC

## dir

---

View the free space and files in flash memory.

## Syntax

- **dir**
- **dir -l**
- **dir -r**
- **dir WORD<1-99>**

## Command Parameters

- l  
Details, dir -l [-r]
- r  
Recursive, dir -r
- WORD<1-99>  
Directory path name, dir <path> [-l] [-r]

## Default

None

## Command Mode

Privileged EXEC

## disable

---

Turns off privileged commands and returns you to the User Exec prompt.

## Syntax

- **disable**
- **disable <0-15>**

## Command Parameters

- <0-15>  
Privilege level to go to.

## Default

None

## Command Mode

Privileged EXEC

## dos-chkdisk

---

Check MS DOS file system for any inconsistencies. If at the end of the output for the dos-chkdisk WORD<1-99> you see: 1) Correct 2) Don't correct, then run the dos-chkdisk WORD<1-99> repair command.

### Syntax

- **dos-chkdisk WORD<1-99>**
- **dos-chkdisk WORD<1-99> repair**

### Command Parameters

**WORD<1-99>**

Specifies the device name to repair.

**WORD<1-99> repair**

Repairs the errors found.

### Default

None

### Command Mode

Privileged EXEC

## dos-format

---

Format the external flash or USB.

### Syntax

- **dos-format WORD<1-99>**

### Command Parameters

**WORD<1-99>**

Specifies the device name to format.

### Default

None

### Command Mode

Privileged EXEC



---

## editing

---

Simple vi line editor to modify script files

### Syntax

- **editing WORD<1-99>**

### Command Parameters

WORD<1-99>

Device name, /intflash.

### Default

None

### Command Mode

Privileged EXEC

---

## energy-saver

---

Activates Energy Saver manually on the switch.

### Syntax

- **energy-saver activate**
- **energy-saver deactivate**

### Command Parameters

**activate**

Activates Energy Saver manually on the switch.

**deactivate**

Deactivates Energy Saver manually on the switch.

### Default

Deactivated

### Command Mode

Privileged EXEC

---

## extend-time-period

---

Extends the 30-day Factory Default Premier Trial License period on your switch. You can run this command up to three times to extend the evaluation license in 30-day increments for an additional 90 days.

### Syntax

- **extend-time-period**

### Default

None

### Command Mode

Privileged EXEC

---

## flight-recorder

---

Perform various functions on the flight recorder data on the switch.

### Syntax

- **flight-recorder all {slot [-slot][,...]}**
- **flight-recorder archive {slot [-slot][,...]}**
- **flight-recorder snapshot {slot [-slot][,...]}**
- **flight-recorder trace {slot [-slot][,...]}**

### Command Parameters

**all {slot [-slot][,...]}**

Creates flight recorder snapshot, trace, and archive. {slot [-slot][,...]} specifies the slot number. Valid slot is 1.

**archive {slot [-slot][,...]}**

Creates tarball of flight recorder files, log files, config file and others. {slot [-slot][,...]} specifies the slot number.

**snapshot {slot [-slot][,...]}**

Takes the snapshot of flight recorder PMEM data. {slot [-slot][,...]} specifies the slot number.

**trace {slot [-slot][,...]}**

Takes the snapshot of always-on-trace data. {slot [-slot][,...]} specifies the slot number.

### Default

None

## Command Mode

Privileged EXEC

## grep

---

Use this Unix command to search files for lines that match a given expression.

## Syntax

- **grep error WORD<1-99>**
- **grep WORD<0-1536> WORD<1-99>**

## Command Parameters

**error WORD <1-99>**

Searches for an error in a file. WORD<1-99> specifies a filename, /intflash/<file>.

**WORD<0-1536> WORD<1-99>**

Searches files for lines that match a given expression. WORD<0-1536> specifies the string to match.

## Default

None

## Command Mode

Privileged EXEC

## maintenance system-action

---

Displays the system action.

## Syntax

- **maintenance system-action WORD<1-99> execute WORD<1-99>**
- **maintenance system-action WORD<1-99> execute WORD<1-99> WORD<0-99>**

## Default

None

## Command Mode

Privileged EXEC

## mkdir

---

Make directory on filesystem.

### Syntax

- **mkdir WORD<1-99>**

### Command Parameters

WORD<1-99>

Directory path name.

### Default

None

### Command Mode

Privileged EXEC

## monitor ip mroute stats

---

Monitor IP multicast route statistics.

### Syntax

- **monitor ip mroute stats [WORD<7-160> {A.B.C.D[,E.F.G.H][,...]}]**

### Command Parameters

WORD<7-160> {A.B.C.D[,E.F.G.H][,...]}

Monitor IP multicast route statistics.

### Default

None

### Command Mode

Privileged EXEC

## monitor ip vrrp statistics

---

Display IP multicast statistics for the Virtual Router Redundancy Protocol (VRRP).

## Syntax

- **monitor ip vrrp statistics gigabitethernet**
- **monitor ip vrrp statistics gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**
- **monitor ip vrrp statistics gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} verbose**
- **monitor ip vrrp statistics gigabitethernet verbose**

## Command Parameters

**gigabitethernet** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### verbose

Specifies the complete list of configuration information.

## Default

None

## Command Mode

Privileged EXEC

## monitor ipv6 mroute stats

---

Monitor Ipv6 multicast route statistics.

## Syntax

- **monitor ipv6 mroute stats [WORD<7-400> {Ipv6address[,Ipv6address] [,...]}]**

## Command Parameters

**WORD<7-400>** {*Ipv6address[,Ipv6address][,...]*}

Monitor IPv6 multicast route statistics.

## Default

None

## Command Mode

Privileged EXEC

## monitor mlt error collision

---

Monitor MultiLink Trunking (MLT) collision error information.

### Syntax

- **monitor mlt error collision**
- **monitor mlt error collision <1-512>**

### Command Parameters

<1-512>

Specifies the MLT ID.

### Default

None

## Command Mode

Privileged EXEC

## monitor mlt error main

---

Monitor MultiLink Trunking (MLT) general error information.

### Syntax

- **monitor mlt error main**
- **monitor mlt error main <1-512>**

### Command Parameters

<1-512>

Specifies the MLT ID.

### Default

None

## Command Mode

Privileged EXEC

## monitor mlt stats interface main

---

Show MultiLink Trunking (MLT) interface statistics.

### Syntax

- **monitor mlt stats interface main**
- **monitor mlt stats interface main <1-512>**

### Command Parameters

<1-512>

Specifies the MLT ID.

### Default

None

### Command Mode

Privileged EXEC

## monitor mlt stats interface utilization

---

Show MultiLink Trunking (MLT) interface statistics utilization.

### Syntax

- **monitor mlt stats interface utilization**
- **monitor mlt stats interface utilization <1-512>**

### Command Parameters

<1-512>

Specifies the MLT ID.

### Default

None

### Command Mode

Privileged EXEC

## monitor ports error

---

Monitor port error information.

### Syntax

- `monitor ports error {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} collision`
- `monitor ports error {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} collision from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports error {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} main`
- `monitor ports error {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} main from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports error {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} ospf`
- `monitor ports error {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} ospf from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports error {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} verbose`
- `monitor ports error {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} verbose from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports error collision`
- `monitor ports error collision from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports error main`
- `monitor ports error main from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports error ospf`
- `monitor ports error ospf from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports error verbose`
- `monitor ports error verbose from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

### Command Parameters

`{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



**collision**

Monitors port collision error information.

**main**

Monitors port general error information.

**ospf**

Monitors ports general Open Shortest Path First (OSPF) information.

**verbose**

Monitors port extended error information.

**verbose**

Monitors port extended error information on a particular slot and port or particular slots and ports.

## Default

None

## Command Mode

Privileged EXEC

## monitor ports statistics

Monitor port statistics.

## Syntax

- **monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} bridging**
- **monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} bridging from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} dhcp-relay**
- **monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} dhcp-relay from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} interface**
- **monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} interface main from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} interface utilization**

- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} interface utilization from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} interface verbose`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} interface verbose from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} ospf main`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} ospf main from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} ospf verbose`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} ospf verbose from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} rmon`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} rmon from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} routing`
- `monitor ports statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} routing from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

## Command Parameters

`{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### bridging

Monitor port bridging statistics.

### dhcp-relay

Monitors port DHCP-relay statistics.

`from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`

Monitors port statistics from a particular starting point.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### interface

Monitor port interface statistics.

#### ospf

Monitor ports statistics for open shortest path first (OSPF) performance.

#### rmon

Monitor port remote monitoring (RMON) statistics.

#### routing

Monitor port Dynamic Host Configuration Protocol (DHCP) routing statistics.

#### verbose

Provides additional information when used with a command.

## Default

None

## Command Mode

Privileged EXEC

## monitor ports statistics bridging

---

Monitor port bridging statistics.

## Syntax

- **monitor ports statistics bridging**
- **monitor ports statistics bridging from {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**from** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Monitors port bridging statistics.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## monitor ports statistics dhcp-relay

---

Monitor port dhcp-relay statistics.

### Syntax

- **monitor ports statistics dhcp-relay**
- **monitor ports statistics dhcp-relay from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

**from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Monitors port bridging statistics from a particular starting port.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

## Command Mode

Privileged EXEC

## monitor ports statistics interface

---

Monitor port interface statistics.

### Syntax

- **monitor ports statistics interface main**
- **monitor ports statistics interface main from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **monitor ports statistics interface utilization**
- **monitor ports statistics interface utilization from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **monitor ports statistics interface verbose**
- **monitor ports statistics interface verbose from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**from** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Monitors port DHCP-relay statistics.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**main**

Monitors port interface statistics.

**utilization**

Monitors port interface utilization statistics.

**utilization from** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Monitors port DHCP-relay statistics from a particular starting port.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**verbose**

Monitors port interface statistics.

**verbose from** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Specifies the slot and port.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## monitor ports statistics ospf

Monitor ports statistics for open shortest path first (OSPF) performance.

## Syntax

- **monitor ports statistics ospf main**
- **monitor ports statistics ospf main from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **monitor ports statistics ospf verbose**
- **monitor ports statistics ospf verbose from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

### main

Monitors ports statistics for OSPF main command.

**main from** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Monitors port interface statistics.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### verbose

Monitors ports statistics for OSPF verbose command.

**verbose from** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Monitors port interface statistics from a particular starting port.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## monitor ports statistics rmon

Monitor port remote monitoring (RMON) statistics.

## Syntax

- **monitor ports statistics rmon**

- **monitor ports statistics rmon from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**from** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Monitors port interface utilization statistics.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## monitor ports statistics routing

---

Monitor port Dynamic Host Configuration Protocol (DHCP) routing statistics.

## Syntax

- **monitor ports statistics routing**
- **monitor ports statistics routing from {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**from** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Monitors port interface utilization statistics from a particular starting port.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## more

---

Display contents of file.

## Syntax

- **more WORD<1-99>**
- **more WORD<1-99> { binary | ascii }**

## Command Parameters

{ binary | ascii }

Filename, a.b.c.d:<file> | /intflash/<file> | /usb/<file>.

WORD<1-99>

Specifies the file name in the following format: /usb/<file>. The file name, including the directory structure, can include up to 99 characters.

## Default

None

## Command Mode

Privileged EXEC

## mv

---

Move or rename file or directory, with wildcard pattern.

## Syntax

- **mv /intflash/<srcfile> /usb/<destfile>**
- **mv WORD<1-255> WORD<1-255>**

## Command Parameters

/intflash/<srcfile>

Specifies the name of the configuration or log file on the internal flash memory. For example, test.cfg or test.log. The file name, including the directory structure, can include up to 255 characters.

/usb/<destfile>



Specifies the name of the configuration or log file when moved to the USB device. The destination file name must be lower case and have a file extension of .cfg or .log. For example, test.cfg or test.log. The file name, including the directory structure, can include up to 255 characters.

**WORD<1-255> WORD<1-255>**

Filename, /intflash/<file> | /usb/<file>.

## Default

None

## Command Mode

Privileged EXEC

## pwd

---

Print current filesystem directory path.

## Syntax

- **pwd**

## Default

None

## Command Mode

Privileged EXEC

## rename

---

Use this command to rename a file.

## Syntax

- **rename WORD<1-255> WORD<1-255>**

## Command Parameters

**WORD<1-255> WORD<1-255>**

Specifies the file name to rename in the following format: /intflash/ <file> or /usb/<file>. Word<1-255> is a string of 1-255 characters.

## Default

None

## Command Mode

Privileged EXEC

---

## reset

Reset the platform to reload system parameters from the most recently saved configuration file.

## Syntax

- **reset**
- **reset [-y] [-coredump]**
- **reset -coredump**
- **reset -y**

## Command Parameters

**-coredump**

Creates an ssio core file and a cbcpr-main.x core file before resetting the switch.

**-y**

Suppresses the confirmation message before the switch resets. If you omit this parameter, you must confirm the action before the switch resets.

## Default

None

## Command Mode

Privileged EXEC

---

## restore

Restore the internal flash from the USB device or restore configuration files stored in a backup zip file. You must disable logging to the compact flash you want to restore before you can use the restore command.

## Syntax

- **restore configure WORD<1-99>**
- **restore intflash**

## Command Parameters

**configure WORD<1-99>**

Specifies the backup configuration files to be restored.

**intflash**

Specifies the internal flash to be restored from the USB device.

## Default

None

## Command Mode

Privileged EXEC

## rlogin

---

Login remotely to a remote host.

## Syntax

- **rlogin {A.B.C.D}**

## Command Parameters

**{A.B.C.D}**

Specifies the IP address.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## rsh

---

Execute a shell command on a remote machine.

## Syntax

- **rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536>**
- **rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536>**
- **rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536>**
- **rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>**
- **rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>**
- **rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>**
- **rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>**
- **rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>**

## Command Parameters

**{A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>**

Specifies the command to execute on the remote host: Param1 for rsh command. String length {0-1536} Param2 for rsh command. String length {0-1536} Param3 for rsh command. String length {0-1536} Param4 for rsh command. String length {0-1536} Param5 for rsh command. String length {0-1536} Param6 for rsh command. String length {0-1536} Param7 for rsh command. String length {0-1536}

**{A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>**

Specifies the user login name.

**{A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>**

Specifies the IP address in the {A.B.C.D} format.

**-l**

Specifies the user login name.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## save config

---

Save configuration information.

### Syntax

- **save config**
- **save config backup WORD<1-99>**
- **save config file WORD<1-99>**
- **save config file WORD<1-99> verbose**
- **save config verbose**

### Command Parameters

**backup WORD<1-99>**

Saves the specified file name and identifies the file as a backup file.

**file WORD<1-99>**

Specifies the file name.

**verbose**

Save current and default configuration.

### Default

None

### Command Mode

Privileged EXEC

## save log

---

Save the log files, assuming the files use the default file names.

### Syntax

- **save log**
- **save log file WORD<1-99>**

## Command Parameters

**file WORD<1-99>**

Specifies the file name in one of the following formats: a.b.c.d: <file>, or /intflash/ <file>.  
WORD<1-99> is a string of 1-99 characters.

## Default

None

## Command Mode

Privileged EXEC

---

## save trace

Save the trace file to the card for retrieval.

## Syntax

- **save trace**
- **save trace file WORD<1-99>**

## Command Parameters

**file WORD<1-99>**

Specifies the file name in one of the following formats: a.b.c.d: <file>, or /intflash/ <file> .

## Default

None

## Command Mode

Privileged EXEC

---

## show access-policy

Show access policy configurations.

## Syntax

- **show access-policy**
- **show access-policy by-mac**
- **show access-policy snmp-group**
- **show access-policy WORD<0-15>**

## Command Parameters

### **by-mac**

Show access policy by-mac information.

### **snmp-group**

Show access-policy snmp-group information.

### **WORD<0-15>**

Specifies an access policy name.

## Default

None

## Command Mode

Privileged EXEC

## show alarm

---

Display the contents of the alarm log buffers.

## Syntax

- **show alarm database**
- **show alarm database alarm-id WORD<0-32>**
- **show alarm database alarm-status WORD<0-32>**
- **show alarm database alarm-type WORD<0-32>**
- **show alarm database event-code <0x0-0x00FFFFFF | 0x0-0x0>**
- **show alarm database module WORD<0-100>**
- **show alarm database severity WORD<0-25>**
- **show alarm statistics**

## Command Parameters

### **database**

Shows the alarm database.

### **database alarm-id WORD<0-32>**

Shows the alarms associated with alarm ID.

### **database alarm-status WORD<0-32>**

Shows the alarms associated with alarm status

### **database alarm-type WORD<0-32>**

Shows the alarms associated with type.

### **database event-code <0x0-0x00FFFFFF | 0x0-0x0>**

Shows the alarms associated with event code.

**database module WORD<0-100>**

Shows the alarms associated with module.

**database severity WORD<0-25>**

Shows the alarms associated with severity.

**statistics**

Shows the alarm database statistics.

## Default

None

## Command Mode

Privileged EXEC

---

## show boot config choice

Make copies of the configuration files before you upgrade the switch software.

## Syntax

- **show boot config choice**

## Default

None

## Command Mode

Privileged EXEC

---

## show boot config flags

Check the status of the boot configuration flags.

## Syntax

- **show boot config flags**

## Default

None



## Command Mode

Privileged EXEC

## Command Output

The **show boot config flags** command displays the following information:

Output field	Description
flags advanced-feature-bandwidth-reservation	Shows if the switch supports advanced features by reserving ports as loopback ports. If enabled, the value is low. If disabled, the value is false.
flags block-snmp	Shows if the switch permits Simple Network Management Protocol (SNMP) access. If enabled, the value is true. If disabled, the value is false.
flags debug-config	Shows if the switch can debug the configuration file while loading the configuration at system boot up. If disabled, the value is false. If enabled, the value shows if the debug information will be stored in a file or displayed on the console.
flags debugmode	Shows if you can enable TRACE on any port by prompting the selection on the console during boot up. If enabled, the value is true. If disabled, the value is false.
flags dvr-leaf-mode	Shows if you can configure the switch as a DvR Leaf. If enabled, the value is true. If disabled, the value is false.
flags enhancedsecure-mode	Shows if the switch operates in enhanced secure mode. If disabled, the value is false. If enabled, the value indicates either the JITC or non-JITC sub-mode.
flags factorydefaults	Shows whether the switch uses the fabric or non-fabric factory default settings at startup. If enabled, the value is true. If disabled, the value is false.
flags flow-control-mode	Shows if flow control is enabled globally. If enabled, the value is true. If disabled, the value is false.
flags ftpd	Shows if the FTP server is enabled on the switch. If enabled, the value is true. If disabled, the value is false.
flags ha-cpu	Shows if the switch operates in High Availability-CPU (HA-CPU) mode. If enabled, the value is true. If disabled, the value is false.
flags hsecure	Shows if the switch operates in High Secure mode. If enabled, the value is true. If disabled, the value is false.
flags ipv6-egress-filter	Shows if IPv6 egress filters are enabled on the switch. If enabled, the value is true. If disabled, the value is false.
flags ipv6-mode	Shows if IPv6 mode is enabled on the switch. If enabled, the value is true. If disabled, the value is false.
flags linerate-directed-broadcast	Shows if the switch supports IP Directed Broadcast in hardware without requiring CPU intervention. If enabled, the value is true. If disabled, the value is false.
flags logging	Shows if system logging is enabled on the switch. If enabled, the value is true. If disabled, the value is false.

Output field	Description
flags macsec	Shows macsec enabled globally if you configure the boot config flag on the switch. If disabled, the value is false.
flags nni-mstp	Shows if you can configure MSTP and VLANs on NNI ports. If enabled, the value is true. If disabled, the value is false.
flags reboot	Shows if the switch automatically reboots after a fatal error. If enabled, the value is true. If disabled, the value is false.
flags rlogind	Shows if the rlogin and rsh server is enabled on the switch. If enabled, the value is true. If disabled, the value is false.
flags savetostandby	Shows if the switch automatically saves the configuration file to the standby CPU. If enabled, the value is true. If disabled, the value is false.
flags spanning-tree-mode	Shows the Spanning Tree mode enabled on the switch.
flags spbm-config-mode	Shows if you can configure SPB and IS-IS on the switch. If enabled, the value is true. If disabled, the value is false.
flags sshd	Shows if the SSHv2 server is enabled on the switch. If enabled, the value is true. If disabled, the value is false.
flags syslog-rfc5424-format	Shows if the format of the syslog and logging outputs conform to RFC 5424. If enabled, the value is true. If disabled, the value is false.
flags telnetd	Shows if the Telnet server is enabled on the switch. If enabled, the value is true. If disabled, the value is false.
flags tftpd	Shows if the Trivial File Transfer Protocol server is enabled on the switch. If enabled, the value is true. If disabled, the value is false.
flags trace-logging	Shows if the switch creates trace logs. If enabled, the value is true. If disabled, the value is false.
flags urpf-mode	Shows if Unicast Reverse Path Forwarding (uRPF) is enabled globally. If enabled, the value is true. If disabled, the value is false.
flags verify-config	Shows if syntax checking of the configuration file is enabled on the switch. If enabled, the value is true. If disabled, the value is false.
flags vrf-scaling	Shows if the switch can support an increased number of VRFs and Layer 3 VSNS. If enabled, the value is true. If disabled, the value is false.
flags vxlan-gw-full-interworking-mode	Shows if VXLAN Gateway is enabled in Full Interworking Mode, If enabled, the value is true. If VXLAN Gateway operates in Base Interworking mode, the value is false.

## Example

The following example displays a configuration for each flag.



### Note

Flags displayed vary across hardware models..

```
Switch:1#show boot config flags
flags advanced-feature-bandwidth-reservation low
flags block-snmp false
```

```
flags debug-config false
flags debugmode false
flags dvr-leaf-mode false
flags enhancedsecure-mode false
flags factorydefaults false
flags flow-control-mode true
flags ftpd true
flags ha-cpu true
flags hsecure false
flags ipv6-egress-filter true
flags ipv6-mode false
flags linerate-directed-broadcast false
flags logging true
flags macsec false
flags nni-mstp false
flags reboot true
flags rlogind false
flags savetostandby true
flags spanning-tree-mode mstp
flags spbm-config-mode true
flags sshd true
flags syslog-rfc5424-format true
flags telnetd true
flags tftpd true
flags trace-logging false
flags urpf-mode true
flags verify-config true
flags vrf-scaling true
flags vxlan-gw-full-interworking-mode false
```

---

## show boot config general

Displays system information.

### Syntax

- **show boot config general**

### Default

None

### Command Mode

Privileged EXEC

---

## show boot config host

Display the current host configuration.

### Syntax

- **show boot config host**

## Default

None

## Command Mode

Privileged EXEC

# show boot config running-config

---

Displays the current boot configuration.

## Syntax

- **show boot config running-config [verbose]**

## Command Parameters

### verbose

Includes all possible information. If you omit verbose, the system displays only the values that you changed from their default value.

## Default

None

## Command Mode

Privileged EXEC

# show boot config sio

---

Displays serial port information.

## Syntax

- **show boot config sio**
- **show boot config sio {<1-8> | SF1 | SF2 | SF3}**

## Command Parameters

**sio {<1-8> | SF1 | SF2 | SF3}**

Specifies the current configuration of the serial port.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

The choice of slot, <1-8> | *SF1* | *SF2* | *SF3*, applies only to VSP 8600 Series.

## show eapol multihost-session-stats interface

---

Display the manage mode parameters for the specified interface type.

## Syntax

- **show eapol multihost-session-stats interface**
- **show eapol multihost-session-stats interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show eapol multihost-session-stats interface vlan <1-4059>**
- **show eapol multihost-session-stats interface vlan <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**gigabitEthernet** {*slot/port[/sub-port] [-slot/port[/sub-port]] [,...]*}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show eapol session interface

---

View EAPoL session statistics to manage network performance.

## Syntax

- **show eapol session interface** [**gigabitethernet** {**slot/port**[/**sub-port**]} [-**slot/port**[/**sub-port**]] [, ...]] [**vlan** <1-4059>]

## Command Parameters

**gigabitethernet** {*slot/port*[/*sub-port*] [-*slot/port*[/*sub-port*]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show eapol summary

---

Display the total number of EAP and NEAP clients without having to display all clients.

## Syntax

- **show eapol summary** {{**slot/port**[/**sub-port**]} [-**slot/port**[/**sub-port**]] [, ...]}
- **show eapol summary verbose**

## Command Parameters

{*slot/port*[/*sub-port*] [-*slot/port*[/*sub-port*]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**verbose**

Displays extended eapol summary information.

## Default

None

## Command Mode

Privileged EXEC

## show energy-saver

---

Displays Energy Saver settings and status on the switch.

## Syntax

- **show energy-saver global**
- **show energy-saver interface** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **show energy-saver savings**
- **show energy-saver schedule**

## Command Parameters

### global

Displays global Energy Saver settings on the switch.

**interface** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Displays per-port Energy Saver settings and status on the switch.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### savings

Displays Energy Saver power savings on the switch.

### schedule

Displays information about Energy SaverEnergy Saver schedules configured on the switch.

## Default

None

## Command Mode

Privileged EXEC

---

## show filter acl

---

Display filter access control list (ACL) configuration information.

### Syntax

- **show filter acl**
- **show filter acl <acl-id>**

### Command Parameters

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

### Default

None

### Command Mode

Privileged EXEC

---

## show filter acl policer

---

Display the filter access control list (ACL) policer configuration information.

### Syntax

- **show filter acl policer <acl-id> <ace-id>**

### Command Parameters

*policer*

Specifies the policer for the flow of traffic in the switch.

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

### Default

None



## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show filter acl ace

---

Display the filter access control list (ACL) access control entry (ACE) configuration information.

## Syntax

- **show filter acl ace**
- **show filter acl ace <acl-id>**
- **show filter acl ace <acl-id> <ace-id>**

## Command Parameters

<ace-id>

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

<acl-id>

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Privileged EXEC

## show filter acl action

---

Display the filter access control list (ACL) advanced information.

## Syntax

- **show filter acl action**
- **show filter acl action <acl-id>**
- **show filter acl action <acl-id> <ace-id>**

## Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Privileged EXEC

## show filter acl arp

---

Display the filter access control list (ACL) ARP operation configuration information.

## Syntax

- **show filter acl arp**
- **show filter acl arp <acl-id>**
- **show filter acl arp <acl-id> <ace-id>**

## Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Privileged EXEC

---

## show filter acl config

---

Review your configuration to ensure that it is correct.

### Syntax

- **show filter acl config**
- **show filter acl config <acl-id>**
- **show filter acl config <acl-id> <ace-id>**

### Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

### Default

None

### Command Mode

Privileged EXEC

---

## show filter acl ethernet

---

Display the filter access control list (ACL) Ethernet configuration information.

### Syntax

- **show filter acl ethernet**
- **show filter acl ethernet <acl-id>**
- **show filter acl ethernet <acl-id> <ace-id>**

### Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Privileged EXEC

## show filter acl ip

---

Display the filter access control list (ACL) IP configuration information.

## Syntax

- **show filter acl ip**
- **show filter acl ip <acl-id>**
- **show filter acl ip <acl-id> <ace-id>**

## Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Privileged EXEC

## show filter acl ipv6

---

Display the filter access control list (ACL) IPv6 configuration information.

## Syntax

- **show filter acl ipv6**
- **show filter acl ipv6 <acl-id>**
- **show filter acl ipv6 <acl-id> <ace-id>**

## Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Privileged EXEC

## show filter acl protocol

---

Display the filter access control list (ACL) protocol configuration information.

## Syntax

- **show filter acl protocol**
- **show filter acl protocol <acl-id>**
- **show filter acl protocol <acl-id> <ace-id>**

## Command Parameters

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

## Default

None

## Command Mode

Privileged EXEC

---

## show filter acl statistics

---

View port statistics to ensure that the access control entry (ACE) operates correctly.

### Syntax

- **show filter acl statistics**
- **show filter acl statistics <acl-id>**
- **show filter acl statistics <acl-id> <ace-id>**
- **show filter acl statistics <acl-id> policer**
- **show filter acl statistics <acl-id> <ace-id>policer**
- **show filter acl statistics <acl-id> qos**
- **show filter acl statistics <acl-id> security**
- **show filter acl statistics all**
- **show filter acl statistics default**
- **show filter acl statistics default <acl-id>**
- **show filter acl statistics default <acl-id> policer**
- **show filter acl statistics default <acl-id> policer**
- **show filter acl statistics default <acl-id> policer**
- **show filter acl statistics global**
- **show filter acl statistics global <acl-id>**

### Command Parameters

#### security

Shows ACL statistics for Security ACEs

*<ace-id>*

Specifies the ACE ID. Different hardware platforms support different ACE ID ranges. Use the CLI Help to see the available range for the switch.

*<acl-id>*

Specifies the ACL ID. Use the CLI Help to see the available range for the switch.

#### all

Shows all statistics for all access control entry.

#### default

Shows traffic statistics for access control entry..

#### global

Shows global statistics for access control entry.

#### policer

Shows policer statistics for access control entry.

**qos**

Shows statistics for Quality of Service (QoS) access control entries.

**Default**

None

**Command Mode**

Privileged EXEC

**Command Output**

The **show filter acl statistics** command displays the following information:

Parameter	Description
Acl ID	Specifies the identifier for the ACL.
Acl Name	Specifies the name for the ACL.
Acl Type	Specifies the ACL type.
Acl Sec Packets	Specifies the ACL secondary packets.
Acl Sec Bytes	Specifies the ACL secondary bytes.
Acl QoS Packets	Specifies the ACL QoS packets.
Acl QoS Bytes	Specifies the ACL QoS bytes.

**Example****Note**

Based on your hardware platform, the output can display all the ACL packets or segregate them as QoS and security ACL packets.

```
Switch:1>enable
Switch:1#show filter acl statistics all
```

```
=====
                        Acl Global Statistics Table
=====
Acl Id  Acl Name   Acl Type  Acl Sec  Acl Sec  Acl QOS  Acl QOS  Acl   Acl
        Packets Bytes    Packets Bytes    Packets Bytes    Packets Bytes
-----
1       ACL-1      inVlan    0         0         0         0         0       0
2       ACL-2      inVlan    0         0         0         0         0       0

Displayed 2 of 2 entries
=====
                        Acl Default Statistics Table
=====
Acl Id  Acl Name   Acl Type  Acl Sec  Acl Sec  Acl QOS  Acl QOS  Acl   Acl
        Packets Bytes    Packets Bytes    Packets Bytes    Packets Bytes
-----
```

```

1      ACL-1      inVlan    0         0         0         0         0         0
2      ACL-2      inVlan    0         0         0         0         0         0

```

Displayed 2 of 2 entries

```
Switch:1#show filter acl statistics default
```

```

=====
                        Acl Default Statistics Table
=====
Acl Id  Acl Name    Acl Type  Acl Sec  Acl Sec  Acl QOS  Acl QOS  Acl    Acl
        Packets Bytes    Packets Bytes    Packets Bytes    Packets Bytes
-----
1      ACL-1      inVlan    0         0         0         0         0         0
2      ACL-2      inVlan    0         0         0         0         0         0

```

Displayed 2 of 2 entries

```
Switch:1#show filter acl statistics global 2
```

```

=====
                        Acl Global Statistics Table
=====
Acl Id  Acl Name    Acl Type  Acl Sec  Acl Sec  Acl QOS  Acl QOS  Acl    Acl
        Packets Bytes    Packets Bytes    Packets Bytes    Packets Bytes
-----
2      ACL-2      inVlan    0         0         0         0         0         0

```

Displayed 1 of 1 entries

## Usage Guidelines

The **show filter acl statistics <acl> <ace> policer** command displays statistics according to the configuration on the switch.

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show history

Shows a list of previously used commands. You can use this command in any mode, beginning with Privileged EXEC. The output shows the last 32 commands used in the active session.

### Syntax

- **show history**

### Default

None

### Command Mode

Privileged EXEC



## show interfaces gigabitEthernet

---

Show configuration information for GigabitEthernet ports.

### Syntax

- **show interfaces gigabitEthernet**
- **show interfaces gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show interfaces gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} <1-4059>**

### Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

Privileged EXEC

## show interfaces gigabitEthernet auto-sense

---

Displays the Auto-sense status and state on a port.

### Syntax

- **show interfaces gigabitEthernet auto-sense [<1-4059>] [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show interfaces gigabitethernet channelize

---

Display port-channelization information. Not all hardware platforms support this feature. For information about hardware support, see your hardware documentation.

## Syntax

- **show interfaces gigabitEthernet channelize**
- **show interfaces gigabitEthernet channelize {slot/port[-slot/port] [,...]}**
- **show interfaces gigabitEthernet channelize detail**
- **show interfaces gigabitEthernet channelize detail {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**[port {slot/port [-slot/port] [,...]}]**

Specifies a specific outgoing interface to use by IP address.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

#### detail

Display the detailed channelization information.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces gigabitEthernet config

Displays the configuration for specific ports such as port type, diff-serv, QoS level, MLT ID, and the Layer 3 trusted/untrusted information for a gigabitEthernet interface.

## Syntax

- **show interfaces gigabitEthernet config**
- **show interfaces gigabitEthernet config <1-4059>**
- **show interfaces gigabitEthernet config {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags,

the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

# show interfaces gigabitethernet error

---

Show general error information for the port.

## Syntax

- **show interfaces GigabitEthernet error** [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]
- **show interfaces GigabitEthernet error collision** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **show interfaces GigabitEthernet error ospf** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **show interfaces GigabitEthernet error verbose** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### collision

Show port collision error information.

### ospf

Show port ospf error information.

### verbose

Show port error information. Display priority-based flow control pause transmit and receive counter.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

On XA1400 Series, the command output for most columns shows values of zero (0). To see port-level error counters, use the **show io nic-counters** command instead. For more information, see [show io](#) on page 1198

## Command Output

The **show interfaces gigabitethernet error ospf** command displays the following information:

Output field	Description
PORT NUM	Indicates the port number.
VERSION MISMATCH	Indicates the number of version mismatches this interface receives.
AREA MISMATCH	Indicates the number of area mismatches this interface receives.
AUTHYPEMISMATCH	Indicates the number of AuthType mismatches this interface receives.
AUTH FAILURES	Indicates the number of authentication failures.
NET_MASK MISMATCH	Indicates the number of net mask mismatches this interface receives.
HELLOINT MISMATCH	Indicates the number of hello interval mismatches this interface receives.
DEADINT MISMATCH	Indicates the number of dead interval mismatches this interface receives.
OPTION MISMATCH	Indicates the number of options mismatches this interface receives.

## show interfaces gigabitethernet fdb-entry

Show the forwarding database (FDB) entries for the port.

### Syntax

- **show interfaces gigabitEthernet fdb-entry**
- **show interfaces gigabitEthernet fdb-entry <1-4059>**
- **show interfaces gigabitEthernet fdb-entry {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

# show interfaces gigabitethernet high-secure

---

Show the high-secure configuration for the port.

## Syntax

- **show interfaces gigabitethernet high-secure**
- **show interfaces gigabitEthernet high-secure {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} <1-4059>**
- **show interfaces gigabitethernet high-secure <1-4059>**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

---

## show interfaces gigabitEthernet interface

---

Show general port information.

## Syntax

- **show interfaces gigabitEthernet interface**
- **show interfaces gigabitEthernet interface <1-4059>**
- **show interfaces gigabitEthernet interface {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} <1-4059>**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

---

## show interfaces gigabitEthernet i-sid

---

Display all configured service instance identifiers (I-SID) on port.

## Syntax

- **show interfaces gigabitEthernet i-sid {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show interfaces gigabitEthernet i-sid** command displays the following information:

Output field	Description
PORTNUM	Specifies the port number.
IFINDEX	Specifies a value that uniquely identifies the port.
ISID ID	Specifies the service interface identifier (I-SID).
VLANID	Specifies the backbone VLAN.
C-VID	Specifies the customer VLAN ID.
ISID TYPE	Specifies the type of I-SID.
ORIGIN	Specifies the origin of the service associated with the I-SID interface.
ISID NAME	Specifies the name of the I-SID.
BPDU	Specifies the BPDU forward option for the untagged traffic port.
MAC SUNI	Specifies the Switched UNI MAC address.

## Example

The following example shows the configured service instance identifiers (I-SID) on a port.

```
Switch:1#show interface gigabitEthernet i-sid
=====
                PORT Isid Info
=====
```



PORTNUM	IFINDEX	ISID ID	VLANID	C-VID	ISID TYPE	ORIGIN	ISID NAME	BPDU	MAC SUNI
1/1	192	27	N/A	4000	ELAN	C --- - --- -	ISID-27		FALSE
1/1	192	270	N/A	4001	ELAN	C --- - --- -	ISID-270		FALSE
1/1	192	309	N/A	309	ELAN	C --- - --- -	ISID-309		FALSE
1/1	192	401	N/A	401	ELAN	C --- - --- -	ISID-401		FALSE
1/1	192	1001	N/A	1001	ELAN	C --- - --- -	ISID-1001		FALSE
1/1	192	1111	N/A	1111	ELAN	C --- - --- -	ISID-1111		FALSE
1/1	192	1121	N/A	1121	ELAN	C --- - --- -	ISID-1121		FALSE
1/1	192	1201	N/A	1201	ELAN	C --- - --- -	ISID-1201		FALSE
1/1	192	2001	N/A	2001	ELAN	C --- - --- -	ISID-2001		FALSE
1/2	193	38	N/A	4000	ELAN	C --- - --- -	ISID-38		FALSE
1/2	193	310	N/A	310	ELAN	C --- - --- -	ISID-310		FALSE
1/2	193	380	N/A	4001	ELAN	C --- - --- -	ISID-380		FALSE
1/2	193	402	N/A	402	ELAN	C --- - --- -	ISID-402		FALSE

13 out of 152 Total Num of i-sid endpoints displayed

#### ORIGIN Legend:

C: manually configured; D: discovered by FA or EPT

M: FA management; E: discovered by EAP; A: auto-sense

l: discover by local switch r: discover by remote VIST switch

## show interfaces gigabitethernet l1-config

Show Layer 1 configuration information for the port.

### Syntax

- **show interfaces gigabitEthernet l1-config**
- **show interfaces gigabitEthernet l1-config {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} <1-4059>**
- **show interfaces gigabitEthernet l1-config <1-4059>**

### Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

---

## show interfaces gigabitEthernet limit-fdb-learning

Show the configuration for the limit forwarding database (FDB) learning feature.

## Syntax

- **show interfaces gigabitEthernet limit-fdb-learning** [**<1-4059>**] [{**slot/port**[/**sub-port**] [**-slot/port**[/**sub-port**]] [,...]]

## Command Parameters

{*slot/port*[/*sub-port*] [*-slot/port*[/*sub-port*]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## show interfaces gigabitEthernet name

Show port names and general configuration information.

## Syntax

- **show interfaces gigabitEthernet name**
- **show interfaces gigabitEthernet name <1-4059>**
- **show interfaces gigabitEthernet name {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces gigabitethernet ospf

---

Shows OSPF port information.

## Syntax

- **show interfaces gigabitEthernet ospf**
- **show interfaces gigabitEthernet ospf <1-4059>**
- **show interfaces gigabitEthernet ospf {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces gigabitethernet private-vlan

---

Shows Private VLAN information for the port.

## Syntax

- **show interfaces gigabitethernet private-vlan {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show interfaces gigabitethernet private-vlan <2-4059>**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces gigabitethernet rate-limit

---

Show rate-limit configuration information for the port.

### Syntax

- **show interfaces gigabitEthernet rate-limit**
- **show interfaces gigabitEthernet rate-limit <1-4059>**
- **show interfaces gigabitEthernet rate-limit {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

## Command Mode

Privileged EXEC

## show interfaces gigabitethernet shape

---

Show the configuration for egress rate-limiting on the port.

### Syntax

- **show interfaces gigabitEthernet shape**
- **show interfaces gigabitEthernet shape {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

---

## show interfaces gigabitethernet slpp

Display the Simple Loop Prevention Protocol (SLPP) configuration information for the port.

## Syntax

- **show interfaces gigabitEthernet slpp**
- **show interfaces gigabitEthernet slpp {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

---

## show interfaces gigabitethernet state

Shows the state of the port.

## Syntax

- **show interfaces gigabitEthernet state**
- **show interfaces gigabitEthernet state <1-4059>**
- **show interfaces gigabitEthernet state {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces gigabitEthernet statistics

Display the statistics of a port, for all ports, or for a VLAN.

## Syntax

- **show interfaces gigabitEthernet statistics**
- **show interfaces gigabitEthernet statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show interfaces gigabitEthernet statistics rate-limiting**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

# show interfaces gigabitethernet statistics bridging

---

Display individual bridging statistics for specific ports to manage network performance.

## Syntax

- **show interfaces gigabitethernet statistics bridging {slot/port[-slot/port] [,...]}**

## Command Parameters

*{slot/port [-slot/port] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show interfaces gigabitethernet statistic bridging** command displays the following information:

Output field	Description
PORT NUMB	Port index of the statistics table.
IN_FRAME UNICAST	The count of inbound Unicast frames.
IN_FRAME MULTICAST	The count of inbound Multicast frames.



Output field	Description
IN_FRAME BROADCAST	The count of inbound Broadcast frames.
OUT_FRAME	The count of outbound frames.

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## show interfaces gigabitethernet statistics dhcp-relay

Show Dynamic Host Configuration Protocol (DHCP) Relay information to view DHCP parameter information for one port, for all ports, or for a VLAN.

## Syntax

- **show interfaces gigabitEthernet statistics dhcp-relay**
- **show interfaces gigabitEthernet statistics dhcp-relay {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show interfaces gigabitEthernet statistics dhcp-relay vrf WORD<1-16>**
- **show interfaces gigabitEthernet statistics dhcp-relay vrfids WORD<0-512>**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vrf WORD<1-16>**

Displays all statistics by port.

**vrfids WORD<0-512>**

Specifies the slot and the port number.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show interfaces gigabitethernet statistics dhcp-relay** command displays the following information:

Output field	Description
PORT_NUM	Indicates the port number.
VRF_NAME	Identifies the VRF
NUMREQUEST	Indicates the total number of DHCP requests on this interface
NUMREPLY	Indicates the total number of DHCP replies on this interface.

## show interfaces gigabitethernet statistics lacp

Display individual Link Aggregation Control Protocol (LACP) statistics for specific ports to manage network performance.

### Syntax

- **show interfaces gigabitEthernet statistics lacp**
- **show interfaces gigabitEthernet statistics lacp {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

Privileged EXEC

## Command Output

The **show interfaces gigabitethernet statistics lacp** command displays the following information:

Output field	Description
PORT_NUM	Indicates the port number.
TX LACPDU	The count of transmitted LACP data units.
RX LACPDU	The count of received LACP data units.
TX MARKERPDU	The count of transmitted marker protocol data units.
RX MARKERPDU	The count of received marker protocol data units.
TX MARKERRESPPDU	The count of transmitted marker protocol response data units.
RX MARKERRESPPDU	The count of received marker protocol response data units.
RX UNKNOWN	The count of received unknown frames.
RX ILLEGAL	The count of received illegal frames.

## show interfaces gigabitethernet statistics policer

Display individual policer statistics for specific ports to manage network performance.

### Syntax

- **show interfaces gigabitEthernet statistics policer {slot/port[-slot/port][,...]}**

### Command Parameters

*{slot/port [-slot/port] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

### Default

None

### Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show interfaces gigabitEthernet statistics rmon

Display individual Remote Network Monitoring (RMON) statistics for specific ports to manage network performance.

## Syntax

- **show interfaces gigabitEthernet statistics rmon**
- **show interfaces gigabitEthernet statistics rmon {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show interfaces gigabitEthernet statistics rmon history**
- **show interfaces gigabitEthernet statistics rmon history {{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### history

Displays all statistics by port.

```
history {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show interfaces GigabitEthernet statistics rmon** command displays the following information:

Output field	Description
PORT NUM	Indicates the port number.
OCTETS	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
PKTS	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
MULTICAST	The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
BROADCAST	The total number of packets received that were directed to the broadcast address. This number does not include multicast packets.
CRC ALLIGN	The total number of packets received that had a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a nonintegral number of octets (Alignment Error).
UNDERSIZE	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
OVERSIZE	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
FRAGMENT	The total number of packets received that were less than 64 octets in length (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 nonintegral number of octets (Alignment Error).
COLLISION	An estimated value for the total number of collisions on this Ethernet segment.

## show interfaces gigabitethernet statistics verbose

Display individual verbose statistics for specific ports to manage network performance.

## Syntax

- **show interfaces gigabitEthernet statistics verbose**
- **show interfaces gigabitEthernet statistics verbose {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show interfaces gigabitEthernet statistics verbose** command displays the following information:

Output field	Description
PORT_NUM	Indicates the port number.
IN_UNICAST	The count of inbound Unicast packets.
OUT_UNICAST	The count of outbound Unicast packets.
IN_MULTICAST	The count of inbound Multicast packets.
OUT_MULTICAST	The count of outbound Multicast packets.
IN_BRDCST	The count of inbound broadcast packets.
OUT_BRDCST	The count of outbound broadcast packets.

## show interfaces gigabitEthernet statistics vlacp

Display individual Virtual Link Aggregation Control Protocol (VLACP) statistics for specific ports to manage network performance.

## Syntax

- **show interfaces gigabitEthernet statistics vlacp [history] [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

### history

Displays the port counter profile.

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show interfaces gigabitethernet statistics vlacp** command displays the following information:

Output field	Description
PORT NUM	Shows the slot and port number.
TX VLACPDU	Shows the number of VLACPDU transmitted on the port.
RX VLACPDU	Shows the number of valid VLACPDU received on the port.
SEQNUM MISMATCH	Shows the number of mismatched VLACPDU in terms of received sequence numbers on the port.

## show interfaces gigabitethernet vlan

Show VLAN information for the port.

## Syntax

- **show interfaces gigabitEthernet vlan**
- **show interfaces gigabitEthernet vlan <1-4059>**
- **show interfaces gigabitEthernet vlan {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces gigabitEthernet vrf

---

Show VRF-association information for the port..

## Syntax

- **show interfaces gigabitEthernet vrf**
- **show interfaces gigabitEthernet vrf {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show interfaces gigabitEthernet vrf vrf WORD<1-16>**
- **show interfaces gigabitEthernet vrf vrfids WORD<0-512>**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.



## Default

None

## Command Mode

Privileged EXEC

## show interfaces loopback

Show loopback interface information.

## Syntax

- **show interfaces loopback**
- **show interfaces loopback vrf WORD <1-16> name**
- **show interfaces loopback vrfids WORD <0-512>**

## Command Parameters

### name

Specifies the name associated with the IPv4 or IPv6 address.

### vrfids WORD<0-512>

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

### vrf WORD<1-16>

Specifies the loopback information for the associated VRF name. WORD<1-16> specifies the VRF name in the range of 1 to 16 characters.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

The *name* parameter is not supported on VSP 8600 Series.

## Example

```
Switch:1#show interfaces loopback
```

```

=====
                          Circuitless IP Interface - GlobalRouter
=====
INTF IP_ADDRESS   NET_MASK   OSPF   PIM   AREA_ID   IF   IP
ID              ID              STATUS STATUS   ID              INDX NAME

```

```

-----
1   1.2.3.4      255.255.0.0   disable disable 0.0.0.0   1344
2   2.3.4.5      255.255.255.0 disable disable 0.0.0.0   1345
15  192.0.2.2    255.255.255.0 disable disable 0.0.0.0   1358 EXTRSERVER101
-----
                                Loopback Ipv6 Interface
-----
IF   VRF          Descr          VLAN PHYSICAL      ADMIN  OPER  TYPE  MTU  HOP  REACHABLE  RETRANSMIT  IPSEC
INDX NAME                                     ADDRESS  STATE  STATE                                     LMT  TIME      TIME      STATE
-----
1234 GREEN          CLIPv6-11      00:00:00:00:00:0b enable  up   ETHER 1500 64  30000    1000    disable
-----
                                Loopback Ipv6 Address
-----
IPV6 ADDRESS/PREFIX LENGTH      LOOPBACK-ID  TYPE  ORIGIN  STATUS      NAME
-----
2001:DB8:2000::1/128            C-11        UNICAST  MANUAL  PREFERRED INF  INF  EXTRSER200

1 out of 1 Total Num of Interface Entries displayed.
1 out of 1 Total Num of Address Entries displayed.

```

## show interfaces mgmtethernet

Show configuration information for MgmtEthernet ports.

### Syntax

- **show interfaces mgmtEthernet**

### Default

None

### Command Mode

Privileged EXEC

## show interfaces mgmtethernet config-L1

Show port config-L1 information.

### Syntax

- **show interfaces mgmtethernet config-L1**

### Default

None

### Command Mode

Privileged EXEC

## show interfaces mgmtethernet error

Show port general error information.

## Syntax

- **show interfaces mgmtethernet error {collision|verbose}**

## Command Parameters

### collision

Shows management port collision error information.

### verbose

Displays all statistics by management port.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces mgmtethernet statistics

---

Display individual statistics for specific management ports to manage network performance.

## Syntax

- **show interfaces mgmtEthernet statistics**
- **show interfaces mgmtEthernet statistics verbose**

## Default

None

## Command Mode

Privileged EXEC

## show interfaces vlan

---

Show basic and advanced VLAN information.

## Syntax

- **show interfaces vlan**
- **show interfaces vlan <1-4059>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces vlan arp

---

Display Address Resolution Protocol (ARP) information for the VLAN.

## Syntax

- **show interfaces vlan arp**
- **show interfaces vlan arp <1-4059>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces vlan autolearn-mac

---

Show bridging autolearn MAC address information for VLANs.

## Syntax

- **show interfaces vlan autolearn-mac**
- **show interfaces vlan autolearn-mac**

## Default

None

## Command Mode

Privileged EXEC

## show interfaces vlan dhcp-relay

---

Show Dynamic Host Configuration Protocol (DHCP) information for the VLAN.

## Syntax

- **show interfaces vlan dhcp-relay**
- **show interfaces vlan dhcp-relay <1-4059>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces vlan igmp

---

Show Internet Group Management Protocol (IGMP) information for the VLAN.

## Syntax

- **show interfaces vlan igmp [<1-4059>]**

- **show interfaces vlan vrf WORD<0-32>**
- **show interfaces vlan vrfid WORD<0-255>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

WORD<0-255>

Enter vrf ids

WORD<0-32>

Specify the vrf name

## Default

None

## Command Mode

Privileged EXEC

## show interfaces vlan igmp-mrdisc

---

Show Internet Group Management Protocol (IGMP) multicast route discovery information for the VLAN.

## Syntax

- **show interfaces vlan igmp-mrdisc [<1-4059>]**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show interfaces vlan ip

---

Show the IP configuration for the VLAN.

### Syntax

- **show interfaces vlan ip**
- **show interfaces vlan ip <1-4059>**
- **show interfaces vlan ip vrf WORD<1-16>**
- **show interfaces vlan ip vrfids WORD<0-512>**

### Command Parameters

**<1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD<0-512>**

Displays ip address information for particular vrfids.

### Default

None

## Command Mode

Privileged EXEC

## show interfaces vlan manual-edit-mac

---

Display the manually-edited bridging MAC address information for VLANs.

### Syntax

- **show interfaces vlan manual-edit-mac**

## Default

None

## Command Mode

Privileged EXEC

---

## show interfaces vlan nlb-mode

Show the Network Load Balancer (NLB) configuration for the VLAN.

## Syntax

- **show interfaces vlan nlb-mode [<1-4059>]**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

---

## show interfaces vlan vlan-bysrcmac

Show source MAC-based VLAN information.

## Syntax

- **show interfaces vlan vlan-bysrcmac**

## Default

None



## Command Mode

Privileged EXEC

## show interfaces vlan vrfs

---

Show VRF-association information for the VLAN.

### Syntax

- **show interfaces vlan vrfs**
- **show interfaces vlan vrfs <1-4059>**
- **show interfaces vlan vrfs {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show interfaces vlan vrfs vrf WORD<1-16>**
- **show interfaces vlan vrfs vrfids WORD<0-512>**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**<1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

### Default

None

### Command Mode

Privileged EXEC

## show ip igmp access

Displays information about the Internet Group Management Protocol (IGMP) multicast access control groups. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

### Syntax

- **show ip igmp access**
- **show ip igmp access vrf WORD<1-16>**
- **show ip igmp access vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

### Default

None

### Command Mode

Privileged EXEC

### Usage Guidelines

This command is not supported on a node configured as the DvR Leaf within a DvR domain.

### Command Output

The **show ip igmp access** command displays the following information:

Output field	Description
INTERFACE	Identifies the interface where multicast access control is configured.
GRP PREFIX	Shows an alphanumeric string that identifies the name of the access policy.
HOSTADDR	Shows the IP address of the host.

Output field	Description
HOSTMASK	Shows the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the host network.
ACCESSMODE	Specifies the action of the access policy. The actions are: <ul style="list-style-type: none"> <li>deny-tx—deny IP multicast transmitted traffic.</li> <li>deny-rx—deny IP multicast received traffic.</li> <li>deny-both—deny both IP multicast transmitted and received traffic.</li> <li>allow-only-rx—allow IP multicast transmitted traffic.</li> <li>allow-only-rx—allow IP multicast received traffic.</li> <li>allow-only-both—allow both IP multicast transmitted and received traffic.</li> </ul>

## show ip igmp cache

Displays information about the IGMP cache. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

### Syntax

- **show ip igmp cache**
- **show ip igmp cache vrf WORD<1-16>**
- **show ip igmp cache vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

### Default

None

### Command Mode

Privileged EXEC

## Command Output

The **show ip igmp cache** command displays the following information:

Output field	Description
GRPADDR	Indicates the multicast group address (Class D) that others want to join. Many incoming ports can use the same group address.
INTERFACE	Indicates the physical interface or a logical interface (VLAN), which received group reports from various sources.
LASTREPORTER	Indicates the IP address of the source of the last membership report received for this IP multicast group address on this interface. If the interface does not receive a membership report, this object uses the value 0.0.0.0.
EXPIRATION	Indicates the minimum amount of time that remains before this entry ages out.
VIHOSTIMER	Indicates the time that remains until the local router assumes that no IGMPv1 members exist on the IP subnet attached to this interface.
TYPE	Indicates whether the entry is learned dynamically or is added statically.
STATICPORTS	Indicates the list of statically-defined ports.
L2ISID	Indicates the I-SID associated with the Layer 2 interface.

## show ip igmp group

Displays information about a statically configured or dynamically learned IGMP group. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp group**
- **show ip igmp group group {A.B.C.D}**
- **show ip igmp group member-subnet {A.B.C.D/X}**
- **show ip igmp group vrf WORD<1-16>**
- **show ip igmp group vrfids WORD<0-512>**

## Command Parameters

### count

Specifies the number of entries.

### group {A.B.C.D}

Specifies the group address.

### member-subnet default |{A.B.C.D/X}

Specifies the IP address and network mask.

### vrf WORD<1-16>

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

The CLI command **show ip igmp group** displays both static and dynamically learned IGMP groups, and the CLI command **show ip igmp static** command displays only the statically configured IGMP groups. In contrast, the EDM display command under **IP > IGMP > Groups** displays the dynamically learned groups, and the EDM command under **IP > IGMP > Static** displays the statically configured IGMP groups.

## Command Output

The **show ip igmp group** command displays the following information:

Output field	Description
GRPADDR	Indicates the multicast group address (Class D) that others want to join. Many incoming ports can use the same group address.
INPORT	Indicates the physical interface or a logical interface (VLAN), which received group reports from various sources.
MEMBER	Indicates the IP address of a source that sent a group report to join this group.
EXPIRATION	Indicates the time left before the group report expires on this port. The port updates this variable after it receives a group report.
TYPE	Indicates whether the entry is learned dynamically or is added statically.
L2ISID	Indicates the I-SID associated with the Layer 2 interface.

## Examples

The following example displays information about the IGMP group.

```
Switch:1#show ip igmp group

=====
                        Igmp Group - GlobalRouter
=====
GRPADDR      INPORT      MEMBER      EXPIRATION  TYPE      L2ISID
-----
224.5.2.1    V701-1/4    62.0.1.1    214         Dynamic   40400
224.5.2.2    V702-1/4    62.0.2.1    221         Dynamic   40400
224.5.2.3    V703-1/4    62.0.3.1    217         Dynamic   40400
224.5.2.4    V704-1/4    62.0.4.1    223         Dynamic   40400
```

```
4 out of 4 group Receivers displayed
Total number of unique groups 2
```

The following example displays information about the IGMP group for a specific VRF.

```
Switch:1# show ip igmp group vrf green

=====
IGMP Group - GlobalRouter
=====
GRPADDR      INPORT      MEMBER      EXPIRATION  TYPE
-----
233.252.0.1  V501-9/16  192.2.0.1   204         Dynamic
233.252.0.2  V501-9/16  192.2.0.1   206         Dynamic
233.252.0.3  V501-9/16  192.2.0.1   206         Dynamic
233.252.0.4  V501-9/16  192.2.0.1   207         Dynamic
233.252.0.5  V501-9/16  192.2.0.1   204         Dynamic
233.252.0.6  V501-9/16  192.2.0.1   209         Dynamic
233.252.0.7  V501-9/16  192.2.0.1   206         Dynamic
233.252.0.8  V501-9/16  192.2.0.1   206         Dynamic
233.252.0.9  V501-9/16  192.2.0.1   211         Dynamic
233.252.0.10 V501-9/16  192.2.0.1   207         Dynamic

10 out of 10 group Receivers displayed
Total number of unique groups 10
```

## show ip igmp group count

Displays the number of entries in the IGMP group. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

### Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X}**
- **show ip igmp group count vrf WORD<1-16>**
- **show ip igmp group count vrfids WORD<0-512>**

### Command Parameters

**group {A.B.C.D}**

Specifies the group address.

**member-subnet default [{A.B.C.D/X}]**

Specifies the IP address and network mask.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group count group {A.B.C.D}

---

Displays the number of entries in the specified IGMP group. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp group count group {A.B.C.D} [detail] [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip igmp group count group {A.B.C.D} detail [port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**detail**

Displays Internet Group Management Protocol version 3 (IGMPv3)-specific data.

**port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

# show ip igmp group count group {A.B.C.D} tracked-members

---

Displays the number of tracked-members in the specified IGMP group.

## Syntax

- **show ip igmp group count group {A.B.C.D} tracked-members**

## Command Parameters

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None



## Command Mode

Privileged EXEC

## show ip igmp group count group {A.B.C.D} tracked-members member-subnet

Displays the number of tracked-members in the specified IGMP group for specific member IP address and subnet mask.

### Syntax

- **show ip igmp group count group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] [source-subnet {A.B.C.D/X}] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

### Command Parameters

**{A.B.C.D/X}**

Specifies the IP address with mask in A.B.C.D/X or A.B.C.D/X.X.X.X format.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Displays the number of tracked-members in the specified IGMP group for the specified port list.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**

Displays the number of tracked-members in the specified IGMP group for a specific source IP address and subnet mask.

**vlan <1-4059>**

Displays the number of tracked-members in the specified IGMP group for a specific VLAN ID.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Displays the number of tracked-members in the specified IGMP group for a specific VRF.

**vrfids WORD<0-512>**

Displays the number of tracked-members in the specified IGMP group for a specific VRF ID.

## Default

None

## Command Mode

Privileged EXEC

# show ip igmp group count group {A.B.C.D} tracked-members port

Displays the number of tracked-members in the specified IGMP group for specific port list.

## Syntax

- **show ip igmp group count group {A.B.C.D} tracked-members port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} [member-subnet {A.B.C.D/X}] [source-subnet {A.B.C.D/X}] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids <0-512>]**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### **member-subnet {A.B.C.D/X}**

Displays the number of tracked-members in the specified IGMP group for specific member IP address and subnet mask.

### **source-subnet {A.B.C.D/X}**

Displays the number of tracked-members in the specified IGMP group for a specific source IP address and subnet mask.

### **vlan <1-4059>**

Displays the number of tracked-members in the specified IGMP group for a specific VLAN ID.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### **vrf WORD<1-16>**

Displays the number of tracked-members in the specified IGMP group for a specific VRF.

### **vrfids WORD<0-512>**

Displays the number of tracked-members in the specified IGMP group for a specific VRF ID.

## Default

None

## Command Mode

Privileged EXEC

# show ip igmp group count group {A.B.C.D} tracked-members source-subnet

Displays the number of tracked-members in the specified IGMP group for a specific source IP address and subnet mask.

## Syntax

- **show ip igmp group count group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} [member-subnet {A.B.C.D/X}] [port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**{A.B.C.D/X}**

Specifies the IP address with mask in A.B.C.D/X or A.B.C.D/X.X.X.X format.

**member-subnet {A.B.C.D/X}**

Displays the number of tracked-members in the specified IGMP group for specific member IP address and subnet mask.

**port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]**

Displays the number of tracked-members in the specified IGMP group for the specified port list.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Displays the number of tracked-members in the specified IGMP group for a specific VLAN ID.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Displays the number of tracked-members in the specified IGMP group for a specific VRF.

**vrfids WORD<0-512>**

Displays the number of tracked-members in the specified IGMP group for a specific VRF ID.

## Default

None

## Command Mode

Privileged EXEC

---

## show ip igmp group count group {A.B.C.D} tracked-members vlan

---

Displays the number of tracked-members in the specified IGMP group for a specific VLAN ID.

## Syntax

- **show ip igmp group count group {A.B.C.D} tracked-members vlan <1-4059> [member-subnet {A.B.C.D/X}] [port {slot/port[/sub-port]}[-slot/port[/sub-port]] [,...]] [source-subnet {A.B.C.D/X}]**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### member-subnet {A.B.C.D/X}

Displays the number of tracked-members in the specified IGMP group for specific member IP address and subnet mask.

**port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]**

Displays the number of tracked-members in the specified IGMP group for the specified port list.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### source-subnet {A.B.C.D/X}

Displays the number of tracked-members in the specified IGMP group for a specific source IP address and subnet mask.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group count group {A.B.C.D} tracked-members vrf

---

Displays the number of tracked-members in the specified IGMP group for a specific VRF.

## Syntax

- **show ip igmp group count group {A.B.C.D} tracked-members vrf WORD<1-16> [vrfids WORD<0-512>]**

## Command Parameters

**vrf WORD<1-16>**

Displays the number of tracked-members in the specified IGMP group for a specific VRF name.

**vrfids WORD<0-512>**

Displays the number of tracked-members in the specified IGMP group for a specific VRF ID.

**WORD<1-16>**

Specifies the VRF name.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group count group {A.B.C.D} tracked-members vrfids

---

Displays the number of tracked-members in the specified IGMP group for a specific VRF ID.

## Syntax

- **show ip igmp group count group {A.B.C.D} tracked-members vrfids WORD<0-512>**

## Command Parameters

**WORD<0-512>**

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

---

## show ip igmp group count member-subnet

Displays the number of members in the specified IGMP group subnet.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X}**

## Command Parameters

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

## Default

None

## Command Mode

Privileged EXEC

---

## show ip igmp group count member-subnet {A.B.C.D/X} group

Displays the number of members in the specified IGMP group subnet.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D}**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} detail

Displays the number of members in the specified IGMP group subnet. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} detail [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members

Displays the number of tracked-members in the specified IGMP group subnet. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members [member-subnet {A.B.C.D/X}] [port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]] [source-subnet {A.B.C.D/X}] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies the ID of the VRF.



## Default

None

## Command Mode

Privileged EXEC

# show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members port

Displays the number of tracked-members in the specified IGMP group subnet for a specified port. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} [member-subnet {A.B.C.D/X}] [source-subnet {A.B.C.D/X}] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids** WORD <0-512>  
Specifies the ID of the VRF.

## Default

None

## Command Mode

Privileged EXEC

# show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet

Displays the number of tracked-members in the specified IGMP group subnet for a specified source IP address and subnet mask. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} [member-subnet {A.B.C.D/X}] [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**{A.B.C.D}**  
Specifies the group address.

**member-subnet {A.B.C.D/X}**  
Specifies the IP address and mask of the IGMP member.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**  
Specifies the source IP address and the subnet mask.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags,

```
show ip igmp group count member-subnet {A.B.C.D/X}
group {A.B.C.D} tracked-members source-subnet
{A.B.C.D/X} port
```

Privileged EXEC

the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

Privileged EXEC

## **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port**

Displays the number of tracked-members in the specified IGMP group subnet for a specified source IP address and subnet mask, and port. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} [member-subnet {A.B.C.D/X}] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

**vlan <1-4059>**

```
show ip igmp group count member-subnet {A.B.C.D/X}  
group {A.B.C.D} tracked-members source-subnet  
{A.B.C.D/X} vlan
```

Privileged EXEC

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vlan

Displays the number of tracked-members in the specified IGMP group subnet for a specified source IP address and subnet mask, and VLAN ID.

## Syntax

- show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vlan <1-4059> [member-subnet {A.B.C.D/X}] [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

```
show ip igmp group count member-subnet {A.B.C.D/X}
group {A.B.C.D} tracked-members source-subnet
{A.B.C.D/X} vrf
```

Privileged EXEC

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vrf**

Displays the number of tracked-members in the specified IGMP group subnet for a specified source IP address and subnet mask, and VRF name.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vrf WORD<1-16>**
- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vrf WORD<1-16> vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

```
show ip igmp group count member-subnet {A.B.C.D/X}  
group {A.B.C.D} tracked-members source-subnet  
{A.B.C.D/X} vrfids
```

Privileged EXEC

## Default

None

## Command Mode

Privileged EXEC

## **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vrfids**

Displays the number of tracked-members in the specified IGMP group subnet for a specified source IP address and subnet mask, and VRF ID.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

Privileged EXEC

## **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members vlan**

Displays the number of tracked-members in the specified IGMP group subnet for a specified VLAN ID.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members vlan <1-4059> [member-subnet {A.B.C.D/X}] [port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]] [source-subnet {A.B.C.D/X}]**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members vrf

Displays the number of tracked-members in the specified IGMP group subnet for a specified VRF name.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members vrf WORD<1-16>**

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members vrf WORD<1-16> vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

Privileged EXEC

## **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members vrfids**

Displays the number of tracked-members in the specified IGMP group subnet for a specified VRF ID.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} tracked-members vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None



## Command Mode

Privileged EXEC

### show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} vrf

---

Displays the number of members in the specified IGMP group subnet for a specified VRF name.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} vrf WORD<1-16>**
- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} vrf WORD<1-16> vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D}**

Specifies the group address.

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

Privileged EXEC

### show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} vrfids

---

Displays the number of members in the specified IGMP group subnet for a specified VRF ID

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} group {A.B.C.D} vrfids WORD<0-512>**

## Command Parameters

{A.B.C.D}

Specifies the group address.

member-subnet {A.B.C.D/X}

Specifies the IP address and mask of the IGMP member.

vrfids WORD <0-512>

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group count member-subnet {A.B.C.D/X} vrf

---

Displays the number of members in the specified IGMP subnet for a specified VRF name.

## Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} vrf WORD<1-16>**
- **show ip igmp group count member-subnet {A.B.C.D/X} vrf WORD<1-16>  
vrfids WORD<0-512>**

## Command Parameters

member-subnet {A.B.C.D/X}

Specifies the IP address and mask of the IGMP member.

vrf WORD<1-16>

Specifies a VRF by name.

vrfids WORD <0-512>

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

Privileged EXEC

---

## show ip igmp group count member-subnet {A.B.C.D/X} vrfids

---

Displays the number of members in the specified IGMP subnet for a specified VRF ID.

### Syntax

- **show ip igmp group count member-subnet {A.B.C.D/X} vrfids WORD<0-512>**

### Command Parameters

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**vrfids WORD <0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

### Default

None

### Command Mode

Privileged EXEC

---

## show ip igmp group group <A.B.C.D>

---

Displays information for a specific group address. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

### Syntax

- **show ip igmp group group {A.B.C.D} [detail] [vlan <1-4059>] [vrf WORD <0-16>] [vrfids WORD <0-512>]**
- **show ip igmp group group {A.B.C.D} detail port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} [vlan <1-4059>] [vrf WORD <0-16>] [vrfids WORD <0-512>]**

### Command Parameters

**detail**

Displays Internet Group Management Protocol version 3 (IGMPv3)-specific data.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf** WORD<1-16>

Specifies a VRF by name.

**vrfids** <0-512>

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group group <A.B.C.D> tracked-members

Displays all the tracked members for a specific group. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp group group {A.B.C.D} tracked-members [member-subnet {A.B.C.D/X}] [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]] [source-subnet {A.B.C.D/X}] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD <0-512>]**

## Command Parameters

**member-subnet {A.B.C.D/X}**

Specifies the IP address and mask of the IGMP member.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**source-subnet {A.B.C.D/X}**

Specifies the source IP address and the subnet mask.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf** WORD<1-16>

Specifies a VRF by name.

**vrfids** <0-512>

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp group member-subnet

---

Displays information for a specific IP address and mask of the IGMP member. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp group member-subnet {A.B.C.D/X}**
- **show ip igmp group member-subnet {A.B.C.D/X} vrf WORD<1-16>**
- **show ip igmp group member-subnet {A.B.C.D/X} vrfids WORD<0-512>**
- **show ip igmp group member-subnet default**

## Command Parameters

{A.B.C.D/X}

Specifies the IP address and mask of the IGMP member.

**default**

Shows information for the default IP address.

**vrf** WORD<1-16>

Specifies a VRF by name.

**vrfids** <0-512>

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip igmp interface

Displays information about the interfaces where Internet Group Management Protocol (IGMP) is enabled. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp interface**
- **show ip igmp interface gigabitethernet** [**<1-4059>**] [{**slot/port[/sub-port]** [**-slot/port[/sub-port]**] [,...]]
- **show ip igmp interface vlan** [**<1-4059>**] [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]
- **show ip igmp interface vrf** **WORD<1-16>** [**vrfids WORD<0-512>**]
- **show ip igmp interface vrfids** **WORD<0-512>**

## Command Parameters

**gigabitethernet** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### interface

Shows Internet Group Management Protocol (IGMP) interfaces.

**vlan** *<1-4059>*

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf** **WORD<1-16>**

Specifies a VRF by name.

**vrfids** **<0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The following table shows the field descriptions for the **show ip igmp interface** if you do not use the interface parameters.

Output Field	Description
IF	Indicates the interface where IGMP is configured.
QUERY INTVL	Indicates the frequency at which IGMP host query packets transmit on this interface.
STATUS	Indicates the activation of a row, which activates IGMP on the interface. The destruction of a row disables IGMP on the interface.
VERS.	Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.
OPER VERS	Indicates the operational version of IGMP.
QUERIER	Indicates the address of the IGMP querier on the IP subnet to which this interface attaches.
QUERY MAXRSPT	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
WRONG QUERY	Indicates the number of queries received where the IGMP version does not match the interface version. You must configure all routers on a LAN to run the same version of IGMP. If queries are received with the wrong version, a configuration error occurs.
JOINS	Indicates the number of times this interface added a group membership.
ROBUST	Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.
LASTMEM QUERY	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.

Output Field	Description
MODE	Indicates the protocol configured on the VLAN added. <ul style="list-style-type: none"> <li>snoop—Indicates IGMP snooping is enabled on a VLAN.</li> <li>snoop-spb—Indicates IGMP is enabled on a VLAN with an associated I-SID (IP multicast over Fabric Connect for a Layer 2 VSN).</li> <li>pim—Indicates PIM is enabled.</li> <li>routed-spb—Indicates IP multicast over Fabric Connect is enabled on the Layer 3 VSN or for IP Shortcuts.</li> <li>pim-gw-spb—Indicates the SPB-PIM Gateway is enabled on the interface.</li> </ul>
L2ISID	Indicates the I-SID associated with the Layer 2 interface.

The following table shows the field descriptions for the **show ip igmp interface** if you use the interface parameters.

Output Field	Description
VLAN ID or PORT NUM	Identifies the VLAN or port where IGMP is configured.
QUERY INTVL	Indicates the frequency at which IGMP host query packets transmit on this interface.
QUERY MAX RESP	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
ROBUST	Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.
VERSION	Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.
LAST MEMB QUERY	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.
PROXY SNOOP ENABLE	Indicates if proxy snoop is enabled on the interface.
SNOOP ENABLE	Indicates if snoop is enabled on the interface.
SNOOP ORIGIN	Specifies the origin of the IGMP Snooping configuration on the port. The supported values are: <ul style="list-style-type: none"> <li>config - Set by the user.</li> <li>radius - Set by the Remote Authentication Dial-In User Service (RADIUS) attribute.</li> </ul>
SSM SNOOP ENABLE	Indicates if SSM snoop is enabled on the interface.
UPnP FILTER ENABLE	Indicates if Universal Plug and Play (uPnP) Filtering is enabled to filter multicast packets destined for a specific range. The default is disabled.



Output Field	Description
FAST LEAVE ENABLE	Indicates if fast leave mode is enabled on the interface.
FAST LEAVE PORTS (VLAN parameter only)	Indicates the set of ports that are enabled for fast leave
SNOOP QUERIER ENABLE (VLAN parameter only)	Indicates if the IGMP Layer 2 Querier feature is enabled.
SNOOP QUERIER ADDRESS (VLAN parameter only)	Indicates the IP address of the IGMP Layer 2 querier.
DYNAMIC DOWNGRADE VERSION	Indicates if the dynamic downgrade feature is enabled.
COMPATIBILITY MODE	Indicates if compatibility mode is enabled.
EXPLICIT HOST TRACKING	Indicates if explicit host tracking is enabled to track all the source and group members.
UPnP FILTER ADDRESS	Indicates the multicast destination IP address to filter on an IGMP-enabled interface. The default is 239.255.255.250/32.

## Examples

The following examples display information about the interfaces where IGMP is enabled.

```
Switch:1#show ip igmp interface
```

```
=====
                        Igmp Interface - GlobalRouter
=====
QUERY      OPER      QUERY  WRONG      LASTMEM
IF  INTVL  STATUS  VERS.  VERS  QUERIER  MAXRSPT  QUERY  JOINS  ROBUST  QUERY  MODE  L2ISID
-----
V100  125   activ  2     2   0.0.0.0  100     0     0     2     10   snoop-spb 1100
```

1 out of 1 entries displayed

```
Switch:1#show ip igmp interface vlan 2
```

```
=====
                        Vlan Ip Igmp
=====
VLAN QUERY  QUERY  ROBUST  VERSION  LAST  PROXY  SNOOP  SNOOP  SSM  UPnP  FAST  FAST
ID  INTVL  MAX    RESP           MEMB  SNOOP  ENABLE  ORIGIN  SNOOP  FILTER  LEAVE  LEAVE
                                QUERY  ENABLE
-----
2   125   100    2     2     10   false  false  RADIUS  false  false
false
```

```
VLAN SNOOP  SNOOP      DYNAMIC  COMPATIBILITY  EXPLICIT  UPnP
ID  QUERIER  QUERIER    DOWNGRADE  MODE          HOSTS  FILTER
     ENABLE  ADDRESS    VERSION    TRACKING  ADDRESS
-----
2   false  0.0.0.0    enable     disable      disable  239.255.255.250/32
```

```
Switch:1#show ip igmp interface gigabitethernet 1/2
```

```
=====
                        Port Ip Igmp
=====
PORT  QUERY  QUERY  ROBUST  VERSION  LAST  PROXY  SNOOP  SNOOP  SSM  UPnP  FAST
```

NUM	INTVL	MAX RESP			MEMB QUERY	SNOOP ENABLE	ENABLE	ORIGIN	SNOOP ENABLE	FILTER ENABLE	LEAVE ENABLE
1/2	125	100	2	2	10	false	false	RADIUS	false	false	false
PORT NUM	DOWNGRADE VERSION	COMPATIBILITY MODE	EXPLICIT HOST TRACKING	UPNP FILTER ADDRESS							
1/2	enable	disable	disable	239.255.255.250/32							

## show ip igmp mrdisc

Displays information about the Internet Group Management Protocol (IGMP) multicast discovery routes. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

### Syntax

- **show ip igmp mrdisc**
- **show ip igmp mrdisc vrf WORD<1-16>**
- **show ip igmp mrdisc vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

### Default

None

### Command Mode

Privileged EXEC

### Usage Guidelines

This command is not supported on a node configured as the DvR Leaf within a DvR domain.

## Command Output

The **show ip igmp mrdisc** command displays the following information:

Output field	Description
VLAN ID	Indicates the VLAN ID.
MRDISC	Indicates the status of multicast router discovery.
MAX ADV INTERVAL	Indicates the maximum number (in seconds) between successive advertisements.
MIN ADV INTERVAL	Indicates the minimum number (in seconds) between successive advertisements.
MAX INIT ADV INTERVAL	Indicates the maximum number (in seconds) between successive initial advertisements.
MAX INIT ADV	Indicates the maximum number of initial multicast advertisements after initialization.
NBR DEAD INTERVAL	Indicates the multicast router discovery dead interval — the number of seconds the multicast route neighbors for the switch must wait before assuming that the multicast router is down.
DISCOVERED RTR PORTS	Indicates the ports discovered.

## show ip igmp mrdisc neighbors

Display information about the Internet Group Management Protocol (IGMP) multicast router discovery neighbors. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

### Syntax

- **show ip igmp mrdisc neighbors**
- **show ip igmp mrdisc neighbors vrf WORD<1-16>**
- **show ip igmp mrdisc neighbors vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

### Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show ip igmp mrdisc neighbors** command displays the following information:

Output field	Description
VLAN ID	Indicates the VLAN ID.
SRC_PORT	Indicates the source port.
IP Addr	Indicates the IP address.
Advert-int	Indicates the advertisement interval in seconds.
QUERY-int	Indicates the query interval in seconds.
Robust-val	Indicates the tuning for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.

## show ip igmp router-alert

Display the status of Internet Group Management Protocol (IGMP) router alert. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

## Syntax

- **show ip igmp router-alert**
- **show ip igmp router-alert vrf WORD<1-16>**
- **show ip igmp router-alert vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command is not supported on a node configured as the DVR Leaf within the DVR domain.

## Command Output

The **show ip igmp router-alert** command displays the following information:

Output field	Description
IFINDEX	Indicates the interface index number.
ROUTER ALERT ENABLE	Indicates the status of the router alert check.

## show ip igmp sender

Display information about the Internet Group Management Protocol (IGMP) senders.

## Syntax

- **show ip igmp sender**
- **show ip igmp sender count**
- **show ip igmp sender group {A.B.C.D}**
- **show ip igmp sender group {A.B.C.D} vrf WORD<1-16>**
- **show ip igmp sender group {A.B.C.D} vrfids WORD<0-512>**
- **show ip igmp sender member-subnet {A.B.C.D/X}**
- **show ip igmp sender member-subnet {A.B.C.D/X} vrf WORD<1-16>**
- **show ip igmp sender member-subnet {A.B.C.D/X} vrfids WORD<0-512>**
- **show ip igmp sender member-subnet default**
- **show ip igmp sender vrf WORD<1-16>**
- **show ip igmp sender vrfids WORD<0-512>**

## Command Parameters

**count**

Specifies the number of entries.

**group {A.B.C.D}**

Specifies the group address.

**member-subnet default |{A.B.C.D/X}**

Specifies the IP address and network mask.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show ip igmp sender** command displays the following information:

Output field	Description
GRPADDR	Indicates the IP multicast address.
IFINDEX	Indicates the interface index number.
MEMBER	Indicates the IP address of the host.
PORT/MLT	Indicates the IGMP sender ports.
STATE	Indicates if a sender exists because of an IGMP access filter. Options include filtered and nonfiltered.
L2ISID	Indicates the I-SID associated with the Layer 2 interface.

## Examples

The following example displays information about IGMP senders:

```
Switch:1#show ip igmp sender
=====
                        Igmp Sender - GlobalRouter
=====
GRPADDR      IFINDEX    MEMBER      PORT/
              STATE      L2ISID
-----
233.252.0.1  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.2  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.3  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.4  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.5  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.6  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.7  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.8  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.9  Vlan 501   192.2.0.1   spb      NOTFILTERED
233.252.0.10 Vlan 501   192.2.0.1   spb      NOTFILTERED

10 out of 10 entries displayed
```

The following example displays information about IGMP senders for a specific VRF:

```
Switch:1# show ip igmp sender vrf green
=====
                        IGMP Sender - GlobalRouter
=====
GRPADDR      IFINDEX    MEMBER      PORT/
              STATE
-----

```

```
-----  
233.252.0.1   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.2   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.3   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.4   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.5   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.6   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.7   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.8   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.9   Vlan 501   192.2.0.1   9/5   NOTFILTERED  
233.252.0.10  Vlan 501   192.2.0.1   9/5   NOTFILTERED  
  
10 out of 10 entries displayed
```

## show ip igmp snooping

Display the status of Internet Group Management Protocol (IGMP) snoop.

### Syntax

- **show ip igmp snooping**
- **show ip igmp snooping vrf WORD<1-16>**
- **show ip igmp snooping vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

### Default

None

### Command Mode

Privileged EXEC

### Usage Guidelines

This command is not supported on a node configured as the DvR Leaf within a DvR domain.

## Command Output

The **show ip igmp snooping** command displays the following information:

Output field	Description
IFINDEX	Indicates the interface index number.
SNOOP ENABLE	Indicates the status of IGMP snoop.
PROXY SNOOP ENABLE	Indicates the status of IGMP proxy snoop.
SSM SNOOP ENABLE	Indicates the status of IGMP Source Specific Multicast (SSM) snoop.
STATIC MROUTER PORTS	Indicates the set of ports in this VLAN that provide connectivity to an IP multicast router.
ACTIVE MROUTER PORTS	Indicates the active ports.
MROUTER EXPIRATION TIME	Indicates the multicast querier router aging timeout in seconds.
SNOOP QUERIER ENABLE	Indicates if the IGMP Layer 2 Querier feature is enabled.
SNOOP QUERIER ADDRESS	Indicates the IP address of the IGMP Layer 2 querier.
DYNAMIC DOWNGRADE VERSION	Indicates if the switch downgrades the version of IGMP to handle older query messages.
COMPATIBILITY MODE	Indicates if IGMPv3 is compatible with IGMPv2

## Example

The following example displays the status of IGMP snoop.

```
Switch:1#show ip igmp snooping

=====
                        IgmP Snooping - GlobalRouter
=====
IFINDEX  SNOOP   PROXY   SSM     STATIC   ACTIVE   MROUTER
         ENABLE SNOOP   SNOOP   MROUTER MROUTER  EXPIRATION
         ENABLE ENABLE  ENABLE  PORTS    PORTS    TIME
-----
V2       false  false  false
V3       false  false  false
V4       true   false  false
V200    false  false  false

IFINDEX  SNOOP   SNOOP           DYNAMIC   COMPATIBILITY
         QUERIER QUERIER         DOWNGRADE  MODE
         ENABLE  ADDRESS        VERSION
-----
V2       false  0.0.0.0         enable    disable
V3       false  0.0.0.0         enable    disable
V4       true   192.0.2.1       enable    disable
V200    false  0.0.0.0         enable    disable

4 out of 4 entries displayed
```

## show ip igmp snoop-trace

View multicast group trace information for Internet Group Management Protocol (IGMP) snoop.



## Syntax

- `show ip igmp snoop-trace [source <A.B.C.D>] [group <A.B.C.D>]`
- `show ip igmp snoop-trace group {A.B.C.D} vrf WORD<1-16>`
- `show ip igmp snoop-trace group {A.B.C.D} vrfids WORD<0-512>`
- `show ip igmp snoop-trace source {A.B.C.D} vrf WORD<1-16>`
- `show ip igmp snoop-trace source {A.B.C.D} vrfids WORD<0-512>`
- `show ip igmp snoop-trace vrf WORD<1-16>`
- `show ip igmp snoop-trace vrfids WORD<0-512>`

## Command Parameters

`group <A.B.C.D>`

Specifies the multicast group address.

`source <A.B.C.D>`

Specifies the multicast source address.

`vrf WORD<1-16>`

Specifies a VRF by name.

`vrfids <0-512>`

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command is not supported on a node configured as the DvR Leaf within the DvR domain.

## Command Output

The following table shows the field descriptions for the `show ip igmp snoop-trace` command.

Parameter	Description
GROUP ADDRESS	Indicates the IP multicast group address for which this entry contains information.
SOURCE ADDRESS	Indicates the source of the multicast traffic.
IN VLAN	Indicates the incoming VLAN ID.
IN PORT	Indicates the incoming port number.
OUT VLAN	Indicates the outgoing VLAN ID.

Parameter	Description
OUT PORT	Indicates the outgoing port number.
TYPE	Indicates where the stream is learned. ACCESS indicates the stream is learned on UNI ports. NETWORK indicates the stream is learned over the SPBM network.

## Example

The following example displays multicast group trace information for IGMP snoop. Multicast group trace tracks the data flow path of the multicast streams.

```
Switch:1# show ip igmp snoop-trace

=====
                        Snoop Trace - GlobalRouter
=====
GROUP          SOURCE          IN    IN    OUT   OUT   TYPE
ADDRESS        ADDRESS          VLAN  PORT  VLAN  PORT
-----
233.252.0.1    192.0.2.6        500   1/1   500   1/5   ACCESS
233.252.0.10  192.0.2.7        500   1/1   500   1/10  ACCESS
```

## show ip igmp ssm

Display the Source Specific Multicast (SSM) group range and the status of dynamic learning.

## Syntax

- **show ip igmp ssm**
- **show ip igmp ssm vrf WORD<1-16>**
- **show ip igmp ssm vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command is not supported on a node configured as the DVR Leaf within a DVR domain.

## Command Output

The **show ip igmp ssm** command displays the following information:

Output field	Description
DYNAMIC LEARNING	Indicates whether dynamic learning is enabled at a global level.
SSM GROUP RANGE	Indicates the IP address range for the SSM group.

## Example

The following example displays the SSM group range and the status of dynamic learning.

```
Switch:1#show ip igmp ssm
=====
                        Igmp Ssm Global - GlobalRouter
=====
DYNAMIC LEARNING      SSM GROUP RANGE
-----
enable                 232.0.0.0/255.0.0.0
```

## show ip igmp ssm-map

Display the list of Source Specific Multicast (SSM) channels.

## Syntax

- **show ip igmp ssm-map**
- **show ip igmp ssm-map vrf WORD<1-16>**
- **show ip igmp ssm-map vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show ip igmp ssm-map** command displays the following information:

Output field	Description
GROUP	Indicates the IP multicast group address that uses the default range of 232/8.
SOURCE	Indicates the IP address of the source that sends traffic to the group source.
MODE	Indicates that the entry is a statically configured entry (static) or a dynamically learned entry from IGMPv3 (dynamic).
ACTIVE	Indicates the activity on the corresponding source and group. If the source is active and traffic is flowing to the switch, this status is active; otherwise, it is nonactive.
STATUS	Indicates the administrative state and whether to use the entry. If the status is enabled (default), the entry is used. If the status is disabled, the entry is not used but is saved for future use.

## Example

The following example displays the list of SSM maps.

```
Switch:1#show ip igmp ssm-map
=====
                        Igmp Ssm Channel - GlobalRouter
=====
GROUP          SOURCE          MODE          ACTIVE          STATUS
-----
233.252.0.1    192.0.2.200  dynamic      false           enabled
233.252.0.2    192.0.2.200  dynamic      false           enabled
233.252.0.3    192.0.2.200  dynamic      false           enabled
233.252.0.4    192.0.2.200  dynamic      false           enabled
233.252.0.5    192.0.2.200  dynamic      false           enabled
233.252.0.6    192.0.2.200  dynamic      false           enabled
233.252.0.7    192.0.2.200  dynamic      false           enabled
233.252.0.8    192.0.2.200  dynamic      false           enabled
233.252.0.9    192.0.2.200  dynamic      false           enabled
233.252.0.10   192.0.2.200  dynamic      false           enabled

10 out of 10 entries displayed
```

## show ip igmp static

Display information about the static and blocked ports for the Internet Group Management Protocol (IGMP)-enabled interfaces.

## Syntax

- **show ip igmp static**
- **show ip igmp static vrf WORD<1-16>**
- **show ip igmp static vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command is not supported on a node configured as the DvR Leaf within a DvR domain.

## Command Output

The **show ip igmp static** command displays the following information:

Output field	Description
GRPADDR	Indicates the IP multicast address. The group address holds the starting range for the address range.
TO-GRPADDR	Indicates the end of the range for the group address.
INTERFACE	Indicates the interface IP address.
STATICPORTS	Indicates the egressing ports.
BLOCKEDPORTS	Indicates the ports not allowed to join.

## show ip igmp stream-limit

Display multicast stream limitation information for the ports on a specific interface.

## Syntax

- **show ip igmp stream-limit interface**
- **show ip igmp stream-limit interface vrf WORD<1-16>**
- **show ip igmp stream-limit interface vrfids WORD<0-512>**
- **show ip igmp stream-limit port**
- **show ip igmp stream-limit port vrf WORD<1-16>**
- **show ip igmp stream-limit port vrfids WORD<0-512>**

## Command Parameters

### interface

Specifies the type of interface to include in the output. The results display all ports using stream limitation on the selected interface type.

### port

Specifies the Internet Group Management Protocol (IGMP) stream limitation port details.

### vrf WORD<1-16>

Specifies a VRF by name.

### vrfids <0-512>

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show ip igmp stream-limit** command displays the following information:

Field	Description
INTERFACE	Indicates the interface IP address.
PORT	Indicates the port for the VLAN.
MAX STREAMS	Indicates the maximum number of streams.
NUM STREAMS	Indicates the current number of streams.

## show ip igmp sys

View the current fast leave mode configuration and Internet Group Management Protocol (IGMP) system parameters on the switch.

## Syntax

- **show ip igmp sys**
- **show ip igmp sys vrf WORD<1-16>**
- **show ip igmp sys vrfids WORD<0-512>**

## Command Parameters

vrf WORD<1-16>

Specifies a VRF by name.

**vrfids <0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip irdp

---

Confirm that the Router Discovery is enabled.

## Syntax

- **show ip irdp**
- **show ip irdp [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip irdp interface gigabitethernet <1-4059>**
- **show ip irdp interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ip irdp interface vlan**
- **show ip irdp interface vlan <1-4059>**
- **show ip irdp vrf WORD<1-16>**
- **show ip irdp vrfids WORD<0-512>**

## Command Parameters

**interface vlan**

Show route discovery per interface information.

**vrfids WORD<0-512>**

Show route discovery for particular vrfids

## Default

None

## Command Mode

Privileged EXEC

---

## show ip msdp count

---

Display the number of sources and groups originated in MSDP SA messages and the number of SA from an MSDP peer.

### Syntax

- **show ip msdp count vrf WORD<1-16>**
- **show ip msdp count vrfids WORD<0-512>**
- **show ip msdp count WORD<0-11>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a particular VRF. Type a name between 1-16 characters in length.

**vrfids WORD<0-512>**

Specifies the VRF ID.

**WORD<0-11>**

0-65535(2-Byte AS) 0-4294967295(4-Byte AS) Default AS Number: 0

### Default

None

### Command Mode

Privileged EXEC

---

## show ip msdp mesh-group

---

Display the configured Mesh groups.

### Syntax

- **show ip msdp mesh-group vrf WORD<1-16>**
- **show ip msdp mesh-group vrfids WORD<0-512>**
- **show ip msdp mesh-group WORD<1-64>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a particular VRF. Type a name between 1-16 characters in length.

**vrfids WORD<0-512>**

Specifies the VRF ID.



**WORD<1-64>**

Specifies the Mesh group name.

## Default

None

## Command Mode

Privileged EXEC

---

## show ip msdp peer

Display detailed information about the MSDP peer.

## Syntax

- **show ip msdp peer {A.B.C.D}**
- **show ip msdp peer vrf WORD<1-16>**
- **show ip msdp peer vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D}**

Specifies the Peer address.

**vrf WORD<1-16>**

Specifies a particular VRF. Type a name between 1-16 characters in length.

**vrfids WORD<0-512>**

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

---

## show ip msdp rpf

Display the rpf-peer information.

## Syntax

- **show ip msdp rpf {A.B.C.D}**

## Command Parameters

**{A.B.C.D}**

Specifies the RPF address.

**vrf WORD<1-16>**

Specifies a particular VRF. Type a name between 1-16 characters in length.

**vrfids WORD<0-512>**

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip msdp sa-cache

---

Display the (S, G) state that is learned from MSDP peers.

## Syntax

- **show ip msdp sa-cache group {A.B.C.D}**
- **show ip msdp sa-cache local**
- **show ip msdp sa-cache rp {A.B.C.D}**
- **show ip msdp sa-cache source {A.B.C.D}**
- **show ip msdp sa-cache vrf WORD<1-16>**
- **show ip msdp sa-cache vrfids WORD<0-512>**

## Command Parameters

**group {A.B.C.D}**

Specifies all cache entries that match the group address.

**local**

Specifies the local SA cache.

**rp {A.B.C.D}**

Specifies cache entries that match the Rendezvous Point address.

**source {A.B.C.D}**

Specifies cache entries that match the source address.

**vrf WORD<1-16>**

Specifies a particular VRF. Type a name between 1-16 characters in length.

**vrfids WORD<0-512>**

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip msdp sa-check

---

Display the peer info from which a router will accept SA originating from the RP and also check whether the specified(S,G,RP) would be accepted from the peer.

## Syntax

- **show ip msdp sa-check source {A.B.C.D} group {A.B.C.D} rp {A.B.C.D}**
- **show ip msdp sa-check source {A.B.C.D} group {A.B.C.D} rp {A.B.C.D} peer A.B.C.D}**
- **show ip msdp sa-check source {A.B.C.D} group {A.B.C.D} rp {A.B.C.D} vrf WORD<0-16>**
- **show ip msdp sa-check source {A.B.C.D} group {A.B.C.D} rp {A.B.C.D} vrfids WORD<0-512>**

## Command Parameters

**group {A.B.C.D}**

Specifies the group IP address.

**peer {A.B.C.D}**

Specifies the MSDP peer IP address.

**rp {A.B.C.D}**

Specifies the RP IP address.

**source {A.B.C.D}**

Specifies the source IP address.

**vrf WORD<0-16>**

Specifies a particular VRF. Type a name between 0-16 characters in length.

**vrfids WORD<0-512>]**

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip msdp show-all

---

Display a collection of show commands output of MSDP protocol.

### Syntax

- **show ip msdp show-all file WORD<1-99>**
- **show ip msdp show-all vrf WORD<1-16>**
- **show ip msdp show-all vrfids WORD<0-512>**

### Command Parameters

**file WORD<1-99>**

Specifies the filename - {/intflash/ } <file> {string length 1...99}.

**vrf WORD<1-16>**

Specifies a particular VRF. Type a name between 1-16 characters in length.

**vrfids WORD<0-512>**

Specifies the VRF ID.

### Default

None

## Command Mode

Privileged EXEC

## show ip msdp summary

---

Display the MSDP global status and peer status.

### Syntax

- **show ip msdp summary vrf WORD<1-16>**
- **show ip msdp summary vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a particular VRF. Type a name between 1-16 characters in length.

**vrfids WORD<0-512>**

Specifies the VRF ID.

## Default

None

## Command Mode

Privileged EXEC

## show ip redistribute

---

Display and ensure the accuracy of the configuration settings.

## Syntax

- **show ip <rip|ospf|bgp> redistribute [interface] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**<ospf|bgp|static|direct|rip>**

Specifies the type of routes to redistribute-the protocol source.

**interface**

Shows rip information for each interface.

**vrf WORD<1-16>**

Displays rip configuration for a particular VRF.

**vrfids WORD<0-512>**

Specifies a list of VRF IDs.

## Default

None

## Command Mode

Privileged EXEC

## show ipv6 fhs statistics

---

Displays the FHS statistics on a port or set of ports.

## Syntax

- **show ipv6 fhs statistics all**
- **show ipv6 fhs statistics all {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ipv6 fhs statistics dhcp-guard**
- **show ipv6 fhs statistics dhcp-guard {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ipv6 fhs statistics nd-inspection**
- **show ipv6 fhs statistics nd-inspection {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ipv6 fhs statistics ra-guard**
- **show ipv6 fhs statistics ra-guard {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Displays the statistics on either a single port or a set of ports.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### **all**

Displays all IPv6 FHS statistics.

### **dhcp-guard**

Displays DHCP-Guard statistics.

### **nd-inspection**

Displays Neighbor Discovery Inspection statistics.

### **ra-guard**

Displays RA-Guard statistics.

## Default

None

## Command Mode

Privileged EXEC

## show ipv6 isis accept

Displays the IPv6 IS-IS Accept Policy Information.

## Syntax

- **show ipv6 isis accept**
- **show ipv6 isis accept vrf WORD<1-16>**
- **show ipv6 isis accept vrf WORD<1-16> vrfids WORD<0-512>**
- **show ipv6 isis accept vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Displays the IPv6 IS-IS Accept Policy Information for a specific VRF.

**vrfids WORD<0-512>**

Displays the IPv6 IS-IS Accept Policy Information for a specific VRF ID.

## Default

None

## Command Mode

Privileged EXEC

## show ipv6 isis redistribute

---

Display the rules for redistribution of routes into ISIS for GRT.

## Syntax

- **show ipv6 isis redistribute**
- **show ipv6 isis redistribute vrf WORD<1-16>**
- **show ipv6 isis redistribute vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

## Default

The default is disabled.

## Command Mode

Privileged EXEC

## show ipv6 ospf default-cost

---

Display the IPv6 OSPF default cost information to ensure accuracy.

### Syntax

- **show ipv6 ospf default-cost [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf default-cost vrf WORD<1-16>**
- **show ipv6 ospf default-cost vrfids WORD<0-512>**

### Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

### Default

None

## Command Mode

Privileged EXEC

## show ipv6 ospf ipsec

---

Display the IPv6 OSPF IPsec information to ensure accuracy.

### Syntax

- **show ipv6 ospf ipsec [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf ipsec vrf WORD<1-16>**
- **show ipv6 ospf ipsec vrfids WORD<0-512>**

### Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.



## Default

None

## Command Mode

Privileged EXEC

## show ipv6 ospf vrf

---

Display the IPv6 OSPF configuration for a particular VRF.

## Syntax

- **show ipv6 ospf vrf WORD<1-16>**
- **show ipv6 ospf vrf WORD<1-16> vrfids WORD<0-512>**

## Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

Privileged EXEC

## show ipv6 ospf vrfids

---

Display the IPv6 OSPF configuration for VRFs by VRF ID.

## Syntax

- **show ipv6 ospf vrfids WORD<0-512>**

## Command Parameters

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

Privileged EXEC

## show ipv6 rip redistribute

---

Display ripng redistribute parameters

## Syntax

- **show ipv6 rip redistribute**

## Default

None

## Command Mode

Privileged EXEC

## show link-flap-detect

---

Show link-flap-detect configuration.

## Syntax

- **show link-flap-detect**

## Default

None

## Command Mode

Privileged EXEC

## show lldp

---

Display LLDP information.

## Syntax

- **show lldp**
- **show lldp location-identification**

## Command Parameters

### location-identification

Specifies the location information parameters.

## Default

None

## Command Mode

Privileged EXEC

---

## show lldp local-sys-data

Display LLDP local system data.

## Syntax

- **show lldp local-sys-data**
- **show lldp local-sys-data med**

## Command Parameters

### med

Displays local LLDP-MED information.

## Default

None

## Command Mode

Privileged EXEC

---

## show lldp med-network-policies

Displays LLDP-MED network policies.

## Syntax

- **show lldp med-network-policies**
- **show lldp med-network-policies guest-voice**
- **show lldp med-network-policies guest-voice-signaling**
- **show lldp med-network-policies softphone-voice**
- **show lldp med-network-policies streaming-video**

- **show lldp med-network-policies video-conferencing**
- **show lldp med-network-policies video-signaling**
- **show lldp med-network-policies voice**
- **show lldp med-network-policies voice-signaling**

## Command Parameters

### guest-voice

Specifies the type of LLDP-MED network policy.

### guest-voice-signaling

Specifies the type of LLDP-MED network policy.

### softphone-voice

Specifies the type of LLDP-MED network policy.

### streaming-video

Specifies the type of LLDP-MED network policy.

### video-conferencing

Specifies the type of LLDP-MED network policy.

### video-signaling

Specifies the type of LLDP-MED network policy.

### voice

Specifies the type of LLDP-MED network policy.

### voice-signaling

Specifies the type of LLDP-MED network policy.

## Default

None

## Command Mode

Privileged EXEC

## show lldp neighbor

---

Display details of LLDP neighbors learned.

## Syntax

- **show lldp neighbor**
- **show lldp neighbor port {slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]} [med]**

- **show lldp neighbor summary** [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]]] [med]

## Command Parameters

### med

Displays LLDP neighbors learned based on LLDP-MED TLV information.

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### summary

Displays the summary of the LLDP neighbors on a single port or a range of ports.

## Default

None

## Command Mode

Privileged EXEC

## show lldp neighbor vendor-specific

---

Show the remote LLDP vendor-specific call server and file server information.

## Syntax

- **show lldp neighbor vendor-specific call-server**
- **show lldp neighbor vendor-specific file-server**

## Command Parameters

### call-server

Displays the remote LLDP vendor-specific call server information.

### file-server

Displays the remote LLDP vendor-specific file server information.

## Default

None

## Command Mode

Privileged EXEC

## show lldp port

Display LLDP port list.

### Syntax

- **show lldp port**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
location-identification**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies guest-voice**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies guest-voice-signaling**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies softphone-voice**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies streaming-video**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies video-conferencing**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies video-signaling**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies voice**
- **show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}  
med-network-policies voice-signaling**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### location-identification

Specifies the location information parameters for specific ports.

**med-network-policies [guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling]**

Displays the LLDP-MED network policies configured on specific ports.

## Default

None

## Command Mode

Privileged EXEC

## show lldp rx-stats

---

Verify that the port is receiving LLDP PDUs successfully.

## Syntax

- **show lldp rx-stats**
- **show lldp rx-stats {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**port** *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## show lldp stats

---

Verify LLDP statistics.

## Syntax

- **show lldp stats**

## Default

None

## Command Mode

Privileged EXEC

## show lldp tx-stats

---

Verify successful LLDP transmission on a port.

### Syntax

- **show lldp tx-stats**
- **show lldp tx-stats {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

## Command Mode

Privileged EXEC

## show lldp tx-tlv

---

Display Link Layer Discovery Protocol (LLDP) transmission TLVs.

### Syntax

- **show lldp tx-tlv**

### Default

None

## Command Mode

Privileged EXEC



## Command Output

The **show lldp tx-tlv** command displays the following information:

Output field	Description
Port	Specifies the port number.
PortDesc	Specifies the port description transmission TLV. The default is enabled.
SysName	Specifies the system capabilities transmission TLV. The default is enabled.
SysDesc	Specifies the system description transmission TLV. The default is enabled.
SysCap	Specifies the system name transmission TLV. The default is enabled.

```
Switch:1(config-if)#show lldp tx-tlv
=====
                        LLDP port tlvs
=====
-----
Port          PortDesc   SysName   SysDesc   SysCap
-----
1/1           enabled   enabled   enabled   enabled
1/2           enabled   enabled   enabled   enabled
1/3/1        enabled   enabled   enabled   enabled
1/3/2        enabled   enabled   enabled   enabled
1/3/3        enabled   enabled   enabled   enabled
1/3/4        enabled   enabled   enabled   enabled
1/4           enabled   enabled   enabled   enabled
1/5           enabled   enabled   enabled   enabled
1/6           enabled   enabled   enabled   enabled
1/7           enabled   enabled   enabled   enabled
1/8           enabled   enabled   enabled   enabled
1/9           enabled   enabled   enabled   enabled
1/10         enabled   enabled   enabled   enabled
```

## show lldp tx-tlv dot3

Display dot3 MAC/PHY configuration/status Link Layer Discovery Protocol (LLDP) TLVs.

### Syntax

- **show lldp tx-tlv dot3**

### Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show lldp tx-tlv dot3** command displays the following information:

Output field	Description
Port	Specifies the port number.
MAC Physical Config Status	Specifies the status of the MAC Physical Config Status TLV. The default is disabled.

```
Switch:1(config-if)#show lldp tx-tlv dot3
=====
                        LLDP port dot3 tlvs
=====
Port          MAC Physical
              Config Status
-----
1/1           disabled
1/2           enabled
1/3           enabled
1/4           disabled
1/5           disabled
```

## show lldp tx-tlv med

Display Link Layer Discovery Protocol (LLDP) Media Endpoint Device (MED) TLV interface information.

## Syntax

- **show lldp tx-tlv med**

## Command Parameters

**port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show lldp tx-tlv med** command displays the following information:

Output field	Description
Port	Specifies the port number.
MedCapabilities	Specifies the system name MED transmission TLV.
NetworkPolicy	Specifies the network policy MED transmission TLV.
Location	Specifies the system description MED transmission TLV.
ExtendedPowerViaMDI	Specifies the extended power-via-MDI Media Endpoint Device (MED) transmission TLV. This TLV is applicable for POE-capable switches only.
Inventory	Specifies the system capabilities MED transmission TLV.

## Example

```
Switch:1#show lldp tx-tlv med
```

```
=====
                        LLDP port med tlvs
=====
-----
Port           Med           Network   Location   ExtendedPower  Inventory
              Capabilities  Policy
              -----
1/1            enabled      enabled   enabled   enabled        enabled
1/2            enabled      enabled   enabled   enabled        enabled
-----
```

## show lldp tx-tlv port

Display Link Layer Discovery Protocol (LLDP) transmission TLVs for transmission on a specific port.

## Syntax

- **show lldp tx-tlv port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show lldp tx-tlv port** command displays the following information:

Output field	Description
Port	Specifies the port number.
PortDesc	Specifies the port description transmission TLV.
SysName	Specifies the system capabilities transmission TLV.
SysDesc	Specifies the system description transmission TLV.
SysCap	Specifies the system name transmission TLV.

```
Switch:1(config-if)#show lldp tx-tlv port 1/2
=====
                        LLDP port tlvs
=====
-----
Port      PortDesc  SysName   SysDesc   SysCap
-----
1/2      enabled   enabled   enabled   enabled
```

## show lldp vendor-specific

Shows lldp vendor-specific call server or file server information.

## Syntax

- **show lldp vendor-specific call-server**
- **show lldp vendor-specific file-server**

## Command Parameters

### call-server

Displays the LLDP vendor-specific call server information.

### file-server

Displays the LLDP vendor-specific file server information.

## Default

None

## Command Mode

Privileged EXEC

---

## show mac-address-entry

Shows the database status and MAC address to display the static forwarding database status.

## Syntax

- **show mac-address-entry**

## Default

None

## Command Mode

Privileged EXEC

---

## show pluggable-optical-modules

View Digital Diagnostic Interface (DDI) module information to view transceiver manufacturing information and characteristics, temperature and voltage information, and configuration details.

## Syntax

- **show pluggable-optical-modules basic**
- **show pluggable-optical-modules basic {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show pluggable-optical-modules config**
- **show pluggable-optical-modules detail**
- **show pluggable-optical-modules detail {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show pluggable-optical-modules temperature**
- **show pluggable-optical-modules temperature {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show pluggable-optical-modules voltage**
- **show pluggable-optical-modules voltage {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### basic

Shows basic transceiver information.

### config

Shows pluggable optical modules configuration information.

### detail

Shows detailed transceiver information. Use this parameter to see extended diagnostic information for supported Extreme parts.

### temperature

Shows transceiver temperature information.

### voltage

Shows transceiver voltage information.

## Default

None

## Command Mode

Privileged EXEC

## show poe-main-status

---

View main PoE status.

## Syntax

- **show poe-main-status**

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show poe-port-status

---

View port PoE status.

### Syntax

- **show poe-port-status**

### Default

None

### Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show poe-power-measurement

---

View PoE power measurement per port.

### Syntax

- **show poe-power-measurement {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show ports statistics ospf extended

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

## Syntax

- **show ports statistics ospf extended {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show ports statistics ospf extended** command displays the following information:

Output field	Description
PORT_NUM	Indicates the port number.
RXLS_REQS	Indicates the number of link state update request packets received by this interface.
TXLS_REQS	Indicates the number of link state request packets transmitted by this interface.



Output field	Description
RXLS_ACKS	Indicates the number of link state acknowledge packets received by this interface.
TXLS_ACKS	Indicates the number of link state acknowledge packets transmitted by this interface.

## show ports statistics ospf main

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

### Syntax

- **show ports statistics ospf main {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

Privileged EXEC

### Command Output

The **show ports statistics ospf main** command displays the following information:

Output field	Description
PORT NUM	Indicates the port number.
RX_HELLO	Indicates the number of hello packets this interface receives.
TX_HELLO	Indicates the number of hello packets this interface transmitted.
RXDB_DESCR	Indicates the number of database descriptor packets this interface receives.
TXDB_DESCR	Indicates the number of database descriptor packets this interface transmitted.

Output field	Description
RXLS_UPDATE	Indicates the number of link state update packets this interface receives.
TXLS_UPDATE	Indicates the number of link state update packets this interface transmitted.

## show qos policer

---

Display ingress rate-limiting information for an interface.

### Syntax

- **show qos policer interface gigabitEthernet** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]]

### Command Parameters

**interface gigabitEthernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

Privileged EXEC

## show routing statistics

---

View port routing statistics to manage network performance.

### Syntax

- **show routing statistics interface**
- **show routing statistics interface gigabitEthernet** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]]

### Command Parameters

**gigabitEthernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

Privileged EXEC

## Command Output

The **show routing statistics interface** command displays the following information:

Output field	Description
PORT NUM	Indicates the port number.
IN_FRAME UNICAST	The count of inbound unicast frames.
IN_FRAME MULTICAST	The count of inbound multicast frames.
IN DISCARD	The count of inbound discarded frames.
OUT_FRAME UNICAST	The count of outbound unicast frames.
OUT_FRAME MULTICAST	The count of outbound multicast frames.

## show running-config

Display the current switch configuration.

## Syntax

- **show running-config**
- **show running-config module {app-telemetry | boot | cfm | cli | diag | dvr | eap | endpoint-tracking | energy-saver | fa | fhs | filter | ike | ip | ipfix | ipsec | ipv6 | iqagent | isis | i-sid | lacp | license | lldp | lst | macsec | mlt | naap | nls | ntp | ovssdb | port | qos | radius | restconf | rmon | sflow | security | slamon | slpp | smtp | spbm | stg | sys | tacacs | virtualservice | vlan | web | vxlan}**
- **show running-config verbose**

## Command Parameters

module {app-telemetry | boot | cfm | cli | diag | dvr | eap | endpoint-tracking | energy-saver | fa | fhs | filter | ike | ip | ipfix | ipsec | ipv6 | iqagent | isis | i-sid | lacp | license | lldp | lst | macsec | mlt |

naap | nls | ntp | ovsdb | port | qos | radius | restconf | rmon | sflow | security | slamon | slpp | smtp  
| spbm | stg | sys | tacacs | virtualservice | vlan | web | vxlan}

Specifies the command group for which you request configuration settings.

#### verbose

Specifies the complete list of configuration information on the switch.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

All configuration modules are not supported on all hardware platforms. For information about feature support, see [VOSS Feature Support Matrix](#).



#### Note

The output from the **show running-config** command displays an "end statement" near the end of the configuration file. This statement means that the script is exiting the Global Configuration mode and loading the rest of the configuration in Privileged EXEC mode, which is a requirement when loading the IP redistribution commands.

If you add **verbose** to the **show running-config** command, the output contains current switch configuration including software (versions), performance, VLANs (numbers, port members), ports (type, status), routes, memory, interface, and log and trace files. With the verbose command, you can view the current configuration and default values.

## Example

If you make a change to the switch configuration, it displays under the specific configuration heading. The following example displays a subset of the output of this command.

```
VSP-8284XSQ:1#show running-config
Preparing to Display Configuration...
#
# Sat Mar 13 14:35:01 2021 UTC
# box type           : VSP-8284XSQ
# software version   : 8.4.0.0
# cli mode           : ECLI
#
#Card Info :
# Slot 1 :
#   CardType         : 8242XSQ
#   CardDescription  : 8242XSQ
#   CardSerial#      : 14JP455C1029
#   CardPart#        : EC8200A01-E6
#   CardAssemblyDate : 20141106
```

```
#      CardHWRevision   : 1
#      CardHWConfig     :
#      AdminStatus      : up
#      OperStatus       : up

# Slot 2 :
#      CardType          : 8242XSQ
#      CardDescription   : 8242XSQ
#      CardSerial#       : 14JP455C1029
#      CardPart#         : EC8200A01-E6
#      CardAssemblyDate  : 20141106
#      CardHWRevision   : 1
#      CardHWConfig     :
#      AdminStatus      : up
#      OperStatus       : up

#
#!end
#
config terminal

#
# BOOT CONFIGURATION
#

boot config flags ftpd
boot config flags sshd
boot config flags telnetd

#boot config sio console baud 9600 1
# end boot flags
```

## show slot

Show slot configuration.

### Syntax

- **show slot**
- **show slot <1>**

### Command Parameters

<1>

Specifies the interface slot number <1>.

### Default

None

### Command Mode

Privileged EXEC

---

## show vlan src-mac

---

View the VLAN source MAC addresses to display the source MAC address for any source MAC-based VLANs on the switch or for the specified VLAN.

### Syntax

- **show vlan src-mac <1-4059>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

Privileged EXEC

---

## show vnid i-sid

---

Display information about all the VNIDs or use the option to specify a particular VNID.

### Syntax

- **show vnid i-sid {<1-500>}**

### Command Parameters

<1-500>

Displays information about the specified VNID.

### Default

None

### Command Mode

Privileged EXEC

---

## show vnid mac-address-entry

---

Display all the VNIDs in the FDB table or use one of the options to specify a particular VNID.

### Syntax

- **show vnid mac-address-entry** [**<1-16777215>** | **port** **<{slot/port[-slot/port]}[,...]>** | **mac** **<0x00:0x00:0x00:0x00:0x00:0x00>** | **remote**]

### Command Parameters

**<1-16777215>** | **port** **<{slot/port [-slot/port]}[,...]>** | **mac** **<0x00:0x00:0x00:0x00:0x00:0x00>** | **remote**]

Display the FDB table for the specified VNID.

### Default

None

### Command Mode

Privileged EXEC

---

## show vtep local

---

Display the VTEP's source IP address and the name of the VRF.

### Syntax

- **show vtep local**

### Default

None

### Command Mode

Privileged EXEC

---

## show vtep remote

---

Display information about all of the remote VTEPs or use the option to specify a particular VTEP.

### Syntax

- **show vtep remote** [**<1-500>**]

## Command Parameters

<1-500>

Displays information about the specified remote VTEP.

## Default

None

## Command Mode

Privileged EXEC

---

## show vtep remote name

Display the names of all remote VTEPs or use the option to specify a particular VTEP.

## Syntax

- **show vtep remote name [<1-500>]**

## Command Parameters

<1-500>

Displays the name of the specified remote VTEP.

## Default

None

## Command Mode

Privileged EXEC

---

## software

Perform various software functions on the switch to ensure it is updated with latest versions.

## Syntax

- **software activate WORD<1-99>**
- **software add WORD<1-99> [-y]**
- **software add-modules WORD<1-99>**
- **software commit**
- **software iqagent reinstall**
- **software remove WORD<1-99>**



## Command Parameters

### activate WORD<1-99>

Copies the software version to the boot flash file. When you use the software activate command, the system checks for hardware dependencies and prevents a downgrade if it detects a dependency. For example, if a hardware component has a minimum software version dependency, you cannot downgrade to an incompatible software version or install the hardware component in a chassis that runs an incompatible software version.

### add WORD<1-99>

Unpacks a software release <version>.

### add-modules WORD<1-99>

Add modules to existing software release in /intflash/release/<version>

### commit

Ensures the running software release is trusted.

### iqagent reinstall

Returns the ExtremeCloud IQ Agent firmware version on the switch to the version bundled with the VOSS image currently installed on the switch.

### remove WORD<1-99>

Removes the software release <version>.

### -y

Suppresses the confirmation message to automatically overwrite the non-primary image. If you omit this parameter, you must confirm the action to overwrite the non-primary image.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

The `-y` parameter is supported on 5420 Series only.

## software reset-commit-time

---

Extends or reduces the commit time after you apply a software upgrade. You may need additional time to verify the software works as expected after the upgrade before you commit or roll back.

## Syntax

- **software reset-commit-time**
- **software reset-commit-time <1-60>**

## Command Parameters

<1-60>

Extends or reduces the commit timer. By default, the commit timer is 10 minutes. As an example, if you enter the command string of software reset-commit-time 5, you reduce the commit timer to 5 minutes. If you enter the command string of software reset-commit-time 25, you extend the commit timer by 15 minutes, for a total of 25 minutes.

## Default

The default is 10 minutes.

## Command Mode

Privileged EXEC

## source

---

Source a configuration to merge a script file into the running configuration or verify the syntax of a configuration file.



### Warning

You are not able to source a complete configuration file to merge it with your running configuration because the system can crash. Use the source command to merge smaller portions of a configuration into the existing configuration.



### Important

Do not source a verbose configuration (verbose.cfg) with the debug stop option. The sourcing process cannot complete if you use these two options with a verbose configuration.

## Syntax

- **source WORD<1-99>**
- **source WORD<1-99> debug**
- **source WORD<1-99> debug stop**
- **source WORD<1-99> debug stop syntax**
- **source WORD<1-99> debug syntax**
- **source WORD<1-99> stop**
- **source WORD<1-99> stop syntax**
- **source WORD<1-99> syntax**

## Command Parameters

debug

Debugs the script by outputting the configuration commands to the screen.

**stop**

Stops the sourcing of a configuration if an error occurs.

**syntax**

Checks the syntax of the configuration file. This parameter does not load the configuration file; only verifies the syntax.

If you use this parameter with the stop parameter (source WORD<1-99> stop syntax), the system displays the output on screen and verification stops if it encounters an error.

If you use this parameter with the debug parameter (source WORD<1-99> debug syntax), the output does not stop if it encounters an error; you must review the on-screen output to verify if an error exists.

If you use this parameter by itself, it does not output to the screen or stop on error; it shows an error message, "syntax errors in script", to indicate if errors exist in the configuration file.

**WORD<1-99>**

Specifies a filename and location.

**Default**

None

**Command Mode**

Privileged EXEC

**sys action**

---

Reset system functions to reset all statistics counters, the console port, and the operation of the switchover function.

**Syntax**

- **sys action reset {console | counters}**
- **sys action reset console**
- **sys action reset counters**

**Command Parameters****reset {console|counters}**

Reinitializes the hardware universal asynchronous receiver transmitter (UART) drivers. Use this command only if the console connection stops responding. Resets all the statistics counters in the switch to zero. Resets the console port.

**Default**

None

## Command Mode

Privileged EXEC

## sys shutdown

---

Use this command to prepare the system for shutdown. This command properly shuts down the file system, and powers off all interface modules. After you use this command, you must physically disconnect the chassis power. To restore power after you use this command, you must physically turn the chassis power on again.

### Syntax

- **sys shutdown**

### Default

None

## Command Mode

Privileged EXEC

## trace ipv6 base

---

Configure trace parameters for the IPv6 base.

### Syntax

- **trace ipv6 base disable {all|debug|error|icmp|info|ipclient|nbr|pkt|warn} [vrf WORD<1-16>]**
- **trace ipv6 base enable {all|debug|error|icmp|info|ipclient|nbr|pkt|warn} [vrf WORD<1-16>]**

### Command Parameters

**<all|debug|error|icmp|info|ipclient|nbr|pkt|warn>**

Specifies the trace category.

**disable**

Disables the trace.

**enable**

Enables the trace.

**vrf WORD<1-16>**

Specifies VRF by name.

## Default

None

## Command Mode

Privileged EXEC

# trace ipv6 forwarding

---

Configure trace parameters for IPv6 forwarding.

## Syntax

- **trace ipv6 forwarding disable** {all|debug|error|info|pkt|warn} [vrf WORD<1-16>]
- **trace ipv6 forwarding enable** {all|debug|error|info|pkt|warn} [vrf WORD<1-16>]

## Command Parameters

<all|debug|error|info|pkt|warn>

Specifies the trace category.

**disable**

Disables the trace.

**enable**

Enables the trace.

**vrf WORD<1-16>**

Specifies VRF by name.

## Default

None

## Command Mode

Privileged EXEC

# trace ipv6 nd

---

Configure trace parameters for IPv6 neighbor discovery.

## Syntax

- `trace ipv6 nd disable {all|debug|error|info|nbr|pkt|redirect|warn} [vrf WORD<1-16>]`
- `trace ipv6 nd disable {all|debug|error|info|nbr|pkt|redirect|warn} [vrf WORD<1-16>]`
- `trace ipv6 nd enable {all|debug|error|info|nbr|pkt|redirect|warn} [vrf WORD<1-16>]`
- `trace ipv6 nd enable {all|debug|error|info|nbr|pkt|redirect|warn} [vrf WORD<1-16>]`

## Command Parameters

`<all|debug|error|info|nbr|pkt|redirect|warn>`

Specifies the trace category.

`disable`

Disables the trace.

`enable`

Enables the trace.

`vrf WORD<1-16>`

Specifies VRF by name.

## Default

None

## Command Mode

Privileged EXEC

## trace ipv6 ospf

---

Configure trace parameters for IPv6 OSPF.

## Syntax

- `trace ipv6 ospf disable {all|debug|error|info|nbr|pkt|redirect|warn} [vrf WORD<1-16>]`
- `trace ipv6 ospf enable {all|debug|error|info|nbr|pkt|redirect|warn} [vrf WORD<1-16>]`

## Command Parameters

`<all|debug|error|info|nbr|pkt|redirect|warn>`

Specifies the trace category.

**disable**

Disables the trace.

**enable**

Enables the trace.

**vrf WORD<1-16>**

Specifies VRF by name.

## Default

None

## Command Mode

Privileged EXEC

## trace ipv6 rtm

---

Configure trace parameters for the IPv6 routing table manager.

## Syntax

- **trace ipv6 rtm disable {all|change-list|debug|error|fib|info|redist|update|warn} [vrf WORD<1-16>]**
- **trace ipv6 rtm enable {all|change-list|debug|error|fib|info|redist|update|warn} [vrf WORD<1-16>]**

## Command Parameters

<all|changelist|debug|error|fib|info|redist|update|warn>

Specifies the trace category.

**disable**

Disables the trace.

**enable**

Enables the trace.

**vrf WORD<1-16>**

Specifies VRF by name.

## Default

None

## Command Mode

Privileged EXEC

## trace ipv6 transport

---

Configure trace parameters for IPv6 transport.

### Syntax

- **trace ipv6 transport disable** {all|common|tcp|udp} [vrf WORD<1-16>]
- **trace ipv6 transport enable** {all|common|tcp|udp} [vrf WORD<1-16>]

### Command Parameters

<all|common|tcp|udp>

Specifies the trace category.

**disable**

Disables the trace.

**enable**

Enables the trace.

**vrf WORD<1-16>**

Specifies VRF by name.

### Default

None

### Command Mode

Privileged EXEC

## traceroute

---

Use traceroute to determine the route packets take through a network to a destination.

### Syntax



#### Note

Command parameters for **traceroute** varies depending on the parameter input order. All syntax possibilities are not listed. You can use the CLI help to verify the syntax for available parameters during command contextual input.

- **traceroute WORD<0-256>**
- **traceroute WORD<0-256> <1-1176>**
- **traceroute WORD<0-256> <1-1176> mgmt clip**
- **traceroute WORD<0-256> <1-1176> mgmt oob**
- **traceroute WORD<0-256> <1-1176> mgmt vlan**



- `traceroute WORD<0-256> <1-1444>`
- `traceroute WORD<0-256> grt`
- `traceroute WORD<0-256> grt source`
- `traceroute WORD<0-256> -m <1-255>`
- `traceroute WORD<0-256> -m <1-255> mgmt clip`
- `traceroute WORD<0-256> -m <1-255> mgmt oob`
- `traceroute WORD<0-256> -m <1-255> mgmt vlan`
- `traceroute WORD<0-256> -p <0-65535>`
- `traceroute WORD<0-256> -p <0-65535> mgmt clip`
- `traceroute WORD<0-256> -p <0-65535> mgmt oob`
- `traceroute WORD<0-256> -p <0-65535> mgmt vlan`
- `traceroute WORD<0-256> -q <1-255>`
- `traceroute WORD<0-256> -q <1-255> mgmt clip`
- `traceroute WORD<0-256> -q <1-255> mgmt oob`
- `traceroute WORD<0-256> -q <1-255> mgmt vlan`
- `traceroute WORD<0-256> source WORD<1-256>`
- `traceroute WORD<0-256> -v`
- `traceroute WORD<0-256> vrf WORD<1-16>`
- `traceroute WORD<0-256> -w <1-255>`
- `traceroute WORD<0-256> -w <1-255> mgmt clip`
- `traceroute WORD<0-256> -w <1-255> mgmt oob`
- `traceroute WORD<0-256> -w <1-255> mgmt vlan`

## Command Parameters

### <1-1444>

Specifies the size of the probe packet. The range depends on the hardware platform.

### grt

Specifies traceroute is executed in Global Router (GRT) context.



#### Note

Exception: not supported on VSP 8600 Series.

### -m <1-255>

Specifies the is maximum time-to-live (TTL).

### mgmt

Run a traceroute test using a zero source IP address and route lookup in the main table.

### mgmt clip

Run a traceroute test using a Segmented Management Instance. If you do not use the mgmt parameter, the traceroute command uses the IP routing stack to initiate the traceroute request.

**mgmt oob**

Run a traceroute test using a Segmented Management Instance. If you do not use the `mgmt` parameter, the traceroute command uses the IP routing stack to initiate the traceroute request.

**mgmt vlan**

Run a traceroute test using a Segmented Management Instance. If you do not use the `mgmt` parameter, the traceroute command uses the IP routing stack to initiate the traceroute request.

**-p <1-65535>**

Specifies the base UDP port number.

**Note**

If you send a traceroute command to a Segmented Management Interface or VOSS interface address, you must use a UDP port range of 33434-33534.

**-q <1-255>**

Specifies the number of probes per TTL.

**source WORD<1-256>**

Specifies the source IP address for use in traceroutes.

**-v**

Specifies verbose mode (detailed output).

**vrf WORD<1-16>**

Specifies the VRF instance by VRF name.

**-w <1-255>**

Specifies the wait time per probe.

**WORD<0-256>**

Specifies the hostname, or IP address.

**WORD<0-256> <1-1176>**

Specifies the wait time per probe. The range depends on the hardware platform.

**WORD<0-256> -m <1-255>**

Specifies the is maximum time-to-live (TTL).

**WORD<0-256> -p <1-65535>**

Specifies the base UDP port number.

**WORD<0-256> -q <1-255>**

Specifies the number of probes per TTL.

**WORD<0-256> source WORD<1-256>**

Source address for trace route.

**WORD<0-256> -v**

Specifies verbose mode (detailed output).

**WORD<0-256> vrf WORD<1-16>**

Vrf name (IPv4 only).

**WORD<0-256> -w <1-255>**

Specifies the source IP address for use in traceroutes.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

The options [-v], [source], and [vrf] are not available if the *mgmt* keyword is specified.

The command parameters do not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## uboot-install

---

Upgrade the boot loader image. Only use this command if specifically advised to do so by Technical Support. Improper use of this command can result in permanent damage to the device and render it unusable.

## Syntax

- **uboot-install WORD<1-99>**

## Command Parameters

**WORD<1-99>**

Specifies the full path and filename that contains the uboot image. This command is not available on all hardware platforms.

## Default

None

## Command Mode

Privileged EXEC

## usb-stop

---

Use this command to safely remove the USB drive from the USB port.

## Syntax

- **usb-stop**

## Default

None

## Command Mode

Privileged EXEC

---

## virtual-service

Configures virtual service on the switch.

## Syntax

- **virtual-service WORD<1-128> console**

## Command Parameters

**console**

Accesses the console for the specific virtual.

**WORD<1-128>**

Specifies the virtual service name.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## virtual-service copy-file WORD<1-256> WORD<1-256>

Copies a file between VOSS and a VM or between VMs.

## Syntax

- **virtual-service copy-file WORD<1-256> WORD<1-256>**

## Command Parameters

WORD<1-256> WORD<1-256>

Specifies the source and destination file to copy.

To specify a VM location, use the format <VM\_name>:<VM\_file\_path/filename>.

To specify a VOSS location, use the format </file\_path/filename> where the valid path can be one of the following:

- /intflash
- /extflash
- /usb
- /var/lib/insight/packages

## Default

None.

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## virtual-service WORD<1-128> install

---

Installs the virtual service package.

## Syntax

- **virtual-service WORD <1-128> install package WORD<1-512>**

## Command Parameters

package WORD<1-512>

Specifies the package to be installed.

WORD<1-128>

Specifies the virtual service name.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## virtual-service WORD<1-128> uninstall

---

Uninstalls the virtual service.

## Syntax

- **virtual-service WORD<1-128> uninstall**

## Command Parameters

**WORD<1-128>**

Specifies the virtual service name.

## Default

None

## Command Mode

Privileged EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## write memory

---

Save to memory.

## Syntax

- **write memory**

## Default

None

## Command Mode

Privileged EXEC



# RA-guard Configuration

---

The following topics document commands available in RA-guard Configuration mode of the command line interface (CLI).

## hop-limit maximum

---

Enables verification of the advertised hop count limit.

### Syntax

- **default hop-limit maximum**
- **hop-limit maximum <0-255>**

### Command Parameters

<0-255>

Specifies hop limit count.

### Default

The default maximum limit is 0.

### Command Mode

RA-guard Configuration

## hop-limit minimum

---

Enables verification of the advertised hop count limit.

### Syntax

- **default hop-limit minimum**
- **hop-limit minimum <0-255>**

### Command Parameters

<0-255>

Specifies hop limit count.



## Default

The default minimum limit is 0.

## Command Mode

RA-guard Configuration

## managed-config-flag

---

Enables verification of managed address configuration flag in the advertised RA packet.

## Syntax

- **default managed-config-flag**
- **managed-config-flag <none | on | off>**

## Command Parameters

### none

Set managed config flag to none.

### off

Set managed config flag to off.

### on

Set managed config flat to on.

## Default

None

## Command Mode

RA-guard Configuration

## match ra-macaddr-list

---

Enables verification of the sender Source MAC address against the configured mac-access-list.

## Syntax

- **default match ra-macaddr-list**
- **match ra-macaddr-list WORD<1-64>**
- **no match ra-macaddr-list**

## Command Parameters

WORD<1-64>

Specifies the MAC access list name.

## Default

None

## Command Mode

RA-guard Configuration

---

## match ra-prefix-list

Enables verification of the advertised prefixes in inspected messages against the configured authorized prefix list.

## Syntax

- **default match ra-prefix-list**
- **match ra-prefix-list WORD<1-64>**
- **no match ra-prefix-list**

## Command Parameters

WORD<1-64>

Specifies the prefix list name.

## Default

None

## Command Mode

RA-guard Configuration

---

## match ra-srcaddr-list

Enables verification of the sender's IPv6 address in inspected messages against the configured authorized device source access list.

## Syntax

- **default match ra-srcaddr-list**
- **match ra-srcaddr-list WORD<1-64>**
- **no match ra-srcaddr-list**

## Command Parameters

WORD<1-64>

Specifies the MAC access list name.

## Default

None

## Command Mode

RA-guard Configuration

---

## router-preference

Enables verification of the advertised default router-preference parameter value is lower than or equal to a specified limit.

## Syntax

- **default router-preference maximum**
- **router-preference maximum {none | high | low | medium}**

## Command Parameters

**maximum {none | high | low | medium}**

Verifies if the advertised default router-preference parameter value is lower than or equal to a specified limit.

## Default

None

## Command Mode

RA-guard Configuration



# RIP Router Configuration

---

The following topics document commands available in RIP Router Configuration mode of the command line interface (CLI).

## default-metric (for RIP)

---

Configure RIP default import metric. This value is used by RIP announce of OSPF internal routes if the policy does not specify metric. 0 is used for deconfiguration.

### Syntax

- **default default-metric**
- **default-metric <0-15>**

### Command Parameters

<0-15>

Configures the value of default import metric to import a route into RIP domain.

### Default

The default value is 8.

### Command Mode

RIP Router Configuration

## ipv6 default-information enable

---

Enable IPv6 default information enable.

### Syntax

- **default ipv6 default-information enable**
- **ipv6 default-information enable**
- **no ipv6 default-information enable**

## Default

The default is disabled.

## Command Mode

RIP Router Configuration

# ipv6 default-information metric

---

Configure IPv6 default route metric value.

## Syntax

- **default ipv6 default-information metric**
- **ipv6 default-information metric <1-15>**

## Command Parameters

<1-15>

Specifies the IPv6 route metric value.

## Default

None

## Command Mode

RIP Router Configuration

# ipv6 redistribute bgp enable

---

Enable BGP redistribute.

## Syntax

- **default ipv6 redistribute bgp enable**
- **ipv6 redistribute bgp enable**
- **no ipv6 redistribute bgp enable**

## Default

The default is disabled.

## Command Mode

RIP Router Configuration

---

## ipv6 redistribute bgp enable (For RIPng)

---

Enable IPv6 BGP redistribute.

### Syntax

- **ipv6 redistribute bgp enable**

### Default

None

### Command Mode

RIP Router Configuration

---

## ipv6 redistribute direct enable

---

Enable direct redistribute.

### Syntax

- **default ipv6 redistribute direct enable**
- **ipv6 redistribute direct enable**
- **no ipv6 redistribute direct enable**

### Default

The default is disabled.

### Command Mode

RIP Router Configuration

---

## ipv6 redistribute isis enable

---

Enable ISIS redistribute.

### Syntax

- **default ipv6 redistribute isis enable**
- **ipv6 redistribute isis enable**
- **no ipv6 redistribute isis enable**

## Default

The default is disabled.

## Command Mode

RIP Router Configuration

---

## ipv6 redistribute ospf enable

Enable OSPF redistribute.

## Syntax

- **default ipv6 redistribute ospf enable**
- **ipv6 redistribute ospf enable**
- **no ipv6 redistribute ospf enable**

## Default

The default is disabled.

## Command Mode

RIP Router Configuration

---

## ipv6 redistribute static enable

Enable static redistribute.

## Syntax

- **default ipv6 redistribute static enable**
- **ipv6 redistribute static enable**
- **no ipv6 redistribute static enable**

## Default

The default is disabled.

## Command Mode

RIP Router Configuration

---

## ipv6 timers basic holddown

Configure RIPng holddown timer.

## Syntax

- **ipv6 timers basic holddown <0-360>**

## Command Parameters

<0-360>

Specifies the RIPng holddown timer in seconds.

## Default

None

## Command Mode

RIP Router Configuration

## ipv6 timers basic timeout

---

Configure RIPng timeout timer.

## Syntax

- **ipv6 timers basic timeout <0-360>**

## Command Parameters

<0-360>

Specifies the RIPng timeout timer in seconds.

## Default

None

## Command Mode

RIP Router Configuration

## ipv6 timers basic update

---

Configure RIPng update timer.

## Syntax

- **ipv6 timers basic update <0-360>**



## Command Parameters

<0-360>

Specifies the RIPv6 update timer in seconds.

## Default

None

## Command Mode

RIP Router Configuration

## network (for RIP)

---

Enable RIP on a network.

## Syntax

- **network {A.B.C.D}**
- **no network {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies the IP address of the network.

## Default

None

## Command Mode

RIP Router Configuration

## redistribute (for RIP)

---

Redistribute learned routes into RIP.

## Syntax

- **default redistribute { direct | isis | ospf | rip | static }**
- **default redistribute { direct | isis | ospf | rip | static } enable**
- **default redistribute { direct | isis | ospf | rip | static } enable vrf-src WORD<1-16>**
- **default redistribute { direct | isis | ospf | rip | static } metric**

- `default redistribute { direct | isis | ospf | rip | static } metric vrf-src WORD<1-16>`
- `default redistribute { direct | isis | ospf | rip | static } route-map`
- `default redistribute { direct | isis | ospf | rip | static } route-map vrf-src WORD<1-16>`
- `default redistribute { direct | isis | ospf | rip | static } vrf-src WORD<1-16>`
- `default redistribute WORD<0-32>`
- `default redistribute WORD<0-32> enable`
- `default redistribute WORD<0-32> enable vrf-src WORD<1-16>`
- `default redistribute WORD<0-32> metric`
- `default redistribute WORD<0-32> metric vrf-src WORD<1-16>`
- `default redistribute WORD<0-32> route-map`
- `default redistribute WORD<0-32> route-map vrf-src WORD<1-16>`
- `default redistribute WORD<0-32> vrf-src WORD<1-16>`
- `no redistribute { direct | isis | ospf | rip | static }`
- `no redistribute { direct | isis | ospf | rip | static } enable`
- `no redistribute { direct | isis | ospf | rip | static } enable vrf-src WORD<1-16>`
- `no redistribute { direct | isis | ospf | rip | static } route-map`
- `no redistribute { direct | isis | ospf | rip | static } route-map vrf-src WORD<1-16>`
- `no redistribute { direct | isis | ospf | rip | static } vrf-src WORD<1-16>`
- `no redistribute WORD<0-32>`
- `no redistribute WORD<0-32> enable`
- `no redistribute WORD<0-32> enable vrf-src WORD<1-16>`
- `no redistribute WORD<0-32> route-map`
- `no redistribute WORD<0-32> route-map vrf-src WORD<1-16>`
- `no redistribute WORD<0-32> vrf-src WORD<1-16>`
- `redistribute { direct | isis | ospf | rip | static }`
- `redistribute { direct | isis | ospf | rip | static } enable`
- `redistribute { direct | isis | ospf | rip | static } enable vrf-src WORD<1-16>`
- `redistribute { direct | isis | ospf | rip | static } metric <0-65535>`
- `redistribute { direct | isis | ospf | rip | static } metric <0-65535> vrf-src WORD<1-16>`
- `redistribute { direct | isis | ospf | rip | static } route-map WORD<0-64>`

- **redistribute { direct | isis | ospf | rip | static } route-map WORD<0-64> vrf-src WORD<1-16>**
- **redistribute { direct | isis | ospf | rip | static } vrf-src WORD<1-16>**
- **redistribute WORD<0-32>**
- **redistribute WORD<0-32> enable**
- **redistribute WORD<0-32> enable vrf-src WORD<1-16>**
- **redistribute WORD<0-32> metric <0-65535>**
- **redistribute WORD<0-32> metric <0-65535> vrf-src WORD<1-16>**
- **redistribute WORD<0-32> route-map WORD<0-64>**
- **redistribute WORD<0-32> route-map WORD<0-64> vrf-src WORD<1-16>**
- **redistribute WORD<0-32> vrf-src WORD<1-16>**

## Command Parameters

### enable

Enables route redistribution of Intermediate-System-to-Intermediate-System (ISIS) learned IP routes into RIP.

### metric <0-65535>

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### route-map WORD<0-64>

Configures the route policy to apply to redistributed routes.

### vrf-src WORD<1-16>

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

### WORD<0-32>

Specifies the protocol type. The possible values are bgp, direct, isis, ospf, rip, or static.

## Default

By default, route redistribution is disabled.

## Command Mode

RIP Router Configuration

## timers basic holddown (for RIP)

Configures the RIP hold-down timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable.

## Syntax

- **default timers basic holddown**
- **timers basic holddown <0-360>**

## Command Parameters

**<0-360>**

Configures the holddown timer value.

## Default

The default is 120 seconds.

## Command Mode

RIP Router Configuration

---

## timers basic timeout

Configure the RIP timeout interval.

## Syntax

- **default timers basic timeout**
- **timers basic timeout <15-259200>**
- **timers basic timeout <15-259200> [holddown <0-360>] [update <1-360>]**

## Command Parameters

**<15-259200>**

Configures the value of default import metric to import a route into RIP domain.

**holddown <0-360>**

Configures the RIP hold-down timer value, the length of time (in seconds) that RIP continues to advertise a network after it determines that the network is unreachable. The default is 120.

**update <1-360>**

Configures the RIP update timer. The update time is the time interval, in seconds, between RIP updates. The default is 30.

## Default

The default value is 180.

## Command Mode

RIP Router Configuration

## timers basic update

---

Configure the RIP update timer. The update time is the time interval between RIP updates.

### Syntax

- `default timers basic update`
- `timers basic update <1-360>`

### Command Parameters

<1-360>

Configures the update interval.

### Default

The default is 30 seconds.

### Command Mode

RIP Router Configuration



# Route-Map Configuration

---

The following topics document commands available in Route-Map Configuration mode of the command line interface (CLI).

## enable (for a route policy)

---

Enable the route policy.

### Syntax

- **default enable**
- **enable**
- **no enable**

### Default

The default is disable.

### Command Mode

Route-Map Configuration

## match as-path

---

If configured, the switch Match the as-path attribute of the Border Gateway Protocol (BGP) routes against the contents of the specified AS-lists. This command is used only for BGP routes and ignored for all other route types.

### Syntax

- **default match as-path WORD<0-256>**
- **match as-path WORD<0-256>**
- **no match as-path WORD<0-256>**

### Command Parameters

**WORD<0-256>**

Specifies the list IDs of AS-lists, separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

---

## match community

If configured, the switch Match the community attribute of the BGP routes against the contents of the specified community lists. This command is used only for BGP routes and ignored for all other route types.

## Syntax

- **default match community WORD<0-256>**
- **match community WORD<0-256>**
- **no match community WORD<0-256>**

## Command Parameters

WORD<0-256>

Specifies the list IDs of up to four defined community lists, separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

---

## match community-exact

When disabled, match community-exact results in a match when the community attribute of the BGP routes match any entry of any community-list specified in match community. When enabled, match community-exact results in a match when the community attribute of the BGP routes Match all of the entries of all the community lists specified in match community.

## Syntax

- **default match community-exact**
- **default match community-exact enable**
- **match community-exact**
- **match community-exact enable**

- `no match community-exact`
- `no match community-exact enable`

## Command Parameters

### enable

Enables match community-exact.

## Default

The default is disable.

## Command Mode

Route-Map Configuration

---

## match extcommunity

Match the extended community.

## Syntax

- `default match extcommunity WORD<0-1027>`
- `match extcommunity WORD<0-1027>`
- `no match extcommunity WORD<0-1027>`

## Command Parameters

### WORD<0-1027>

Specifies the list IDs of AS-lists, separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

---

## match interface

Match the IP address of the interface by which the RIP route was learned against the contents of the specified prefix list. This command is used only for RIP routes and ignored for all other route types.



## Syntax

- **default match interface WORD<0-259>**
- **match interface WORD<0-259>**
- **no match interface WORD<0-259>**

## Command Parameters

**WORD<0-259>**

Specifies the name of up to four defined prefix lists, separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

## match local-preference

---

Match the preference value from 0-2147483647.

## Syntax

- **default match local-preference**
- **match local-preference <0-2147483647>**

## Command Parameters

**<0-2147483647>**

Specifies the preference value.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

## match metric

---

Match the metric of the incoming advertisement or existing route against the specified value. If 0, this field is ignored.

## Syntax

- **default match metric**
- **match metric <0-65535>**

## Command Parameters

<0-65535>

Specifies the metric to match.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

---

## match metric-type-isis

Match ISIS metric type, applicable to ISIS only, ignored otherwise.

## Syntax

- **default match metric-type-isis**
- **match metric-type-isis {any | internal | external}**

## Command Parameters

{ any | internal | external }

Specifies IS-IS routes of the specified type. • internal – permits or denies routes that are internal to the IS-IS domain. • external – permits or denies routes that originate from an external routing protocol domain. • any – permits or denies both internal routes as well as external routes.

## Default

The default is any.

## Command Mode

Route-Map Configuration

---

## match network

Match the destination network against the contents of the specified prefix lists.

## Syntax

- **default match network WORD<0-259>**
- **match network WORD<0-259>**
- **no match network WORD<0-259>**

## Command Parameters

WORD<0-259>

Specifies the name of up to four defined prefix lists, separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

## match next-hop

---

Match the next-hop IP address of the route against the contents of the specified prefix list. This command applies only to nonlocal routes.

## Syntax

- **default match next-hop WORD<0-259>**
- **match next-hop WORD<0-259>**
- **no match next-hop WORD<0-259>**

## Command Parameters

WORD<0-259>

Specifies the name of up to four defined prefix lists, separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

## match protocol

---

Match the protocol through which the route is learned.

## Syntax

- **default match protocol**
- **match protocol WORD<0-60>**
- **no match protocol**
- **no match protocol WORD<0-60>**

## Command Parameters

**WORD<0-60>**

Specifies the protocol as any|xxx, where xxx is local, OSPF, External BGP (EBGP), Internal BGP (IBGP), RIP, static, or any combination, in a string length 0 to 60.

## Default

The default is any.

## Command Mode

Route-Map Configuration

---

## match route-source

Match the next-hop IP address for RIP routes and advertising router IDs for OSPF routes against the contents of the specified prefix list. This option is ignored for all other route types.

## Syntax

- **default match route-source WORD<0-259>**
- **match route-source WORD<0-259>**
- **no match route-source WORD<0-259>**

## Command Parameters

**WORD<0-259>**

Specifies the name of up to four defined prefix lists, separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

---

## match route-type

---

Configure a specific route type to match. This command applies only to OSPF routes.

### Syntax

- **default match route-type**
- **match route-type { any | local | internal | external | external-1 | external-2 }**

### Command Parameters

{ any | local | internal | external | external-1 | external-2 }

Specifies OSPF routes of the specified type only (External-1 or External-2). Any other value is ignored.

### Default

The default is any.

### Command Mode

Route-Map Configuration

---

## match tag

---

Specify a list of tags used during the match criteria process.

### Syntax

- **default match tag**
- **match tag WORD<0-256>**
- **no match tag**

### Command Parameters

WORD<0-256>

Specifies one or more tag values.

### Default

None

### Command Mode

Route-Map Configuration

---

## match vrf

---

Configure a specific VRF to match.

### Syntax

- **default match vrf WORD<1-16>**
- **match vrf WORD<1-16>**
- **no match vrf WORD<1-16>**

### Command Parameters

WORD<1-16>

Specifies the VRF name.

### Default

None

### Command Mode

Route-Map Configuration

---

## match vrfids

---

Configure a specific VRF to match.

### Syntax

- **default match vrfids WORD<0-511>**
- **match vrfids WORD<0-511>**
- **no match vrfids WORD<0-511>**

### Command Parameters

WORD<0-511>

Specifies the VRF ID.

### Default

None

### Command Mode

Route-Map Configuration

---

## name

---

Rename a policy and changes the name field for all sequence numbers under the given policy.

### Syntax

- **name WORD<1-64>**

### Command Parameters

**WORD<1-64>**

Specifies the new name for the policy.

### Default

None

### Command Mode

Route-Map Configuration

---

## permit

---

Specifies the action to take when a permit or deny policy is selected for a specific route. Permit allows the route, deny (no permit) ignores the route.

### Syntax

- **default permit**
- **no permit**
- **permit**

### Default

The default is permit.

### Command Mode

Route-Map Configuration

---

## set as-path

---

Add the AS number of the AS-list to the BGP routes that match this policy.

### Syntax

- **default set as-path WORD<0-256>**

- **no set as-path WORD<0-256>**
- **set as-path WORD<0-256>**

## Command Parameters

**WORD<0-256>**

Specifies the list ID of up to four defined AS-lists separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

---

## set as-path-mode

Configure the AS path mode.

## Syntax

- **default set as-path-mode**
- **set as-path-mode prepend**
- **set as-path-mode tag**

## Command Parameters

**prepend**

Prepends the Autonomous System (AS) number of the AS-list specified in set-as-path to the old as-path attribute of the BGP routes that match this policy.

**tag**

Configures the Autonomous System (AS) path mode to tag.

## Default

The default is prepend.

## Command Mode

Route-Map Configuration

---

## set automatic-tag

Configure the tag automatically. This command is used for BGP routes only.



## Syntax

- `default set automatic-tag`
- `default set automatic-tag enable`
- `no set automatic-tag`
- `no set automatic-tag enable`
- `set automatic-tag`
- `set automatic-tag enable`

## Command Parameters

`enable`

Enables this configuration.

## Default

The default is disable.

## Command Mode

Route-Map Configuration

## set community

---

Add the community number of the community list to the BGP routes that match this policy.

## Syntax

- `default set community WORD<0-256>`
- `no set community WORD<0-256>`
- `set community WORD<0-256>`

## Command Parameters

`WORD<0-256>`

Specifies the list ID of up to four defined community lists separated by a comma.

## Default

None

## Command Mode

Route-Map Configuration

---

## set community-mode

---

Configure the community mode.

### Syntax

- **default set community-mode**
- **set community-mode additive**
- **set community-mode none**
- **set community-mode unchanged**

### Command Parameters

#### additive

Prepends the community number of the community list specified in set-community to the old community path attribute of the BGP routes that match this policy.

#### none

Removes the community path attribute of the BGP routes that match this policy to the specified value.

#### unchanged

Configures the community mode to unchanged.

### Default

The default is unchanged.

### Command Mode

Route-Map Configuration

---

## set injectlist

---

Replace the destination network of the route that Match this policy with the contents of the specified prefix list.

### Syntax

- **default set injectlist**
- **no set injectlist**
- **set injectlist WORD<0-1027>**

### Command Parameters

#### WORD<0-1027>

Specifies one prefix list by name.

## Default

None

## Command Mode

Route-Map Configuration

---

## set ip-preference

Configure the preference to a value greater than 0. Specify the route preference value to assign to the routes that match this policy. This command applies to accept policies only.

## Syntax

- **default set ip-preference**
- **set ip-preference <0-255>**

## Command Parameters

<0-255>

Assigns the preference to the routes. If you configure the default, the global preference value is used.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

---

## set local-preference

Specify a value used during the route decision process in the BGP protocol. This command applies to BGP only.

## Syntax

- **default set local-preference**
- **set local-preference <0-65535>**

## Command Parameters

<0-65535>

Specifies the local preference value.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

---

## set mask

Configure the mask of the route that matches this policy. This command applies only to RIP accept policies.

## Syntax

- **default set mask**
- **no set mask**
- **set mask {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies a valid contiguous IP mask.

## Default

The default is 0.0.0.0.

## Command Mode

Route-Map Configuration

---

## set metric

Configure the metric value for the route while announcing a redistribution. If you configure the default, the original cost of the route is advertised into OSPF; for RIP, the original cost of the route or defaultimport- metric is used.

## Syntax

- **default set metric**
- **set metric <0-65535>**

## Command Parameters

<0-65535>

Specifies a metric value.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

---

## set metric-type

Configure the metric type for the routes to announce into the OSPF domain that Match this policy. This command applies only for OSPF announce policies.

## Syntax

- **default set metric-type**
- **set metric-type { type1 | type2 }**

## Command Parameters

{ type1 | type2 }

Specifies the metric type to announce.

## Default

The default is type 2.

## Command Mode

Route-Map Configuration

---

## set metric-type-internal

Configure the MED value for routes advertised to EBGp neighbors to the specified IGP metric value.

## Syntax

- **default set metric-type-internal**
- **set metric-type-internal <0-1>**

## Command Parameters

<0-1>

Specifies the Interior Gateway Protocol (IGP) metric value.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

## set metric-type-isis

---

Set ISIS metric type, applicable to ISIS only, ignored otherwise.

## Syntax

- **default set metric-type-isis**
- **set metric-type-isis {any | internal | external}**

## Command Parameters

{ any | internal | external }

Specifies IS-IS routes of the specified type. • internal – permits or denies routes that are internal to the IS-IS domain. • external – permits or denies routes that originate from an external routing protocol domain. • any – permits or denies both internal routes as well as external routes.

## Default

The default is any.

## Command Mode

Route-Map Configuration

## set next-hop

---

Specify the IPv4 or IPv6 address of the next-hop router.

## Syntax

- **default set next-hop**
- **no set next-hop**
- **set next-hop WORD<1-256>**

## Command Parameters

WORD<1-256>

Specifies the IP address of the next-hop router.

## Default

None

## Command Mode

Route-Map Configuration

---

## set nssa-pbit

Configure the not so stubby area (NSSA) translation P bit. This command applies to OSPF announce policies only.

## Syntax

- **default set nssa-pbit**
- **default set nssa-pbit enable**
- **no set nssa-pbit**
- **no set nssa-pbit enable**
- **set nssa-pbit**
- **set nssa-pbit enable**

## Command Parameters

**enable**

Enables P bit translation.

## Default

The default is enable.

## Command Mode

Route-Map Configuration

---

## set origin

Change the origin path attribute of the BGP routes that match this policy to the specified value.

## Syntax

- **default set origin**
- **set origin { igp | egp | incomplete }**

## Command Parameters

`{ igp | egp | incomplete }`

Specifies the origin path attribute.

## Default

The default is unchanged.

## Command Mode

Route-Map Configuration

---

## set origin-egp-as

Configure the origin EGP autonomous system (AS). This command applies to BGP only.

## Syntax

- **default set origin-egp-as**
- **set origin-egp-as <0-65535>**

## Command Parameters

`<0-65535>`

Indicates the remote Autonomous System (AS) number.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

---

## set tag

Configure the tag of the destination routing protocol. If not specified, the switch forwards the tag value in the source routing protocol.

## Syntax

- **default set tag**
- **set tag <0-65535>**



## Command Parameters

<0-65535>

Specifies the tag value. A value of 0 indicates that this parameter is not set.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

---

## set weight

Configure the weight for the routing table. This command applies to BGP only. This value overrides the weight configured through `NetworkTableEntry`, `FilterListWeight`, or `NeighborWeight`.

## Syntax

- **default set weight**
- **set weight <0-65535>**

## Command Parameters

<0-65535>

Specifies the weight value. A value of 0 indicates that this parameter is not set.

## Default

The default is 0.

## Command Mode

Route-Map Configuration

---

## set-metric-type-live-metric

Configure metric type for BGP routes. This command applies to BGP policies only, ignored otherwise.

## Syntax

- **default set-metric-type-live-metric**
- **set-metric-type-live-metric**

## Default

The default is disable.

## Command Mode

Route-Map Configuration



# User EXEC

---

The following topics document commands available in User EXEC mode of the command line interface (CLI).

## clear-stats

---

Clear port statistic counters.

### Syntax

- **clear-stats**
- **clear-stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **clear-stats port mgmt**

### Command Parameters

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**port mgmt**

Clear the management port stats.

### Default

None

### Command Mode

User EXEC

## clock set

---

Configure the calendar time in the form of month, day, year, hour, minute, and second.

### Syntax

- **clock set <MMddyyyyhhmmss>**

## Command Parameters

<MMddyyhhmmss>

Specifies the month, day, year, hours, minutes, and seconds.

## Default

None

## Command Mode

User EXEC

## cpld-install app

---

Update the latest version of CPLD (Complex Programmable Logic Device) image for the app module.

## Syntax

```
cpld-install app [WORD<1-99>]
```

## Command Parameters

Word<1-99>

Specifies the image filename.



### Note

This parameter is optional. If you do not specify the filename, the command checks the image file from the running VOSS file system.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## cpld-install boot

---

Update the latest version of CPLD (Complex Programmable Logic Device) image for the boot module.

## Syntax

```
cpld-install boot [WORD<1-99>]
```

## Command Parameters

### Word<1-99>

Specifies the image filename.



#### Note

This parameter is optional. If you do not specify the filename, the command checks the image file from the running VOSS file system.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## cpld-install cpu

---

Update the latest version of CPLD (Complex Programmable Logic Device) image for the CPU module.

## Syntax

```
cpld-install cpu [WORD<1-99>]
```

## Command Parameters

### Word<1-99>

Specifies the image filename.



#### Note

This parameter is optional. If you do not specify the filename, the command checks the image file from the running VOSS file system.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## cpld-install fpga

---

Update the latest version of CPLD image for the Field-Programmable Gate Array (FPGA) module.

## Syntax

```
cpld-install fpga [WORD<1-99>]
```

## Command Parameters

### Word<1-99>

Specifies the image filename.



### Note

This parameter is optional. If you do not specify the filename, the command checks the image file from the running VOSS file system.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## cpld-install main

---

Update the latest version of CPLD (Complex Programmable Logic Device) image for the main module.

## Syntax

```
cpld-install main [WORD<1-99>]
```

## Command Parameters

**Word<1-99>**

Specifies the image filename.



### Note

This parameter is optional. If you do not specify the filename, the command checks the image file from the running VOSS file system.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## cpld-install port

---

Update the latest version of CPLD image for the port module.

## Syntax

```
cpld-install port [WORD<1-99>]
```

## Command Parameters

**Word<1-99>**

Specifies the image filename.



### Note

This parameter is optional. If you do not specify the filename, the command checks the image file from the running VOSS file system.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## cpld-install vim

---

Update the latest version of CPLD image for the Versatile Interface Module (VIM) module.

## Syntax

```
cpld-install vim [WORD<1-99>]
```

## Command Parameters

### Word<1-99>

Specifies the image filename.



### Note

This parameter is optional. If you do not specify the filename, the command checks the image file from the running VOSS file system.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## debug-file remove

---

Clears all types of debug files. To remove a specific file, use the remove command instead. Debug files include core, archive, dmalloc, wd\_stats, PMEM and flrec files.

## Syntax

- **debug-file remove**
- **debug-file remove {slot[-slot][, ...]}**
- **debug-file remove {slot[-slot][, ...]} all**
- **debug-file remove all**



## Command Parameters

**{slot[-slot][,...]}**

Removes the debug files for one or more specific slots. You can specify a specific slot number , a range of slots, or use the value of all to view information for all slots. This parameter does not apply to all hardware platforms.

**all**

Removes all types of debug files. If you do not use this parameter, you remove all but the most recent file.

## Default

None

## Command Mode

User EXEC

## debug-ipsec level <-1-5>

---

Configure how much debugging information to log for IPsec.

## Syntax

- **debug-ipsec level <-1-5>**

## Command Parameters

**<-1-5>**

Defines the debugging level. Use the following values:

- -1 for silent; nothing is logged
- 0 for basic auditing logs
- 1 for control flow logs
- 2 for more detailed control flow logs
- 3 for raw data
- 4 to include sensitive information
- 5 to clear the logs

## Default

The default is 1.

## Command Mode

User EXEC

## Usage Guidelines

This command only applies to XA1400 Series.

Use the **show io ipsec logs** command to view the logged information.

## dump ar

---

To aid in troubleshooting, a dump of the hardware records can be captured.

## Syntax

- **dump ar <1> WORD <1-1536> <0-3>**

## Command Parameters

**<0-3>**

Specifies the verbosity from 0 to 3. Higher numbers specify more verbosity.

**WORD<1-1536>**

Specifies a record type in the AR table. Options include vlan, ip\_subnet, mac\_vlan, mac, arp, ip, ipmc, ip\_filter, protocol, all.

## Default

None

## Command Mode

User EXEC

## dvr apply redistribute

---

Applies the configuration of Distributed Virtual Routing (DvR) route redistribution.

## Syntax

- **dvr apply redistribute**
- **dvr apply redistribute vrf WORD<1-16>**

## Command Parameters

**vrf WORD<1-16>**

Applies DvR route redistribution configuration for the specified VRF.

## Default

None

## Command Mode

User EXEC

## dvr apply redistribute direct

---

Applies the configuration of Distributed Virtual Routing (DvR) route redistribution for direct routes.

### Syntax

- **dvr apply redistribute direct**
- **dvr apply redistribute direct vrf WORD<1-16>**

### Command Parameters

**none**

Applies DvR route redistribution configuration of direct routes on the GRT.

**vrf WORD<1-16>**

Applies DvR route redistribution configuration of direct routes for the specified VRF.

### Default

none

## Command Mode

User EXEC

## dvr apply redistribute static

---

Applies the configuration of Distributed Virtual Routing (DvR) route redistribution for static routes.

### Syntax

- **dvr apply redistribute static**
- **dvr apply redistribute static vrf WORD<1-16>**

### Command Parameters

**none**

Applies DvR route redistribution configuration of static routes on the GRT.

**vrf WORD<1-16>**

Applies DvR route redistribution configuration of static routes for the specified VRF.

## Default

none

## Command Mode

User EXEC

## eapol init

---

Initialize Extensible Authentication Protocol (EAPoL) administration traffic control direction.

## Syntax

- **eapol init**
- **eapol init {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**re-authenticate {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Starts re-authentication immediately. {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## eapol re-authenticate

---

Starts re-authentication immediately.

## Syntax

- **eapol re-authenticate {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**port** {slot/port[/sub-port][[-slot/port[/sub-port]][,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## enable

---

Use this command to enter Privileged EXEC mode.

## Syntax

- **enable**

## Default

None

## Command Mode

User EXEC

## exit

---

Use this command to exit a command mode and enter the lower command mode. If you use this command in User EXEC mode, you end the current CLI session.

## Syntax

- **exit**

## Default

None

## Command Mode

User EXEC

## file-checksum

---

Calculates or compares a Message Digest 5 algorithm (MD5) or SHA512 digest for a specified file.

### Syntax

- `file-checksum md5 WORD<1-99>`
- `file-checksum md5 WORD<1-99> -a`
- `file-checksum md5 WORD<1-99> -a -f`
- `file-checksum md5 WORD<1-99> -c`
- `file-checksum md5 WORD<1-99> -c -a`
- `file-checksum md5 WORD<1-99> -c -f`
- `file-checksum md5 WORD<1-99> -f WORD<1-99>`
- `file-checksum md5 WORD<1-99> -r`
- `file-checksum md5 WORD<1-99> -r -a`
- `file-checksum md5 WORD<1-99> -r -c`
- `file-checksum md5 WORD<1-99> -r -f`
- `file-checksum sha512 WORD<1-99>`
- `file-checksum sha512 WORD<1-99> -a`
- `file-checksum sha512 WORD<1-99> -a -f`
- `file-checksum sha512 WORD<1-99> -c`
- `file-checksum sha512 WORD<1-99> -c -a`
- `file-checksum sha512 WORD<1-99> -c -f`
- `file-checksum sha512 WORD<1-99> -f WORD<1-99>`
- `file-checksum sha512 WORD<1-99> -r`
- `file-checksum sha512 WORD<1-99> -r -a`
- `file-checksum sha512 WORD<1-99> -r -c`
- `file-checksum sha512 WORD<1-99> -r -f`

### Command Parameters

**-a**

Adds data to the output file instead of overwriting it.

**-c**

Compares the checksum of the specified file with the checksum present in the checksum file name.

**-f**

Stores the result of the checksum to a file. If the output file specified is one of the reserved filenames on the switch, the command fails with the error message: Error: Invalid operation.

**md5**

Calculate or compare the Message Digest 5 algorithm (MD5) digest to verify the MD5 checksum for a specified file. The md5 command displays the output on screen or stores the output in a file that you specify.

**-r**

Reverses the output.

**sha512**

Calculate or compare the SHA512 digest for a file.

**WORD<1-99>**

Specifies the filename.

## Default

None

## Command Mode

User EXEC

## help

---

Use this command to see parameters for a particular command. You can use this command in any mode. You can also request Help at any point by entering a question mark after a command, which shows the available options.

## Syntax

- **help**
- **help WORD<1-255>**

## Command Parameters

**WORD<1-255>**

Enters a command to see the options for that command.

## Default

None

## Command Mode

User EXEC

## ip bgp apply redistribute

---

Configure a redistribute entry to announce routes of a certain source protocol type into the Border Gateway Protocol (BGP) domain, for example, static, Routing Information Protocol (RIP), or direct routes.

### Syntax

- `ip bgp apply redistribute`
- `ip bgp apply redistribute direct`
- `ip bgp apply redistribute direct vrf WORD<1-16>`
- `ip bgp apply redistribute direct vrf-src WORD<1-16>`
- `ip bgp apply redistribute isis`
- `ip bgp apply redistribute isis vrf WORD<1-16>`
- `ip bgp apply redistribute isis vrf-src WORD<1-16>`
- `ip bgp apply redistribute ospf`
- `ip bgp apply redistribute ospf vrf WORD<1-16>`
- `ip bgp apply redistribute ospf vrf-src WORD<1-16>`
- `ip bgp apply redistribute rip`
- `ip bgp apply redistribute rip vrf WORD<1-16>`
- `ip bgp apply redistribute rip vrf-src WORD<1-16>`
- `ip bgp apply redistribute static`
- `ip bgp apply redistribute static vrf WORD<1-16>`
- `ip bgp apply redistribute static vrf-src WORD<1-16>`
- `ip bgp apply redistribute vrf WORD<1-16>`

### Command Parameters

`{direct|dvr|isis|ospf|rip|static|vrf}`

Specifies the protocol type.

`vrf WORD<1-16>`

Specifies a VRF instance by name.

`vrf-src WORD<1-16>`

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

### Default

None



## Command Mode

User EXEC

## ip bgp restart-bgp

---

Restart BGP for a particular peer.

### Syntax

- **ip bgp restart-bgp**
- **ip bgp restart-bgp neighbor WORD<0-1536>**
- **ip bgp restart-bgp neighbor WORD<0-1536> soft-reconfiguration {in|out}**
- **ip bgp restart-bgp neighbor WORD<0-1536> vrf WORD<1-16>**
- **ip bgp restart-bgp vrf WORD<1-16>**
- **ip bgp restart-bgp vrf WORD<1-16> soft-reconfiguration {in|out}**

### Command Parameters

#### **soft-reconfiguration {in|out}**

Enables or disables soft-reconfiguration. If peer soft-reconfiguration is enabled in the in-bound direction, the policy can be changed and routes can be re-learned without having to reset the BGP connection. Enabling soft-reconfiguration, using the in parameter, causes the system to store all BGP routes in local memory. Even non-best routes will be stored if soft-reconfiguration in is enabled. Setting the value to out forces the neighbor to send out all the updates to the remote neighbor without resetting the connection.

#### **vrf WORD<1-16>**

Applies the BGP configuration for a particular VRF.

#### **WORD<1-1536>**

Specifies the neighbor IP address or the neighbor group name.

### Default

The default for soft-reconfiguration is: in

## Command Mode

User EXEC

## ip bgp stats-clear-counters

---

Clears the BGP configuration statistics.

### Syntax

- **ip bgp stats-clear-counters**

- **ip bgp stats-clear-counters neighbor <nbr\_ipaddr|peer-group-name>**
- **ip bgp stats-clear-counters vrf WORD<1-16>**

## Command Parameters

**neighbor <nbr\_ipaddress|peer-groupname>**

Clears the BGP configuration statistics for the peer IP address or the peer group name.

**vrf WORD<1-16>**

Clears the statistics for the BGP configuration for a particular VRF.

## Default

None

## Command Mode

User EXEC

## ip ecmp path-list apply

---

Apply changes to all Equal Cost Multipath (ECMP) path-list configurations.

## Syntax

- **ip ecmp path-list apply**
- **ip ecmp path-list apply vrf WORD<1-16>**
- **ip ecmp pathlist-apply**
- **ip ecmp pathlist-apply vrf WORD<1-16>**

## Command Parameters

**path-list apply**

Apply changes to all Equal Cost Multipath (ECMP) path-list configurations.

**vrf WORD<1-16>**

Apply changes to all Equal Cost Multipath (ECMP) path-list configurations for a particular VRF.

## Default

None

## Command Mode

User EXEC

---

## ip igmp flush port

---

Use this command to flush Internet Group Management Protocol (IGMP) group members on a port.

### Syntax

- **ip igmp flush port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} grp-member**

### Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**grp-member**

Specifies a group member.

### Default

None

### Command Mode

User EXEC

---

## ip igmp flush vlan

---

Use this command to flush Internet Group Management Protocol (IGMP) group members, the multicast router and senders.

### Syntax

- **ip igmp flush vlan <1-4059>**
- **ip igmp flush vlan <1-4059> grp-member**
- **ip igmp flush vlan <1-4059> mrouter**
- **ip igmp flush vlan <1-4059> sender**
- **ip igmp flush vlan <1-4059> sender {A.B.C.D}**
- **ip igmp flush vlan <1-4059> sender {A.B.C.D} {A.B.C.D}**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**grp-member**

Specifies a group member.

**mrouter**

Specifies a multicast router.

**sender {A.B.C.D} {A.B.C.D}**

Specifies a sender. The first IP address specifies the source IP address of the sender. The second IP address specifies the group IP address of the sender.

## Default

None

## Command Mode

User EXEC

## ip ospf apply accept

---

Apply OSPF accept policy changes to allow the configuration changes in the policy to take effect in an OSPF Accept context (and to prevent the switch from attempting to apply the changes one by one after each configuration change).

## Syntax

- **ip ospf apply accept**
- **ip ospf apply accept vrf WORD<1-16>**

## Command Parameters

[vrf WORD<1-16>]

Specifies the name of the VRF.

**apply**

Commits entered changes. Issue this command after modifying any policy configuration that affects an OSPF accept policy.

## Default

The default is disabled.

## Command Mode

User EXEC

## ip ospf apply accept adv-rtr

---

Apply the OSPF accept policy change to accept external routes from a specified advertising route.

### Syntax

- **ip ospf apply accept adv-rtr {A.B.C.D}**
- **ip ospf apply accept adv-rtr {A.B.C.D} vrf WORD<1-16>**

### Command Parameters

{A.B.C.D}

Specifies the advertising router IP address.

vrf WORD<1-16>

Specifies the configuration for a particular VRF. WORD<1-16> specifies the VRF name.

### Default

None

## Command Mode

User EXEC

## ip ospf apply redistribute

---

Apply the OSPF redistribution.

### Syntax

- **ip ospf apply redistribute**
- **ip ospf apply redistribute {bgp | direct | isis | ospf | rip | static | dvr}**
- **ip ospf apply redistribute {bgp | direct | isis | ospf | rip | static | dvr} vrf WORD<1-16>**
- **ip ospf apply redistribute {bgp | direct | isis | ospf | rip | static | dvr} vrf WORD<1-16> vrf-src WORD<1-16>**
- **ip ospf apply redistribute {bgp | direct | isis | ospf | rip | static | dvr} vrf-src WORD<1-16>**
- **ip ospf apply redistribute vrf WORD<1-16>**
- **ip ospf apply redistribute WORD<1-32>**

- **ip ospf apply redistribute WORD<1-32> vrf WORD<1-16>**
- **ip ospf apply redistribute WORD<1-32> vrf-src WORD<1-16>**

## Command Parameters

**{bgp | direct | isis | ospf | rip | static | dvr }**

Specifies the type of routes to be redistributed (the protocol source), including BGP, RIP, OSPF, ISIS, DVR, static, and direct.

**vrf WORD<1-16>**

Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.

**vrf-src WORD<1-16>**

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

None

## Command Mode

User EXEC

## ip ospf spf-run

---

Force the switch to update its shortest-path calculations so that the switch uses the latest OSPF routing information.

## Syntax

- **ip ospf spf-run**
- **ip ospf spf-run vrf WORD<1-16>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF instance by name.

## Default

None

## Command Mode

User EXEC

## ip rip apply redistribute

Apply RIP redistribution.

### Syntax

- `ip rip apply redistribute`
- `ip rip apply redistribute`
- `ip rip apply redistribute { direct | isis | ospf | rip | static }`
- `ip rip apply redistribute { direct | isis | ospf | rip | static } vrf WORD<1-16>`
- `ip rip apply redistribute { direct | isis | ospf | rip | static } vrf WORD<1-16> vrf-src WORD<1-16>`
- `ip rip apply redistribute { direct | isis | ospf | rip | static } vrf-src WORD<1-16>`
- `ip rip apply redistribute bgp`
- `ip rip apply redistribute bgp vrf WORD<1-16>`
- `ip rip apply redistribute bgp vrf-src WORD<1-16>`
- `ip rip apply redistribute direct`
- `ip rip apply redistribute direct vrf WORD<1-16>`
- `ip rip apply redistribute direct vrf-src WORD<1-16>`
- `ip rip apply redistribute dvr`
- `ip rip apply redistribute dvr vrf WORD<1-16>`
- `ip rip apply redistribute dvr vrf-src WORD<1-16>`
- `ip rip apply redistribute isis`
- `ip rip apply redistribute isis vrf WORD<1-16>`
- `ip rip apply redistribute isis vrf-src WORD<1-16>`
- `ip rip apply redistribute ospf`
- `ip rip apply redistribute ospf vrf WORD<1-16>`
- `ip rip apply redistribute ospf vrf-src WORD<1-16>`
- `ip rip apply redistribute rip`
- `ip rip apply redistribute rip vrf WORD<1-16>`
- `ip rip apply redistribute rip vrf-src WORD<1-16>`
- `ip rip apply redistribute static`
- `ip rip apply redistribute static vrf WORD<1-16>`
- `ip rip apply redistribute static vrf-src WORD<1-16>`
- `ip rip apply redistribute vrf WORD<1-16>`

- **ip rip apply redistribute vrf WORD<1-16>**
- **ip rip apply redistribute vrf WORD<1-16>**

## Command Parameters

**{ direct | isis | ospf | rip | static }**

Specifies the type of routes to be redistributed (the protocol source), including OSPF, static, direct, RIP.

**{bgp | direct | dvr | isis | ospf | rip | static | vrf}**

Specifies the protocol type.

**vrf WORD<1-16>**

Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrf-src WORD<0-16>**

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

**vrf-src WORD<1-16>**

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

None

## Command Mode

User EXEC

## ipv6 bgp apply redistribute

---

Apply bgp redistribute commands

## Syntax

- **ipv6 bgp apply redistribute**
- **ipv6 bgp apply redistribute direct [vrf WORD<1-16>]**
- **ipv6 bgp apply redistribute isis [vrf WORD<1-16>]**
- **ipv6 bgp apply redistribute ospf [vrf WORD<1-16>]**
- **ipv6 bgp apply redistribute rip**



- **ipv6 bgp apply redistribute static [vrf WORD<1-16>]**
- **ipv6 bgp apply redistribute vrf WORD<1-16>**

## Command Parameters

### direct

Enter the protocol type direct.

### isis

Enter the protocol type isis.

### ospf

Enter the protocol type ospf.

### rip

Enter the protocol type ripng.

### static

Enter the protocol type static.

### vrf WORD<1-16>

Apply BGP configuration for a particular VRF.

## Default

None

## Command Mode

User EXEC

## ipv6 isis apply accept

---

Applies the configured IPv6 Intermediate-System-to-Intermediate-System (IS-IS) accept policies.

## Syntax

- **ipv6 isis apply accept**
- **ipv6 isis apply accept vrf WORD<1-16>**

## Command Parameters

### vrf WORD<1-16>

Applies the configured IPv6 IS-IS accept policies for the specified VRF.

## Default

None

## Command Mode

User EXEC

## ipv6 isis apply redistribute

---

Apply the IPv6 Intermediate-System-to-Intermediate-System (IS-IS) redistribution.

### Syntax

- **ipv6 isis apply redistribute**
- **ipv6 isis apply redistribute {bgp | direct | isis | ospf | rip | static}**
- **ipv6 isis apply redistribute {bgp | direct | isis | ospf | static } vrf WORD<1-16>**
- **ipv6 isis apply redistribute vrf WORD<1-16>**

### Command Parameters

{ bgp | direct | isis | rip | static | vrf }

Specifies a protocol type.

vrf WORD<1-16>

Specifies the VRF name.

### Default

None

## Command Mode

User EXEC

## ipv6 mld flush

---

Flushes MLD group members and senders.

### Syntax

- **ipv6 mld flush port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} grp-member**
- **ipv6 mld flush vlan <1-4059> grp-member**
- **ipv6 mld flush vlan <1-4059> sender**

### Command Parameters

grp-member

Flushes MLD group members.

**port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

Flushes MLD group members by brouter port.

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### **sender**

Flushes MLD senders.

**vlan** <1-4059>

Flushes MLD group members or senders by VLAN.

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## ipv6 ospf apply redistribute

Apply the OSPF redistribution.

## Syntax

- **ipv6 ospf apply redistribute**
- **ipv6 ospf apply redistribute {bgp | direct | isis | ospf | rip | static }**
- **ipv6 ospf apply redistribute {bgp | direct | isis | ospf | rip | static } vrf WORD<1-16>**
- **ipv6 ospf apply redistribute vrf WORD<1-16>**

## Command Parameters

{ bgp| direct | isis | rip | static | vrf }

Specifies a protocol type.

vrf WORD<1-16>

Specifies the VRF name.

## Default

None

## Command Mode

User EXEC

## isis apply accept

---

Apply IS-IS accept policy changes. This command can disrupt traffic and cause temporary traffic loss. After you apply accept policy changes, the command reapplies the accept policies, which deletes all of the IS-IS routes, and adds the IS-IS routes again. You should make all the relevant accept policy changes, and then apply the changes at the end.

## Syntax

- **isis apply accept**
- **isis apply accept vrf WORD<1-16>**

## Command Parameters

vrf WORD<1-16>

Specifies a VRF instance.

## Default

None

## Command Mode

User EXEC

## isis apply redistribute

---

Apply the redistribution of the specified protocol into the Shortest Path Bridging MAC (SPBM) network.

## Syntax

- **isis apply redistribute**
- **isis apply redistribute bgp**
- **isis apply redistribute bgp vrf WORD<1-16>**
- **isis apply redistribute direct**
- **isis apply redistribute direct vrf WORD<1-16>**

- **isis apply redistribute ospf**
- **isis apply redistribute ospf vrf WORD<1-16>**
- **isis apply redistribute rip**
- **isis apply redistribute rip vrf WORD<1-16>**
- **isis apply redistribute static**
- **isis apply redistribute static vrf WORD<1-16>**
- **isis apply redistribute vrf WORD<1-16>**

## Command Parameters

{bgp | direct | isis | ospf | rip | static | vrf}

Specifies the protocol type.

WORD<1-16>

Specifies the VRF name.

## Default

None

## Command Mode

User EXEC

## isis dup-detection-temp-disable

---

Temporarily disables isis duplicate detection

## Syntax

- **isis dup-detection-temp-disable**

## Default

None

## Command Mode

User EXEC

## isis multi-area ip apply redistribute routed-multicast

---

Configures the Intermediate-System-to-Intermediate-System (IS-IS) Multi-area SPB IPv4 multicast routing redistribution for home to remote direction, remote to home direction, or a specific Virtual Router Forwarding (VRF) instance.

## Syntax

- `isis multi-area ip apply redistribute routed-multicast`
- `isis multi-area ip apply redistribute routed-multicast [home-to-remote]`
- `isis multi-area ip apply redistribute routed-multicast [home-to-remote] [vrf WORD<1-16>]`
- `isis multi-area ip apply redistribute routed-multicast [remote-to-home]`
- `isis multi-area ip apply redistribute routed-multicast [remote-to-home] [vrf WORD<1-16>]`
- `isis multi-area ip apply redistribute routed-multicast [vrf WORD<1-16>]`

## Command Parameters

### home-to-remote

Applies the multicast routing redistribution configuration for home to remote direction.

### remote-to-home

Applies the multicast routing redistribution configuration for remote to home direction.

### vrf WORD<1-16>

Applies the multicast routing redistribution configuration for specific Virtual Forwarding Router (VRF) instance.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis multi-area ip apply redistribute unicast

---

Configures the Intermediate-System-to-Intermediate-System (IS-IS) Multi-area SPB IPv4 unicast redistribution for home to remote direction, remote to home direction, or a specific Virtual Router Forwarding (VRF) instance.

## Syntax

- `isis multi-area ip apply redistribute unicast`
- `isis multi-area ip apply redistribute unicast [home-to-remote]`
- `isis multi-area ip apply redistribute unicast [home-to-remote] [vrf WORD<1-16>]`
- `isis multi-area ip apply redistribute unicast [remote-to-home]`
- `isis multi-area ip apply redistribute unicast [remote-to-home] [vrf WORD<1-16>]`
- `isis multi-area ip apply redistribute unicast [vrf WORD<1-16>]`

## Command Parameters

### home-to-remote

Applies the unicast redistribution configuration for home to remote direction.

### remote-to-home

Applies the unicast redistribution configuration for remote to home direction.

### vrf WORD<1-16>

Applies the unicast redistribution configuration for specific VRF instance.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis multi-area ipv6 apply redistribute unicast

---

Configures the Intermediate-System-to-Intermediate-System (IS-IS) Multi-area SPB IPv6 unicast redistribution for home to remote direction, remote to home direction, or a specific Virtual Router Forwarding (VRF) instance.

## Syntax

- `isis multi-area ipv6 apply redistribute unicast`
- `isis multi-area ipv6 apply redistribute unicast [home-to-remote]`
- `isis multi-area ipv6 apply redistribute unicast [home-to-remote] [vrf WORD<1-16>]`

- **isis multi-area ipv6 apply redistribute unicast [remote-to-home]**
- **isis multi-area ipv6 apply redistribute unicast [remote-to-home] [vrf WORD<1-16>]**
- **isis multi-area ipv6 apply redistribute unicast [vrf WORD<1-16>]**

## Command Parameters

### home-to-remote

Applies the unicast redistribution configuration for home to remote direction.

### remote-to-home

Applies the unicast redistribution configuration for remote to home direction.

### vrf WORD<1-16>

Applies the unicast redistribution configuration for specific VRF instance.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis multi-area l2 apply redistribute i-sid

---

Configures the IS-IS Multi-area SPB layer 2 I-SID redistribution globally.

## Syntax

- **isis multi-area l2 apply redistribute i-sid**

## Default

The default is none.

## Command Mode

User EXEC



## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis multi-area l2 apply redistribute snoop-multicast

---

Configures the IS-IS Multi-area SPB layer 2 multicast snooping redistribution globally.

### Syntax

- **isis multi-area l2 apply redistribute snoop-multicast**
- **isis multi-area l2 apply redistribute snoop-multicast [home-to-remote]**
- **isis multi-area l2 apply redistribute snoop-multicast [remote-to-home]**

### Command Parameters

#### home-to-remote

Applies the layer 2 multicast snooping redistribution configuration for home to remote direction.

#### remote-to-home

Applies the layer 2 multicast snooping redistribution configuration for remote to home direction.

### Default

The default is none.

### Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## l2 ping ip-address

---

Trigger a Layer 2 ping, which acts like a native ping. Enable Connectivity Fault Management (CFM) to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

### Syntax

- **l2 ping ip-address WORD<0-255>**
- **l2 ping ip-address WORD<0-255> burst-count <1-200>**
- **l2 ping ip-address WORD<0-255> burst-count <1-200> priority <0-7>**

- **l2 ping ip-address WORD<0-255> burst-count <1-200> source-mode nodal**
- **l2 ping ip-address WORD<0-255> burst-count <1-200> source-mode smltVirtual**
- **l2 ping ip-address WORD<0-255> burst-count <1-200> testfill-pattern all-zero**
- **l2 ping ip-address WORD<0-255> burst-count <1-200> testfill-pattern all-zero-crc**
- **l2 ping ip-address WORD<0-255> burst-count <1-200> testfill-pattern pseudo-random-bit-sequence**
- **l2 ping ip-address WORD<0-255> burst-count <1-200> testfill-pattern pseudo-random-bit-sequence-crc**
- **l2 ping ip-address WORD<0-255> data-tlv-size <0-400>**
- **l2 ping ip-address WORD<0-255> frame-size <64-1500>**
- **l2 ping ip-address WORD<0-255> time-out <1-10>**
- **l2 ping ip-address WORD<0-255> vrf WORD<1-16>**

## Command Parameters

### **burst-count <1-200>**

Specifies the burst count.

### **data-tlv-size <0-400>**

Specifies the data Type-Length-Value (TLV) size. The default is 0.

### **frame-size <64-1500>**

Specifies the frame size. The default is 0.

### **priority <0-7>**

Specifies the priority. The default is 7.

### **source-mode nodal**

Specifies the source mode of nodal or smltVirtual. Nodal MPs provide both MEP and MIP functionality for SPBM deployments. Nodal MPs are associated with a B-VLAN and are VLAN encapsulated packets. The default is nodal.

### **source-mode smltVirtual**

Specifies the source mode of nodal or smltVirtual. The switch supports SMLT interaction with SPBM. The platform uses two B-VIDs into the core from each pair of SMLT terminating nodes. Both nodes advertise the Nodal B-MAC into the core on both B-VIDS. In addition each node advertises the SMLT virtual B-MAC on one of the two B-VLANs. The default is nodal.

### **testfill-pattern all-zero**

Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.

### **testfill-pattern all-zero-crc**

Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.

#### **testfill-pattern pseudo-random-bit-sequence**

Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.

#### **testfill-pattern pseudo-random-bit-sequence-crc**

Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.

#### **time-out <1-10>**

Specifies the interval in seconds. The default is 3.

#### **vrf WORD<1-16>**

Specifies the VRF name.

#### **WORD<0-255>**

Specifies the IP address.

## Default

None

## Command Mode

User EXEC

## I2 ping vlan

---

Trigger a Layer 2 ping, which acts like a native ping. Enable Connectivity Fault Management (CFM) to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

## Syntax

- **12 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> burst-count <1-200>**
- **12 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> data-tlv-size <0-400>**

- `l2 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> frame-size <64-1500>`
- `l2 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> priority <0-7>`
- `l2 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern all-zero`
- `l2 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern all-zero-crc`
- `l2 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern pseudo-random-bit-sequence`
- `l2 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern pseudo-random-bit-sequence-crc`
- `l2 ping vlan <1-4059> mac <0x00:0x00:0x00:0x00:0x00:0x00> time-out <1-10>`
- `l2 ping vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00`
- `l2 ping vlan <1-4059> routernodename WORD<0-255>`
- `l2 ping vlan <1-4059> routernodename WORD<0-255>`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> burst-count <1-200>`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> data-tlv-size <0-400>`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> frame-size <64-1500>`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> priority <0-7>`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> testfill-pattern all-zero`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> testfill-pattern all-zero-crc`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> testfill-pattern pseudo-random-bit-sequence`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> testfill-pattern pseudo-random-bit-sequence-crc`
- `l2 ping vlan <1-4059> routernodename WORD<0-255> time-out <1-10>`

## Command Parameters

`<1-4059>`

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

`burst-count <1-200>`

Specifies the burst count.

`data-tlv-size <0-400>`

Specifies the data Type-Length-Value (TLV) size. The default is 0.

**frame-size <64-1500>**

Specifies the frame size. The default is 0.

**mac <0x00:0x00:0x00:0x00:0x00:0x00>**

Specifies the MAC address.

**priority <0-7>**

Specifies the priority. The default is 7.

**routernodename WORD<0-255>**

Specifies the router node name.

**testfill-pattern all-zero**

Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.

**testfill-pattern all-zero-crc**

Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.

**testfill-pattern pseudo-random-bit-sequence**

Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.

**testfill-pattern pseudo-random-bit-sequence-crc**

Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.

**time-out <1-10>**

Specifies the interval in seconds. The default is 3.

## Default

None

## Command Mode

User EXEC

## l2 tracemroute

---

Trigger a Layer 2 multicast traceroute. Enable Connectivity Fault Management (CFM) to debug Layer 2.

### Syntax

- **l2 tracemroute source {A.B.C.D} group {A.B.C.D}**
- **l2 tracemroute source {A.B.C.D} group {A.B.C.D} priority <0-7>**
- **l2 tracemroute source {A.B.C.D} group {A.B.C.D} ttl-value <1-255>**
- **l2 tracemroute source {A.B.C.D} group {A.B.C.D} vlan <1-4059>**
- **l2 tracemroute source {A.B.C.D} group {A.B.C.D} vrf WORD<1-16>**

### Command Parameters

**group {A.B.C.D}**

Specifies the multicast group address.

**priority <0-7>**

Specifies the priority. The default is 7.

**source {A.B.C.D}**

Specifies the source address.

**ttl-value <1-255>**

Specifies the time-to-live value for the trace.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the VRF name.

### Default

None

### Command Mode

User EXEC

## Command Output

The **12 tracemroute** command displays the following information for a VLAN:

Output field	Description
Source	Specifies the source IP address of the flow where the multicast trace tree originates.
Group	Specifies the IP address of the multicast group.
VLAN	Specifies the VLAN.
BMAC	Specifies the backbone MAC address.
B-VLAN	Specifies the backbone VLAN.
I-SID	Specifies the service identifier.

The **12 tracemroute** command displays the following information for a VRF:

Output field	Description
Source	Specifies the source IP address of the flow where the multicast trace tree originates.
Group	Specifies the IP address of the multicast group.
VRF	Specifies the VRF.
BMAC	Specifies the backbone MAC address.
B-VLAN	Specifies the backbone VLAN.
I-SID	Specifies the service identifier.

## I2 traceroute ip-address

Trigger a Layer 2 traceroute, which acts like native traceroute. Enable Connectivity Fault Management (CFM) to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

### Syntax

- **12 traceroute ip-address WORD<0-255>**
- **12 traceroute ip-address WORD<0-255> ttl-value <1-255>**
- **12 traceroute ip-address WORD<0-255> vrf WORD<1-16>**

### Command Parameters

**ip-address WORD<0-255>**

Specifies the IP address.

**priority <0-7>**

Specifies the priority. The default is 7.

**source-mode nodal**

Specifies the source mode of nodal. Nodal MPs provide both MEP and MIP functionality for SPBM deployments. Nodal MPs are associated with a B-VLAN and are VLAN encapsulated packets. The default is nodal.

#### source-mode smItVirtual

Specifies the source mode of smItVirtual. The switch supports SMLT interaction with SPBM. The platform uses two B-VIDs into the core from each pair of SMLT terminating nodes. Both nodes advertise the Nodal B-MAC into the core on both B-VIDS. In addition each node advertises the SMLT virtual B-MAC on one of the two B-VLANs. The default is nodal.

#### tTl-value <1-255>

Specifies the time-to-live (TTL) value. The default is 64.

#### vrf WORD<1-16>

Specifies the VRF name.

#### WORD<0-255>

Specifies the IP address.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

If you use this command on a DvR Leaf node, the output only shows DvR Controller IP addresses if the IP address or host route specified is unknown in the DvR domain.

## I2 traceroute vlan

Trigger a Layer 2 traceroute, which acts like native traceroute. Enable Connectivity Fault Management (CFM) to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

## Syntax

- **12 traceroute vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00**
- **12 traceroute vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00**
- **12 traceroute vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7>**
- **12 traceroute vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00 ttl-value <1-255>**
- **12 traceroute vlan <1-4059> routernodename WORD<0-255>**
- **12 traceroute vlan <1-4059> routernodename WORD<0-255> priority <0-7>**



- `12 traceroute vlan <1-4059> routernodename WORD<0-255> source-mode`
- `12 traceroute vlan <1-4059> routernodename WORD<0-255> source-mode nodal ttl-value <1-255>`
- `12 traceroute vlan <1-4059> routernodename WORD<0-255> source-mode smltVirtual ttl-value <1-255>`
- `12 traceroute vlan <1-4059> routernodename WORD<0-255> ttl-value <1-255>`
- `12 traceroute vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7> source-mode nodal ttl-value <1-255>`
- `12 traceroute vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7> source-mode nodal ttl-value <1-255>`
- `12 traceroute vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7> source-mode smltVirtual ttl-value <1-255>`
- `12 traceroute vlan <1-4059> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7> source-mode smltVirtual ttl-value <1-255>`

## Command Parameters

`<1-4059>`

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

`mac <0x00:0x00:0x00:0x00:0x00:0x00>`

Specifies the MAC address.

`priority <0-7>`

Specifies the priority. The default is 7.

`routernodename WORD<0-255>`

Specifies the router node name.

`ttl-value <1-255>`

Specifies the time-to-live (TTL) value. The default is 64.

## Default

None

## Command Mode

User EXEC

## I2 tracetree

Trigger a Layer 2 tracetree. Layer 2 tracetree allows a user to trigger a multicast link trace message (LTM) by specifying the Backbone VLAN (B-VLAN) and service instance identifier (I-SID). The command allows the user to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

### Syntax

- **l2 tracetree <1-4059> <1-16777215>**
- **l2 tracetree <1-4059> <1-16777215> mac 0x00:0x00:0x00:0x00:0x00:0x00**
- **l2 tracetree <1-4059> <1-16777215> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7>**
- **l2 tracetree <1-4059> <1-16777215> priority <0-7>**
- **l2 tracetree <1-4059> <1-16777215> routernodename WORD<0-255>**
- **l2 tracetree <1-4059> <1-16777215> routernodename WORD<0-255> priority <0-7>**
- **l2 tracetree <1-4059> <1-16777215> routernodename WORD<0-255> source-mode nodal ttl-value <1-255>**
- **l2 tracetree <1-4059> <1-16777215> routernodename WORD<0-255> source-mode smltVirtual ttl-value <1-255>**
- **l2 tracetree <1-4059> <1-16777215> routernodename WORD<0-255> ttl-value <1-255>**
- **l2 tracetree <1-4059> <1-16777215> source-mode nodal ttl-value <1-255>**
- **l2 tracetree <1-4059> <1-16777215> source-mode smltVirtual ttl-value <1-255>**
- **l2 tracetree <1-4059> <1-16777215> ttl-value <1-255>**

### Command Parameters

**<1-16777215>**

Specifies the service instance identifier (I-SID).

**<1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**mac <0x00:0x00:0x00:0x00:0x00:0x00>**

Specifies the MAC address.

**priority <0-7>**

Specifies the priority value. The default is 7.

**routernodename WORD<0-255>**

Specifies the router node name.

**source-mode nodal**

Specifies the source mode of nodal. The default is nodal.

**source-mode smltVirtual**

Specifies the source mode of smltVirtual. The default is nodal.

**ttl-value <1-255>**

Specifies the time-to-live (TTL) value. The default is 64.

## Default

None

## Command Mode

User EXEC

## l2 tracetree-fan

Trigger a Layer 2 tracetree-fan. Layer 2 tracetree-fan allows a user to trigger an LTM on the internal Fabric Area Network (FAN) I-SID.

## Syntax

- **l2 tracetree-fan mac 0x00 : 0x00 : 0x00 : 0x00 : 0x00 : 0x00**
- **l2 tracetree-fan mac 0x00 : 0x00 : 0x00 : 0x00 : 0x00 : 0x00 priority <0-7>**
- **l2 tracetree-fan priority <0-7>**
- **l2 tracetree-fan routernodename WORD <0-255>**
- **l2 tracetree-fan routernodename WORD <0-255> priority <0-7>**
- **l2 tracetree-fan routernodename WORD <0-255> ttl-value <1-255>**
- **l2 tracetree-fan ttl-value <1-255>**

## Command Parameters

**mac <0x00:0x00:0x00:0x00:0x00:0x00>**

Specifies the MAC address.

**priority <0-7>**

Specifies the priority value. The default is 7.

**routernodename WORD<0-255>**

Specifies the router node name.

**ttl-value <1-255>**

Specifies the time-to-live (TTL) value. The default is 64.

## Default

None

## Command Mode

User EXEC

## line-card

---

Perform trace commands for input/output cards.

## Syntax

- **line-card** <1-4> **trace grep** WORD<0-1024>
- **line-card** <1-4> **trace level** <<Module\_ID>> <0-4>
- **line-card** <1-4> **trace level**
- **line-card** <1-4> **trace grep**

## Command Parameters

<1-4>

Specifies the slot number. The number of slots supported depends on the hardware platform. For more information, see your hardware documentation.

**grep** <0-1024>

Greps the string in the range of 0 to 1024.

**trace**

Sets the trace level.

**trace grep** WORD<0-1024>

Greps the string in the range of 0 to 1024.

**trace level** <Module\_ID> <0-4>

Sets the trace level.

<Module\_ID> specifies the module for the trace. Different hardware platforms support different ID ranges because of feature support differences. To see which module IDs are available on the switch, use the **show trace modid-list** command or CLI command completion Help.

<0-4> specifies the trace level.

## Default

None

## Command Mode

User EXEC

## linktrace

Trigger a linktrace. The linktrace message is often compared to traceroute. A MEP transmits the Linktrace Message packet to a maintenance endpoint with intermediate points responding to indicate the path of the traffic within a domain for the purpose of fault isolation. The packet specifies the target MAC address of a MP, which is the SPBM system ID or the virtual SMLT MAC. MPs on the path to the target address respond with an LTR.

## Syntax

- `linktrace WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00>`
- `linktrace WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> detail`
- `linktrace WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> priority <0-7>`
- `linktrace WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> source-mode nodal`
- `linktrace WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> ttl-value <1-255>`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
detail`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
priority <0-7>`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
source-mode nodal`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
ttl-value <1-255>`

## Command Parameters

`<0-22 | 1-22 >`

Specifies the Maintenance domain name. The range depends on the hardware platform.

`<0x00:0x00:0x00:0x00:0x00:0x00>`

Specifies the remote MAC address to reach the MEP/MIP.

`<1-8191>`

Specifies the MEP ID.

`detail`

Displays linktrace result details.

**priority <0-7>**

Specifies the priority. The default is 7.

**source-mode nodal**

Specifies the source mode as nodal.

**ttl-value <1-255>**

Specifies the time-to-live (TTL) value. The default is 64.

## Default

None

## Command Mode

User EXEC

## login

---

Login to a different user access level.

## Syntax

- **login**

## Default

None

## Command Mode

User EXEC

## logout

---

Ends the current session.

## Syntax

- **logout**

## Default

None

## Command Mode

User EXEC

## loopback

Trigger the loopback test. The LBM packet is often compared to ping. A MEP transmits the loopback message to an intermediate or endpoint within a domain for the purpose of fault verification. This can be used to check the ability of the network to forward different sized frames.

### Syntax

- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00>`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> burst-count <1-200>`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> data-tlv-size <0-400>`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> frame-size <64-1500>`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> priority <0-7>`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> source-mode nodal`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern all-zero`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern all-zero-crc`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern pseudo-random-bit-  
sequence-crc`
- `loopback WORD<0-22> WORD<0-22> <1-8191>  
<0x00:0x00:0x00:0x00:0x00:0x00> time-out <1-10>`
- `loopback WORD<0-22> WORD<0-22> <1-8191><  
0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern pseudo-random-bit-  
sequence`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
burst-count <1-200>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
data-tlv-size <0-400>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
testfill-pattern all-zero-crc`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
time-out <1-10>`
- `loopback WORD<1-22> WORD<1-22> <1-8191>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00  
frame-size <64-1500>`

- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00 interframe-interval <0-1000>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00 source-mode nodal`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00 source-mode smltVirtual`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00 testfill-pattern all-zero`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00 testfill-pattern pseudo-random-bit-sequence`
- `loopback WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00 testfill-pattern pseudo-random-bit-sequence-crc`

## Command Parameters

`<0x00:0x00:0x00:0x00:0x00:0x00>`

Specifies the remote MAC address to reach the MEP/MIP.

`<1-8191>`

Specifies the MEP ID.

`burst-count <1-200>`

Specifies the burst count.

`data-tlv-size <0-400>`

Specifies the data Type-Length-Value (TLV) size.

`frame-size <64-1500>`

Specifies the frame size. The default is 0.

`interframe-interval <0-1000>`

Specifies the interval between LBM frames in msecs. A value of 0 msecs indicates to send the frames as fast as possible. The default is 500.

`priority <0-7>`

Specifies the priority. The default is 7.

`source-mode {nodal|noVlanMac|smltVirtual}`

Specifies the source mode as nodal, noVlanMac, or smltVirtual. Use the smltVirtual value with B-VLANs only. Use the noVlanMac value with C-VLANs only. The default is nodal.

`source-mode {nodal}`

Specifies the source mode as nodal.

`test-fill-pattern {all-zero|all-zero-crc|pseudo-random-bit-sequence|pseudo-random-bit-sequence-crc}`

Specifies the testfill pattern: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence:



PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: pseudo-random-bit-sequence with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is 1:all-zero.

**time-out <1-10>**

Specifies the time-out interval in seconds. The default is 3.

**WORD<1-22> WORD<1-22>**

The first parameter, specifies the Maintenance domain name. The second parameter, specifies the Maintenance association name.

## Default

None

## Command Mode

User EXEC

---

## ls

Lists files in a directory.

## Syntax

- **ls**
- **ls -r**
- **ls WORD<1-99>**

## Command Parameters

**-r**

Recurse into directories.

**WORD<1-99>**

Specify the directory path name.

## Default

None

## Command Mode

User EXEC

---

## manualtrigger ip rip interface

Sends a triggered update.

## Syntax

- **manualtrigger ip rip interface vlan <1-4059>**

## Command Parameters

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## ping

---

Ping a device to test the connection between the switch and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, displays a message that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address is not responding.

## Syntax



### Note

Command parameters for **ping** varies depending on the parameter input order. All syntax possibilities are not listed. You can use the CLI help to verify the syntax for available parameters during command contextual input.

- **ping WORD<0-256>**
- **ping WORD<0-256> count <1-9999>**
- **ping WORD<0-256> count <1-9999> mgmt [clip | oob | vlan]**
- **ping WORD<0-256> -d**
- **ping WORD<0-256> datasize <28-51200>**
- **ping WORD<0-256> datasize <28-51200> mgmt [clip | oob | vlan]**
- **ping WORD<0-256> grt**
- **ping WORD<0-256> grt interface gigabitEthernet {slot/port[sub-port]}**
- **ping WORD<0-256> grt interface tunnel <1-2000>**

- `ping WORD<0-256> grt interface vlan <1-4059>`
- `ping WORD<0-256> grt source WORD<1-256>`
- `ping WORD<0-256> -I <1-60>`
- `ping WORD<0-256> interface gigabitEthernet {slot/port[sub-port]}`
- `ping WORD<0-256> interface mgmtEthernet mgmt`
- `ping WORD<0-256> interface tunnel <1-2000>`
- `ping WORD<0-256> interface vlan <1-4059>`
- `ping WORD<0-256> mgmt [clip | oob | vlan]`
- `ping WORD<0-256> -s`
- `ping WORD<0-256> -s mgmt [clip | oob | vlan]`
- `ping WORD<0-256> scopeid <1-9999>`
- `ping WORD<0-256> source WORD<1-256>`
- `ping WORD<0-256> -t <1-120>`
- `ping WORD<0-256> -t <1-120> mgmt [clip | oob | vlan]`
- `ping WORD<0-256> vrf WORD<1-16>`
- `ping WORD<0-256> vrf WORD<1-16> interface gigabitEthernet {slot/port[sub-port]}`
- `ping WORD<0-256> vrf WORD<1-16> interface tunnel <1-2000>`
- `ping WORD<0-256> vrf WORD<1-16> interface vlan <1-4059>`
- `ping WORD<0-256> vrf WORD<1-16> source WORD<0-256>`

## Command Parameters

### `interface gigabitEthernet {slot/port[sub-port]}`

Specifies a specific outgoing interface to use by IP address. {slot/port[sub-port]} identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the subport in the format slot/port/sub-port.

### `interface gigabitEthernet {slot/port[sub-port]} | tunnel <1-2000> | vlan <1-4059>`

Specifies a specific outgoing interface to use by IP address. Additional ping interface filters: gigabitEthernet: {slot/port[sub-port]} gigabit vlan: Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### `mgmt`

Ping a network connection using a zero source IP address and route lookup in the main table.

### `mgmt clip`

Ping a network connection using a Segmented Management Instance. If you do not use the mgmt parameter, the ping command uses the IP routing stack to initiate the ping request.

### `mgmt oob`

Ping a network connection using a Segmented Management Instance. If you do not use the `mgmt` parameter, the ping command uses the IP routing stack to initiate the ping request.

**Note**

Exception: not supported on VSP 8600 Series or XA1400 Series.

**mgmt vlan**

Ping a network connection using a Segmented Management Instance. If you do not use the `mgmt` parameter, the ping command uses the IP routing stack to initiate the ping request.

**Note**

Exception: not supported on VSP 8600 Series.

**WORD <0-256>**

Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x:x:x:x:x) address (string length 0-256). Specifies the address to ping.

**WORD<0-256> count <1-9999>**

Specifies the number of times to ping(for IPV4/IPV6).

**WORD<0-256> -d**

Configures the ping debug mode. This variable detects local software failures (ping related threads creation or write to sending socket) and receiving issues (ICMP packet too short or wrong ICMP packet type) (for IPV4/IPV6).

**WORD<0-256> datasize <28-51200>**

Specifies the size of ping data sent in bytes. The `datasize` for IPv4 addresses is <28-9216>. The `datasize` for IPv6 addresses is <28-51200>. The default is 0.

**WORD<0-256> grt**

Specifies the ping is executed in Global Router (GRT) context.

**WORD<0-256> -I <1-60>**

Specifies the interval between transmissions (for IPV4/IPV6).

**WORD<0-256> interface mgmtEthernet mgmt**

Specifies an IP address that will be used as the source IP address in the packet header.

**Note**

Exception: only supported on VSP 8600 Series.

**WORD<0-256> interface tunnel <1-2000>**

Specifies the tunnel interface.

**WORD<0-256> interface vlan <1-4059>**

Specifies the virtual routing and forwarding (VRF) name from 1-16 characters.

**WORD<0-256> -s**

Configures the continuous ping at the interval rate defined by the [-I] parameter (for IPV4/IPV6).

**WORD<0-256> scopeid <1-9999>**

Specifies the scope ID. <1-9999> specifies the circuit ID for IPv6.

**WORD<0-256> source WORD<1-256>**

Specifies an IP address that will be used as the source IP address in the packet header.

**WORD<0-256> -t <1-120>**

Specifies the no-answer timeout value in seconds (1-120) (for IPV4/IPV6).

**WORD<0-256> vrf WORD<1-16>**

Specifies the virtual routing and forwarding (VRF) name from 1-16 characters.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The options [-d], [-l], [interface], [scopeid], [source], and [vrf] are not available if the *mgmt* keyword is specified.

All command parameters do not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## pwc ---

Prints the current working level.

## Syntax

- **pwc**

## Default

None

## Command Mode

User EXEC

## quick-config-mgmt ---

Runs the management interface setup utility to quickly configure an OOB or VLAN Segmented Management Instance.

## Syntax

- **quick-config-mgmt**

## Default

None

## Command Mode

User Exec

## Usage Guidelines

Segmented Management Instance support varies across hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## remove

---

Remove files or directories to free space.

## Syntax

- **remove WORD<1-255>**
- **remove WORD<1-255> -y**

## Command Parameters

**WORD<1-255>**

Specifies the file to rename.

**WORD<1-255> -y**

Skips the confirm question.

## Default

None

## Command Mode

User EXEC

---

## show alarm database

---

Show the contents of alarm-log buffers

## Syntax

- **show alarm database**
- **show alarm database alarm-id WORD<0-32>**
- **show alarm database alarm-status WORD<0-32>**
- **show alarm database alarm-type WORD<0-32>**
- **show alarm database event-code <0x0-0x00FFFFFF | 0x0-0x0>**
- **show alarm database module WORD<0-100>**
- **show alarm database severity WORD<0-25>**

## Command Parameters

**alarm-id WORD<0-32>**

Alarm ID

**alarm-status WORD<0-32>**

Alarm status

**alarm-type WORD<0-32>**

Specifies the type of alarm.

**event-code <0x0-0x00FFFFFF | 0x0-0x0>**

Event Code

**module WORD<0-100>**

Module

**severity WORD<0-25>**

Severity

## Default

None

## Command Mode

User EXEC

## Example

The following example displays the local alarms.

```
Switch:1#show alarm database
      ALARM      EVENT      ALARM      ALARM      CREATION  UPDATED      CLEARED
SLOT  ID          CODE          TYPE        STATUS     SEVERITY  FREQ        TIME        TIME        TIME        REASON
-----
CP1   00300001.238  0x0000c5e7  DYNAMIC    SET        INFO      1           [11/17/15 06:42:55.928] [11/17/15 06:42:55.928] [--/--/--]
--:--:--:--] Link Down(1/47)
CP1   00300001.239  0x0000c5e7  DYNAMIC    SET        INFO      1           [11/17/15 06:42:55.946] [11/17/15 06:42:55.946] [--/--/--]
--:--:--:--] Link Down(1/48)
CP1   00300001.241  0x0000c5e7  DYNAMIC    SET        INFO      1           [11/17/15 06:42:55.971] [11/17/15 06:42:55.971] [--/--/--]
--:--:--:--] Link Down(1/50)
```

```
CP1 00400005      0x000045e5  DYNAMIC   SET      INFO    1      [11/17/15 06:43:41.929] [11/17/15 06:43:41.929] [--/--/--]
--:--:--:--] Sending Cold-Start Trap
```

---

## show alarm statistics

---

Show the statistics of alarm-log buffers

### Syntax

- **show alarm statistics**

### Default

None

### Command Mode

User EXEC

---

## show application auto-provision

---

Display auto-provisioning status on the switch.

### Syntax

- **show application auto-provision**

### Default

None

### Command Mode

User Exec

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Example

The following example displays the auto-provision configuration and operational status:

```
Switch:1>show application auto-provision

Admin state      : Enabled
Operational state : Running
```



## show application iqagent

Show ExtremeCloud IQ Agent configuration information and status.

### Syntax

- **show application iqagent**

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show application iqagent** command displays the following information:

Output field	Description
Agent Admin State	Specifies the administrative state of the IQ Agent.
Agent Version	Specifies the IQ Agent version that runs on the device.
Agent Oper State	Specifies the operational status of the IQ Agent, whether IQ Agent is connected to ExtremeCloud IQ.
Server Address	Specifies the default ExtremeCloud IQ server.
Server Address Origin	Specifies the origin of the server IP address. <ul style="list-style-type: none"> <li>• None - displays the default value (nac.extremecloudiq.com) or 0.0.0.0</li> <li>• Configured - displays the static server IP address configured using CLI or EDM.</li> <li>• DHCP - displays the dynamic server IP address configured by the DHCP server.</li> </ul>
Proxy Address	Specifies the proxy address.
Proxy TCP Port	Specifies the proxy TCP port.
Proxy Username	Specifies the proxy server username.
Proxy Password	Specifies the proxy server password.

## Example

The following example displays the ExtremeCloud IQ Agent configuration.

```
Switch:1>show application iqagent

=====
                               IQAgent Info
=====
Agent Admin State      : true
Agent Version          : 0.2.7
Agent Oper State       : connected
Server Address         : hac.extremecloudiq.com
Server Address Origin  : None
Proxy Address          : extremeiq.com
Proxy TCP Port         : 21
Proxy Username         : admin
```

## show application iqagent status

Show IQAgent status information.

### Syntax

- **show application iqagent status**

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show application iqagent status** command displays the following information:

Output	Description
Connection Status	Specifies that ExtremeCloud IQ and IQAgent are connected.
Last Onboard Time	Specifies the Last Onboard Time for the feature.
Agent Version	Specifies the IQAgent version running on the device.
Association URL	Specifies the Association URL of the feature.

Output	Description
Poll URL	Specifies the poll URL of the feature.
Monitor Frequency	Specifies the monitor frequency of the feature.
Poll Frequency	Specifies the poll frequency of the feature.
Last Poll Status	Specifies the last poll status of the feature.
Last Poll Success Time	Specifies the last poll success time of the feature.
Last Health Status	Specifies the last health status of the feature.
Last Health Success Time	Specifies the last health success time of the feature.
Last Monitor Status	Specifies the last monitor status of the feature.
Last Monitor Success Time	Specifies the last monitor success time of the feature.

## Example

```
Switch:1>show application iqagent status
=====
                        IQAgent Status
=====
Connection Status      : Connected
Last Onboard Time     : 18:54:23 11 27 2019 UTC
Agent Version         : 0.2.7
Association URL        : https://10.16.231.98/hac-webapp/rest/v1/association
Poll URL              : https://10.16.231.98/hac-webapp/rest/v1/poll/1904Q-20028
Monitor Frequency     : 600
Poll Frequency        : 30
Last Poll Status      : SUCCESS
Last Poll Success Time : 14:39:16 11 28 2019 UTC
Last Health Status    : SUCCESS
Last Health Success Time : 14:38:35 11 28 2019 UTC
Last Monitor Status   : SUCCESS
Last Monitor Success Time : 14:38:35 11 28 2019 UTC
```

## show application restconf

Show the RESTCONF configuration and operation status.

### Syntax

- **show application restconf**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show application restconf** command displays the following information:

Output field	Description
Admin State	Specifies the administrative state of the RESTCONF application.
TCP Port	Specifies the TCP port for the RESTCONF server.
Certificate File Status	Specifies the status of TLS/SSL certificate file whether it is installed or uninstalled.
TLS Enable	Specifies whether TLS/SSL is enabled or disabled for the RESTCONF server.
Trap Notification	Specifies whether trap notification is enabled or disabled when the RESTCONF server is not available.
Oper State	Specifies the operational status of the RESTCONF server.
Web Server Version	Specifies the RESTCONF web server version that is running on the device.
RESTCONF Server Version	Specifies the RESTCONF server version that is running on the device.

## Example

The following example displays the RESTCONF configuration.

```
Switch:1>show application restconf
=====
                                RESTCONF Info
=====
Admin State           : true
TCP Port              : 8080
Certificate File Status : install
TLS Enable            : false
Trap Notification     : true
Oper State            : up
Web Server Version    : 1.0.1.11
RESTCONF Server Version : 1.0.1.39
=====
```

## show application restconf conflict-ifname

Show conflicting interface name information. To enable RESTCONF, the interface name (VLAN name, MLT name, and Port interface name) must be unique.

### Syntax

- **show application restconf conflict-ifname**

### Default

None

## Command Mode

User EXEC

## Example

The following example displays the RESTCONF conflicting interface name information.

```
Switch:1>show application restconf conflict-ifname
-----
Conflicting Interface IfName - Port, VLAN Name and MLT Name
-----
Mlt 1 name is same as Vlan 1001 name - "Interface-1"
Mlt 2 name is same as Vlan 1002 name - "VLAN-1002"
Vlan 1003 name is Mlt 1 Default Name - "MLT-1"
-----
Total Conflict Count: 3
```

## show application restconf invalid-name

Show VLAN or MLT names that contain prohibited special characters. To enable RESTCONF, VLAN and MLT names cannot contain special characters other than underscore (\_) or en dash (-).

## Syntax

- **show application restconf invalid-name mlt**
- **show application restconf invalid-name vlan**

## Command Parameters

**mlt**

Lists all MLT names that contain special characters.

**vlan**

Lists all VLAN names that contain special characters.

## Default

None

## Command Mode

User EXEC

## Example

The following example displays the RESTCONF MLT names that contain prohibited special characters.

```
Switch:1>show application restconf invalid-name mlt
-----
Invalid MLT names - Only "-" and "_" special characters are allowed
-----
```

```
Mlt 3 name has special characters - "gigi#g"  
Mlt 4 name has special characters - "my%mlt"  
Mlt 5 name has special characters - "isa.text"  
-----  
Total Invalid Names Count: 3
```

---

## show application slamon agent

Display the configuration information of the SLA Mon agent application.

### Syntax

- **show application slamon agent**

### Default

None

### Command Mode

User EXEC

---

## show app-telemetry counter

Displays the Application Telemetry status counters.

### Syntax

- **show app-telemetry counter**
- **show app-telemetry counter id <number>**
- **show app-telemetry counter name <rule>**

### Command Parameters

**id <1-2000>**

Specifies the rule ID number.

**id <1-2000>**

Shows the counters for the specified rule number.

**name WORD<1-32>**

Specifies the name of the rule.

**name WORD<1-32>**

Shows the counters for the specified rule name.

### Default

None

## Command Mode

User EXEC

## Command Output

The **show app-telemetry counter** command displays the following information:

Output field	Description
EntryId	Displays the Application Telemetry rule ID.
Name	Displays the rule name.
Packets	Displays the number of packets transmitted to the Analytics Engine that matched the specified pattern in the rule.
Bytes	Displays the total number of bytes in the packets.

## Example

The following example displays the Application Telemetry counters.

```
Switch:1>show app-telemetry counter

=====
Application Telemetry Counters
=====
EntryId      Name      Packets    Bytes
-----
1            ssh       1258       72145
2            sslclient 457         27000
-----

All 2 out of 2 Total Num of Application Telemetry counters entries displayed
```

## show app-telemetry status

Displays whether Application Telemetry is enabled or disabled and whether or not the collector is reachable.

## Syntax

- **show app-telemetry status**

## Default

None

## Command Mode

User EXEC

---

## show auto-sense

---

Displays the Auto-sense configuration on the switch.

### Syntax

- **show auto-sense [access-differv] [data] [dhcp-detection] [eapol] [fa] [isis] [onboarding] [qos] [voice] [wait-interval]**

### Command Parameters

#### access-differv

Displays the Auto-sense configuration related to Differentiated Services (DiffServ).

#### data

Displays the Auto-sense configuration related to the data I-SID.

#### dhcp-detection

Displays the Auto-sense configuration related to DHCP server auto-detection.

#### eapol

Displays the Auto-sense configuration related to Link Layer Discovery Protocol (LLDP) authentication for Extensible Authentication Protocol over LAN (EAPoL or EAP).

#### fa

Displays the Auto-sense configuration related to Fabric Attach (FA) message authentication and FA client-specific configuration.

#### isis

Displays the Auto-sense configuration related to Intermediate-System-to-Intermediate-System (IS-IS) authentication.

#### onboarding

Displays the Auto-sense configuration related to the onboarding I-SID.

#### qos

Displays the Auto-sense configuration related to overriding 802.1p bits.

#### voice

Displays the Auto-sense configuration related to voice for IP phones.

#### wait-interval

Displays the Auto-sense configuration related to the time to wait for an LLDP neighbor to be detected in the Auto-sense wait state before transitioning to the Auto-sense onboarding state.

### Default

None.

### Command Mode

User EXEC



## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show autotopology nmm-table

View topology message status to view the interconnections between Layer 2 devices in a network.

## Syntax

- **show autotopology nmm-table**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show autotopology nmm-table** command displays the following information:

Output field	Description
Local Port	Specifies the slot and port that received the topology message.
IpAddress	Specifies the IP address of the sender of the topology message.
SegmentId	Specifies the segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddress	Specifies the MAC address of the sender of the topology message.
ChassisType	Specifies the chassis type of the device that sent the topology message.
BT	Specifies the backplane type of the device that sent the topology message. The switch uses a backplane type of 12.
LS	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CS	Specifies the current state of the sender of the topology message. The choices are <ul style="list-style-type: none"> <li>• topChanged—Topology information recently changed.</li> <li>• HtBt (heartbeat)—Topology information is unchanged.</li> <li>• new—The sending agent is in a new state.</li> </ul>
Rem Port	Specifies the slot and port that sent the topology message.

## Example

The following example displays the topology message status.

```
Switch:1(config)#show autotopology nmm-table
=====
                        Topology Table
=====
Local                               Rem
Port      IPAddress      SegmentId MacAddress  ChassisType      BT LS  CS  Port
-----
0/0        192.0.2.81      0x000000  0030ab707a00 ChassisType 1      12 Yes HtBt 0/0
1/1        192.0.2.81      0x000000  0050ea268800 ChassisType 2      12 Yes HtBt 1/50
1/42       192.0.2.81      0x000000  070ab307aa00 ChassisType 3      12 Yes HtBt 1/1
2/1        192.0.2.81      0x000000  0030ab57ab00 ChassisType 4      12 Yes HtBt 1/49
2/2        192.0.2.81      0x000000  0030ab307af0 ChassisType 5      12 Yes HtBt 1/50
2/41       192.0.2.81      0x000000  00e0ba327c00 ChassisType 6      12 Yes HtBt 2/1
2/42/1     192.0.2.81      0x000000  0050eb127400 ChassisType 7      12 Yes HtBt 1/2
```

## show banner

Display the banner information.

### Syntax

- **show banner**

### Default

None

### Command Mode

User EXEC

## show basic config

Display the basic switch configuration.

### Syntax

- **show basic config**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show basic config** command displays the following information:

Output field	Description
setdate	Displays the system date configuration.
mac-flap-time-limit	Displays the time limit for the loop-detect feature, in milliseconds, for MAC flapping.
auto-recover-delay	Displays the time interval, in seconds, after which autorecovery runs on ports to clear actions taken by CP Limit or link flap.

## Example

The following example displays the basic switch configuration.

```
Switch:1#show basic config
                setdate : N/A
mac-flap-time-limit : 500
auto-recover-delay : 30
```

## show bgp ipv6 aggregates

Display BGP IPv6 aggregates information.

## Syntax

- **show bgp ipv6 aggregates** [**WORD** <1-256>] [**vrf** **WORD**<1-16>] [**vrfids** **WORD**<0-512>]
- **show bgp ipv6 aggregates vrf** **WORD**<1-16>
- **show bgp ipv6 aggregates vrfids** **WORD**<0-512>
- **show bgp ipv6 aggregates** **WORD**<1-256>

## Command Parameters

**vrf** <WORD 1-16>

Specifies the VRF name.

**vrfids** <WORD 0-512>

Specifies VRF IDs.

**WORD** <1-256>

Specifies the IPv6 prefix and length.

## Default

None

## Command Mode

User EXEC

## show bgp ipv6 imported-routes

---

Display BGP IPv6 imported-routes information.

### Syntax

- **show bgp ipv6 imported-routes** [WORD <1-256>] [longer-prefixes] [vrf WORD<1-16>] [vrfids WORD<0-512>]
- **show bgp ipv6 imported-routes** WORD<1-256>
- **show bgp ipv6 imported-routes** WORD<1-256> longer-prefixes

### Command Parameters

#### longer-prefixes

Shows long prefixes. the longer-prefixes indicate the mask length from any specified prefix to 32 (for example show from prefix A.B.C.D/len to A.B.C.D/32.)

#### vrf <WORD 1-16>

Specifies the VRF name.

#### vrfids <WORD 0-512>

Specifies VRF IDs.

#### WORD <1-256>

Specifies the IPv6 prefix and length.

### Default

None

## Command Mode

User EXEC

## show bgp ipv6 neighbors

---

Display BGP IPv6 neighbors.

### Syntax

- **show bgp ipv6 neighbors** WORD <1-256> vrf WORD<1-16>
- **show bgp ipv6 neighbors** WORD <1-256> vrf WORD<1-16> vrfids WORD<0-512>
- **show bgp ipv6 neighbors** WORD <1-256> vrfids WORD<0-512>
- **show bgp ipv6 neighbors** WORD<1-256> advertised-routes

- **show bgp ipv6 neighbors WORD<1-256> advertised-routes WORD<1-256>**
- **show bgp ipv6 neighbors WORD<1-256> advertised-routes WORD<1-256> longer-prefixes**
- **show bgp ipv6 neighbors WORD<1-256> routes**
- **show bgp ipv6 neighbors WORD<1-256> routes community disable**
- **show bgp ipv6 neighbors WORD<1-256> routes community enable**
- **show bgp ipv6 neighbors WORD<1-256> routes WORD<1-256>**
- **show bgp ipv6 neighbors WORD<1-256> routes WORD<1-256> longer-prefixes**

## Command Parameters

**advertised-routes WORD<1-256>**

Displays information about BGP peer advertised routes. The IPv6 address is optional.

**community <disable | enable>**

Enables the display of community attributes.

**longer-prefixes**

Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c.d/32).

**routes WORD<1-256>**

Displays information about BGP peer routes.

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

**WORD<1-256>**

Specifies the IPv4 or IPv6 address.

## Default

None

## Command Mode

User EXEC

## show bgp ipv6 networks

Display information about BGP network configurations.

## Syntax

- **show bgp ipv6 networks WORD <1-256> vrf WORD<1-16>**
- **show bgp ipv6 networks WORD <1-256> vrf WORD<1-16> vrfids WORD<0-512>**
- **show bgp ipv6 networks WORD <1-256> vrfids WORD<0-512>**
- **show bgp ipv6 networks WORD<1-256>**

## Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

**WORD <1-256>**

Specifies IPv6 prefix and length in the range of 1 to 256

## Default

None

## Command Mode

User EXEC

# show bgp ipv6 redistributed-routes

---

Display BGP IPv6 redistributed-routes information.

## Syntax

- **show bgp ipv6 redistributed-routes vrf WORD<1-16>**
- **show bgp ipv6 redistributed-routes [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show bgp ipv6 redistributed-routes vrfids WORD<0-512>**

## Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

## show bgp ipv6 route

---

Display information about BGP IPv6 routes.

### Syntax

- **show bgp ipv6 route vrfids WORD<0-512>**
- **show bgp ipv6 route community {disable|enable}**
- **show bgp ipv6 route ipv6 WORD<1-256>**
- **show bgp ipv6 route vrf WORD<1-16>**
- **show bgp ipv6 route vrf WORD<1-16> vrfids WORD<0-512>**
- **show bgp ipv6 route WORD <1-256>**
- **show bgp ipv6 route WORD<1-256> longer-prefixes**

### Command Parameters

**community {disable|enable}**

Enables or disables the display of community attributes.

**ipv6 WORD<1-256>**

Specifies an IPv6 address.

**longer-prefixes**

Shows long prefixes. the longer-prefixes indicate the mask length from any specified prefix to 32 (for example show from prefix A.B.C.D/len to A.B.C.D/32.)

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

**WORD <1-256>**

Specifies IPv6 address and length in the range of 1 to 256

### Default

None

### Command Mode

User EXEC

## show bgp ipv6 summary

---

Shows a summary of BGP peering over IPv6 transport.

### Syntax

- **show bgp ipv6 summary vrf WORD<1-16>**
- **show bgp ipv6 summary vrf WORD<1-16> vrfids WORD<0-512>**
- **show bgp ipv6 summary vrfids WORD<0-512>**

### Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

### Default

None

### Command Mode

User EXEC

## show brouter

---

Show brouter port information.

### Syntax

- **show brouter**

### Default

None

### Command Mode

User EXEC

## show certificate ca

---

Display the certificate authority details.



## Syntax

- **show certificate ca WORD<1-45>**

## Command Parameters

**WORD<1-45>**

Specifies name of the Certificate Authority. If the name is not specified, the command displays the CA details of all configured CA.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show certificate ca** command displays the following information:

Output field	Description
<i>Name</i>	Specifies the user defined name referring to the Certificate Authority issuing the Digital Certificate.
<i>CommonName</i>	Specifies the Common Name of the Certificate Authority issuing the Digital Certificate.
<i>KeyName</i>	Specifies the generated key pair that was first associated with the CA trustpoint.
<i>SubjectName</i>	Specifies the subject Distinguished Name (DN) or subject alternative name identity to bind with the CA trustpoint. The default is Global.
<i>CaUrl</i>	Specifies the URL of the Certificate Authority issuing the Digital Certificate.
<i>UsePost</i>	Specifies if the HTTP request type is URL or POST. Where, TRUE indicates EJBCA and FALSE indicates Win2012 CA.
<i>SubjectCertValidityDays</i>	Specifies number of days for which subject certificate is valid.

Output field	Description
<i>Action</i>	Specifies the various actions that a Certificate Authority can take. <ul style="list-style-type: none"> <li>• noop - No operation</li> <li>• caauth - Certificate Authority authentication</li> <li>• enroll - Certificate Enrolment Request</li> <li>• renew - Certificate Renew Request</li> <li>• remove - Removes the subject certificate obtained online from the Certificate Authority</li> <li>• install - Installs the subject certificate obtained online from the Certificate Authority</li> <li>• generateCsr - Generates the Certificate Signing Request required to obtain the Offline Subject Certificate</li> </ul>
<i>LastActionStatus</i>	Specifies the status of the last action. <ul style="list-style-type: none"> <li>• none - No action is performed yet</li> <li>• success - Execution of the action triggered is completed successfully</li> <li>• failed - Execution of the action triggered has failed</li> <li>• inProgress - Execution of the action triggered is in progress</li> </ul>
<i>LastActionFailureReason</i>	Specifies the reason of failure for the last action performed by the Certificate Authority.
<i>UsedFor</i>	Specifies if the CA trustpoint is used by a specific application, such as SSH-X509. Default indicates the first configured CA trustpoint. Default displays in this field if you have only one CA trustpoint configured.

The following examples displays the certificate CA information:

```
Switch:1(config)#show certificate ca

CA table entry
Name           : a1
CommonName    : CaA1
KeyName       : rsa_2048
SubjectName   :
CaUrl         : http://192.51.100.9:8080/ejbca/publicweb/apply/scep/test/
pkiclient.exe
UsePost       : 1
SubjectCertValidityDays : 365
Action        : (null)
LastActionStatus : (null)
LastActionFailureReason :
CA-Auth Sha256Fingerprint :
bd9bb74b3f4d75e86113222a8d291b6349c7a42c457e487b9be0a48b4f09cc7c
UsedFor       :

CA table entry
Name           : a2
CommonName    : CaA2
KeyName       : pki_key
SubjectName   : 822
CaUrl         : http://192.51.100.9:8080/ejbca/publicweb/apply/scep/test/
pkiclient.exe
```

```
UsePost          : 1
SubjectCertValidityDays : 365
Action           : (null)
LastActionStatus  : (null)
LastActionFailureReason :
CA-Auth Sha256Fingerprint :
0ccb8d0c38d36cf427187f0e1dd380536c078fd6fae39ec9872187327912056b
UsedFor          : Default
```

## show certificate cert-type

Display the digital certificate for given certificate type or lists all the certificate details from the local store for given certificate type.

### Syntax

- **show certificate cert-type default-tls-certificate**
- **show certificate cert-type intermediate-ca-cert WORD<1-80>**
- **show certificate cert-type offline-ca-cert**
- **show certificate cert-type offline-subject-cert**
- **show certificate cert-type online-ca-cert**
- **show certificate cert-type online-subject-cert**
- **show certificate cert-type root-ca-cert WORD<1-80>**

### Command Parameters

#### default-tls-certificate

Displays the default TLS certificate (self-signed).

#### intermediate-ca-cert WORD<1-80>

Specifies the intermediate certificate obtained offline from Certificate Authority.

#### offline-ca-cert

Specifies Certificate Authority certificate obtained offline from Certificate Authority

#### offline-subject-cert

Specifies subject certificate obtained offline from Certificate Authority.

#### online-ca-cert

Specifies Certificate Authority Certificate obtained online from Certificate Authority.

#### online-subject-cert

Specifies subject certificate obtained online from Certificate Authority.

#### root-ca-cert WORD<1-80>

Specifies root certificate obtained offline from Root Certificate Authority.

### Default

None

## Command Mode

User EXEC

## Command Output

The **show certificate cert-type** command displays the following information:

Output field	Description
Certificate Type	Indicates the type of certificate. <ul style="list-style-type: none"> <li>• Self-signed certificate</li> <li>• Root Certificate</li> <li>• Offline subject certificate</li> <li>• Online subject certificate</li> <li>• Intermediate CA certificate</li> <li>• Offline CA certificate</li> <li>• Online CA certificate</li> </ul>
VersionNumber	Indicates the certificate version number for the subject as issued by the Certificate Authority.
SerialNumber	Indicates the certificate serial number for the subject as issued by the Certificate Authority.
IssuerName	Indicates the certificate issuer name for the subject as issued by the Certificate Authority.
ValidityPeriodNotBefore	Indicates the certificate validation period start date for the subject as issued by the Certificate Authority.
ValidityPeriodNotAfter	Indicates the certificate validation period last date for the subject as issued by the Certificate Authority.
CertificateSignatureAlgorithm	Indicates the algorithm used for the issuer's signature on the certificate for the subject as issued by the Certificate Authority.
CertificateSignature	Indicates the issuer's signature on the certificate for the subject as issued by the Certificate Authority.
Subject	Indicates the details of the subject on its certificate as issued by Certificate Authority.
SubjectPublicKeyAlgorithm	Indicates the algorithm used to generate the subject's public key for the certificate issued by the Certificate Authority.
SubjectPublicKey	Indicates the public key of the subject used for Certificate Signing Request.
HasBasicConstraint	Indicates whether certificate contains basic certificate constraint.
HasKeyUsage	Indicates whether certificate contains basic key usage constraint.
IsCa	Indicates if the certificate is a CA certificate or not.

Output field	Description
KeyUsage	Indicates the purpose of the key used in the certificate. It is represented in the form of bits as follows: <ul style="list-style-type: none"> <li>• bit 0 - digitalSignature</li> <li>• bit 1 - nonRepudiation</li> <li>• bit 2 - keyEncipherment</li> <li>• bit 3 - dataEncipherment</li> <li>• bit 4 - keyAgreement</li> <li>• bit 5 - keyCertSign</li> <li>• bit 6 - cRLSign</li> <li>• bit 7 - encipherOnly</li> <li>• bit 8 - decipherOnly</li> </ul>
ExtendedKeyUsage	Indicates the purpose for which the key is used in addition to or in place of the basic purposes indicated in the key-usage field of the certificate.
CDPUrl	Indicates the CDP URL present in the Digital Certificate Extensions field.
OCSPUrl	Indicates the OCSP URL present in the Digital Certificate AIA field.
Status	Indicates the certificate status.
Installed	Indicates if the certificate is installed.

The following example displays the offline subject certificate:

```
Switch:1>show certificate cert-type offline-subject-cert
CERT table entry
Certificate Type           : Offline Subject Certificate
VersionNumber             : X.509 v3
SerialNumber              : 5de44b25394462b8
IssuerName                : CN:subCa1, EM:, OU:, O:, L:, P:, C:
ValidityPeriodNotBefore  : 07/05/2021 12:24:45
ValidityPeriodNotAfter   : 07/05/2022 12:24:45
CertificateSignatureAlgorithm : sha256withRSAEncryption
CertificateSignature      :
34f5037b30b0332e15f504316be86afcc41ad0b93699bc8de1b5cbe97a8cc834593837032ab492e0c5eee9a1fe
8db
99e8ea7aeb41fdce86818e0c08b1ed9e79a43247383e88fd3ef504a28b1ee525be60cba78291be16f57fb54174
33ec9dce601c9b4e77986c5db9430ce6cece48b
3dc143d042614404bdc3c2df16f68bb1b0609e593636a2806b285cb8fa7e470b442b50e4d3c4a663ac99d5d3b4
29a9b4966ea5ce16da6b7d7c5607832cc6acaea
e578419ba52e11cbe30d2cbb53a05de58e374657fc5983a92c699ba6896160c9f32e6625bd6f71003259773e71
d7c89df3ddc0a8603c1a8c8f6e248002f2bd217
1a6e922abf2e8134b311d1897319bbb7
Subject                   : CN:s15, EM:demo, OU:demo, O:demo, L:demo, P:demo, C:RO
SubjectPublicKeyAlgorithm : rsaEncryption
SubjectPublicKey          :
0000000000000000000020000000100000000300d06092a864886f70d010101050000000000000010d02000000003
010
00100000100c150b1851644aaaf08060f3b3a7a0618758b84184867ffd80b3e02ec30676171fe36e99f545065
6fc6e6db672b6239f760c97c3e49639cea5d503
c0e478bf7a4d213d5698d09d63622ccb279adbaa34135c81d70660489b55b6abca594f17d8ed250cf917325d
f0f73a10896157e6e3a24a584bc713b2e6493d0
59c8efd53bbbf5db0aa95b43c1668ba1053d0fe0e5c44dc889bd35bf11730e5827cb2068048ab97e9f0757514f
47332337376eed83a7cb95a53462639f5a47f02
6b0172cfa3ddfefe7269e737a32d8f2e5590a9ee07d3f329af4e4f2a73ed9de599916bc25e6ac51e482cbbb71f
```

```

736ec0e396fc314e5eed3c438efff68d1a31bdb
ed24d55
HasBasicConstraint      : 1
HasKeyUsage             : 1
IsCa                    : 0
KeyUsage                : 15 digitalSignature nonRepudiation keyEncipherment
dataEncipherment
ExtendedKeyUsage       : TLS Web Client Authentication, OCSP Signing, TLS Web
Server Authentication,
CDPUrl                 : http://192.51.100.9:8080/ejbca/publicweb/webdist/
certdist?cmd=crl&issuer=CN=subCa1
OCSPUrl                : http://192.51.100.9:8080/ejbca/publicweb/status/ocsp

Revocation Status      : unknown
Status                 : offline-certificate
Installed               : 1

CertificateFileName     : self_cert_s15.der

```

## show certificate key-name

Display the name and public key of all the key-pairs.

### Syntax

- **show certificate key-name**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show certificate key-name** command displays the following information:

Output field	Description
Key Name	Indicates the name of the key-pair generated for the subject. It is an auto generated entity, generated as the combination of key-type and key-size.
Public Key Value	Indicates the public key of the subject used to the Certificate Signing Request.

The following examples displays the key-pairs:

```

Switch:1>show certificate key-name
Key Name: pki_key
Public Key Value:
00000000000000010000000102000000000301000100000100bdb1cf8382d66a2d2d0d24b4477908641c16423c
089d9131781a3ada005e

```

```

52074e1ff3561e29598f93c53dcb06e4d235335573419bb938b6ccf93d3e6767d0932e129ea2f556276efce2be
825df1f9dc661d3cafee7125f4f7126f5ba7e8
d9029623398b7d3fb00063ea0e4bedd56e276c52a6371b289de3ee4198ff2397b512b516604eac4e5f0f4a0621
d7ac42541491d368f21e17a440aa6130a825a2
a7ca6ab1d7a7868f93e4d0d83c7e4973cf204b4f5f654abbaa9aa6199247976488b0957e65b656a6d21a2a4ac4
d322a36c786d8a8deec763b6aec0d05b0f6bfe
87602caecb2cc71e2e4f9f4f8c4d4d4e9b25adf9c02eb44b763542f0449a326d0f3b

```

Key Name: rsa\_2048

Public Key Value:

```

0000000000000001000000010200000000301000100000100c150b1851644aaaf08060f3b3a7a0618758b841
84867ffd80b3e02ec306
76171fe36e99f5450656fc6e6db672b6239f760c97c3e49639cea5d503c0e478bf7a4d213d5698d09d63622ccb
279addbaa34135c81d70660489b55b6babca59
4f17d8ed250cf917325df0f73a10896157e6e3a24a584bc713b2e6493d059c8efd53bbbf5db0aa95b43c1668ba
1053d0fe0e5c44dc889bd35bf11730e5827cb2
068048ab97e9f0757514f47332337376eed83a7cb95a53462639f5a47f026b0172cfa3ddf0e7269e737a32d8f
2e5590a9ee07d3f329af4e4f2a73ed9de59991
6bc25e6ac51e482cbbb71f736ec0e396fc314e5eed3c438efff68d1a31bdbed24d55

```

## show certificate subject

Display the details of the configured subject.

### Syntax

- **show certificate subject**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show certificate subject** command displays the following information:

Output field	Description
Subject Name	Specifies the Subject Name field of the subject sending the Certificate Signing Request (CSR) to the Certificate Authority. The default is Global.
CommonName	Specifies the Common Name field of the subject sending the CSR to the Certificate Authority.
EmailAddress	Specifies the Email address of the subject sending the CSR to the Certificate Authority.
OrganizationalUnit	Specifies the Organizational Unit field of the subject sending the CSR to the Certificate Authority.

Output field	Description
Organization	Specifies the Organization of the subject sending the CSR to the Certificate Authority.
Locality	Specifies the name of the Locality of the subject sending the CSR to the Certificate Authority.
Province	Specifies the Province name of the subject sending the CSR to the Certificate Authority.
Country	Specifies the name of the country of the subject sending the CSR to the Certificate Authority.

The following examples displays the details of the configured subject:

```
Switch:1>show certificate subject
Subject Name      : client1
Common Name      : client1.example.dod.mil
Email Address    : client1@extemenetworks.com
Organizational Unit : Engineering
Organization     : ExtremeNetworks
Locality        : Salem
Province        : Massachusetts
Country         : US

Subject Name      : Global
Common Name      : s15
Email Address    : enduser15@extremenetworks.com
Organizational Unit : Engineering
Organization     : ExtremeNetworks
Locality        : Salem
Province        : Massachusetts
Country         : US
```

## show certificate subject-alternative-name

View the subject alternative names configured on the switch.

### Syntax

- **show certificate subject-alternative-name**

### Default

None.

### Command Mode

User EXEC



## Command Output

The **show certificate subject-alternative-name** command displays the following information:

Output field	Description
TYPE	Specifies the type of subject alternative name in the table.
NAME	Specifies the alternative name in table.

## Example

The following example displays the switch configuration.

```
Switch:1>show certificate subject-alternative-name
=====
SAN Table
=====
TYPE      NAME                               SUBJECT
-----
E-MAIL    name@company.com                   822
DNS       822.extremenetworks.com           822
IP        192.0.2.22                         822
```

## show cfm cmac

Displays the global CFM CMAC configuration for the C-VLAN. This command does not apply to all hardware platforms.

## Syntax

- **show cfm cmac**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show cfm cmac** command displays the following information:

Output field	Description
LEVEL	Specifies the global C-VLAN CFM maintenance level for the chassis. The default is 4.
ADMIN	Specifies if CFM C-VLAN MEPs and MIPs are globally enabled.
MEP ID	Specifies the global MEP ID. The default is 1.
MAC	Specifies the MAC address.

## show cfm maintenance-association

Display the Connectivity Fault Management (CFM) Maintenance-Association configuration. An MA represents a logical grouping of monitored entities within its Maintenance Domain.

### Syntax

- **show cfm maintenance-association**

### Default

None

### Command Mode

User EXEC

## show cfm maintenance-domain

Display the Connectivity Fault Management (CFM) Maintenance-Domain configuration. A Maintenance-Domain is the part of a network that is controlled by a single administrator. A single MD may contain several Maintenance-Associations (MA).

### Syntax

- **show cfm maintenance-domain**

### Default

None

### Command Mode

User EXEC

---

## show cfm maintenance-endpoint

---

Display the Connectivity Fault Management Maintenance Endpoint configuration. A Maintenance Endpoint (MEP) represents a managed CFM entity, associated with a specific Domain Service Access Point of a service instance, which can generate and receive CFM Protocol Data Units (PDUs) and track any responses. MEP functionality can be divided into the following functions: Fault Detection, Fault Verification, Fault Isolation and Fault Notification.

### Syntax

- **show cfm maintenance-endpoint**

### Default

None

### Command Mode

User EXEC

---

## show cfm spbm

---

Displays the global CFM MEP configuration for SPBM VLANs.

### Syntax

- **show cfm spbm**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show cfm spbm** command displays the following information:

Output field	Description
LEVEL	Specifies the global SPBM CFM maintenance level for the chassis. The default is 4.
ADMIN	Specifies if CFM MEPs and MIPs are globally enabled.
MEP ID	Specifies the global MEP ID. The default is 1.
MAC	Specifies the MAC address.

## show cli info

Display general Console settings.

### Syntax

- **show cli info**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show cli info** command displays the following information:

Output field	Description
more	Displays if scrolling for the output display is enabled.
screen-lines	Displays the number of lines in the output display for the current session.
telnet-sessions	Displays the number of supported inbound Telnet sessions
rlogin-sessions	Displays the number of supported inbound Rlogin sessions
timeout	Displays the idle timeout period before automatic logoff.
monitor duration	Displays the duration for which statistics are monitored.
monitor interval	Displays the interval at which statistics are monitored.
use default login prompt	Displays if the system uses the default login prompt.
default login prompt	Displays the default login prompt.
custom login prompt	Displays the custom login prompt.
use default password prompt	Displays if the system uses the default password prompt.
default password prompt	Displays the default password prompt.
custom password prompt	Displays the custom password prompt.
prompt	Displays the system prompt.

### Example

The following example displays information about the CLI configuration.

```
Switch:1>show cli info  
  
cli configuration
```

```
more          : true
screen-lines  : 23
telnet-sessions : 8
rlogin-sessions : 8
timeout       : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt : true
default login prompt     : Login:
custom login prompt      : Login:
use default password prompt : true
default password prompt  : Password:
custom password prompt    : Password:
prompt : Switch
```

## show cli password

---

Display the access, logon name, and password combinations.

### Syntax

- **show cli password**

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

After you enable enhanced secure mode, the parameters in the output for the **show cli password** command apply to all of the role-based users, except for the admin user. So for instance, the system mandates that the admin user must have a password length of 15, and a password with two of each of the following characters:

- uppercase
- lowercase
- numeric
- special character

However, the admin user can configure this differently for the other user access levels. The values that display for min-passwd-len and password-rule are those configured by admin, and they apply to the privilege, operator, security, and auditor access levels.

## Command Output

The **show cli password** command displays the following information:

Output field	Description
aging	Displays the maximum validity period, in days, for a password.
min-passwd-len	Displays the minimum length for passwords.
password-history	Displays the number of previous passwords the switch stores.
password-hashing	Displays the Secure Hash Algorithm (SHA) level.
change-interval	Displays the minimum period of time, in hours, between password changes.
password-rule	Displays the password complexity rule. The first variable defines the number of uppercase characters required. The second variable defines the number of lowercase characters required. The third variable defines the number of numeric characters required. The fourth variable defines the number of special characters required.
pre-expiry-notification-interval	Displays the interval between notifications to users that their passwords will expire.
post-expiry-notification-interval	Displays the interval between notifications to users that their passwords have expired.
ACCESS	Displays the access level.
LOGIN	Displays the username associated with the access level.
STATE	Displays if the access level is enabled.
MAX-SSH-SESSIONS	Displays the maximum number of SSH sessions allowed for each access level.
Default Lockout Time	Displays the lockout time, in seconds, after the configured number of invalid attempts.
Default Lockout Retries	Displays the number of invalid attempts allowed before lockout.
Lockout-Time	Displays the IP address and timeout for locked out hosts due to invalid login attempts.

## Examples

The following example displays output from the **show cli password** command if enhanced secure mode is disabled.

```
Switch:1#show cli password
access-level
aging      90

min-passwd-len 10
password-history 3
password-hashing sha2

ACCESS    LOGIN      STATE
13        13         ena
12        12         ena
11        11         ena
Default Lockout Time 60
```

```

Default Lockout Retries          3
Lockout-Time:
  IP                               Time
src = 10.1.213.11                timeout = 60

```

The following example displays output from the **show cli password** command if enhanced secure mode is enabled.

```

Switch:1#show cli password
  change-interval 24
  min-passwd-len 8
  password-history 3
  password-rule 1 1 1 1
  pre-expiry-notification-interval 1 7 30
  post-expiry-notification-interval 1 7 30
  access-level
ACCESS      LOGIN      AGING  MAX-SSH-SESSIONS  STATE
admin       rwa          90    3                  ena
privilege   rwa          90    3                  dis
operator    oper1        90    3                  ena
security    security     90    3                  ena
auditor     auditor      90    3                  ena
Default Lockout Time          60
Lockout-Time:

```

## show cliilog

Verify the configuration and view the log file.

### Syntax

- **show cliilog**
- **show cliilog [file] [tail] [grep WORD<1-256>]**

### Command Parameters

#### file

Shows the log file.

#### grep WORD <1-256>

Shows the last results first.

#### tail

Performs a string search in the log file. WORD <1-256> is the string, of up to 256 characters in length, to match.

### Default

None

### Command Mode

User EXEC

## Usage Guidelines

This command only applies to log files generated by releases earlier than Release 3.2. Not all hardware platforms support these earlier releases. In later releases, the command is replaced by **show logging file module cliilog**. For more information about software release support on your platform, see the hardware and software compatibility information in [VSP 8600 Release Notes](#).

## show clock

---

Display the current time.

### Syntax

- **show clock**
- **show clock detail**
- **show clock time-zone**

### Command Parameters

#### detail

Displays detailed date information.

#### time-zone

Displays the local time-zone configuration.

### Default

None

### Command Mode

User EXEC

## show debug

---

Shows debugging configuration.

### Syntax

- **show debug ip pim**
- **show debug ipv6 pim**

### Command Parameters

#### ip pim

Shows the configuration of IP PIM debugging commands.

#### ipv6 pim



Shows the configuration of IPv6 PIM debugging commands.

## Default

None

## Command Mode

User EXEC

## show debug-file

---

Shows how you view all debug files for all slots.

## Syntax

- **show debug-file**

## Command Parameters

{slot[-slot][...]}

Displays debug files for the slot that you select. If you do not select a slot number, the device displays all types of the archived debug files present in a slot by slot basis. If you select a slot number, the device only displays archived files for the slot you select.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show debug-file** command displays the following information:

Output field	Description
Directory	Specifies a directory name in /intflash/<file>.
File	Specifies the file name of each dir.
Size	Specifies the sizes of each directory.
Created	Specifies when the directory was created.

## Example

The following example displays the debug files information on the switch.

```
Switch:1> show debug-file

=====
                          Core Files
=====
Directory: /intflash/coreFiles/1
1. File: core.logServer.20120611084204.1.tar
   Size: 60928 bytes
   Created: Mon Jun 11 08:42:04 2012
2. File: core.trcServer.20120611084213.1.tar
   Size: 60928 bytes
   Created: Mon Jun 11 08:42:13 2012
3. File: core.logServer.20120611164647.1.tar
   Size: 64000 bytes
   Created: Mon Jun 11 16:46:48 2012
4. File: core.trcServer.20120611164652.1.tar
   Size: 64000 bytes
   Created: Mon Jun 11 16:46:52 2012
5. File: core.dbgServer.20120611164700.1.tar
   Size: 64000 bytes
   Created: Mon Jun 11 16:47:01 2012
6. File: core.logServer.20120611164740.1.tar
   Size: 64000 bytes
   Created: Mon Jun 11 16:47:41 2012

Remote CP Directory: /intflash/coreFiles/2
1. File: core.coreManager.x.20120612085548.2.tar
   Size: 1162240 bytes
   Created: Tue Jun 12 08:55:49 2012
2. File: core.coreManager.x.20120612085602.2.tar
   Size: 478208 bytes
   Created: Tue Jun 12 08:56:02 2012
3. File: core.coreManager.x.20120612085553.2.tar
   Size: 1170432 bytes
   Created: Tue Jun 12 08:55:56 2012
4. File: core.coreManager.x.20120612085558.2.tar
   Size: 1883136 bytes
   Created: Tue Jun 12 08:56:00 2012

=====
                          Archive Files
=====
Directory: /intflash/archive/1
1. File: archive.20120611083021.1.tar
   Size: 34296320 bytes
   Created: Mon Jun 11 08:30:22 2012
2. File: archive.20120611163454.1.tar
   Size: 31108096 bytes
   Created: Mon Jun 11 16:34:54 2012

Remote CP Directory: /intflash//archive/2
1. File: archive.20120611163507.2.tar
   Size: 30903296 bytes
   Created: Mon Jun 11 16:35:08 2012
2. File: archive.20120611164408.2.tar
   Size: 31314432 bytes
   Created: Mon Jun 11 16:44:09 2012

Directory: /intflash/archive/4
1. File: archive.20120611163515.4.tar
```

```

Size: 4725760 bytes
Created: Mon Jun 11 16:35:18 2012
2. File: archive.20120611164416.4.tar
Size: 5639168 bytes
Created: Mon Jun 11 16:44:20 2012

Directory: /intflash/archive/SF4
1. File: archive.20120611163536.SF4.tar
Size: 1550336 bytes
Created: Mon Jun 11 16:35:40 2012
2. File: archive.20120611164436.SF4.tar
Size: 1781248 bytes
Created: Mon Jun 11 16:44:39 2012

```

```

=====
                          PMEM Files
=====

```

```

Directory: /intflash/PMEM/4
1. File: pmem.20120607194023.4.bin.gz
Size: 571048 bytes
Created: Thu Jun 7 19:40:23 2012

```

```

=====
                          DMalloc Files
=====

```

```

=====
                          Flrec Files
=====

```

```

=====
                          WdStats Files
=====

```

```

Directory: /intflash/wd_stats/4
1. File: wd_stats.log.backup
Size: 2311 bytes
Created: Mon Jun 11 09:25:07 2012

```

## show dvr

Displays a summary of the DvR configuration on a DvR Controller or a DvR Leaf.

### Syntax

- **show dvr**

### Command Parameters

**none**

Displays a summary of the DvR configuration on a DvR Controller or a DvR Leaf.

### Default

none

## Command Mode

User EXEC

## Command Output

The **show dvr** command displays the following information on a Controller:

Output field	Description
Domain ID	Specifies the domain ID of the DvR domain to which the Controller belongs.
Domain I-SID	Specifies the DvR domain I-SID. The range is 16678217 to 16678727.
Backbone I-SID	Specifies the backbone I-SID. The value is 16678216.
Role	Specifies the role of the node in the DvR domain, namely Controller.
My SYS ID	Specifies the MAC address of the Controller.
Operational State	Specifies the operational state of the Controller.
GW MAC	Specifies the gateway MAC address.
InjectDefaultRouteDisable	Specifies whether injection of default routes is disabled on the Controller. The default is disabled.

The **show dvr** command displays the following information on a Leaf node:

Output field	Description
Domain ID	Specifies the domain ID of the DvR domain to which the Leaf node belongs.
Domain I-SID	Specifies the DvR domain I-SID. The range is 16678217 to 16678727.
Role	Specifies the role of the node in the DvR domain, namely Leaf.
My SYS ID	Specifies the MAC address of the Leaf node.
Operational State	Specifies the operational state of the Leaf node.
GW MAC	Specifies the gateway MAC address.
Inband Mgmt Clip IP	Specifies the in-band management CLIP IP address.
Virtual Ist local address	Specifies the local IP address of the node, if vIST is configured.
Virtual Ist local subnet mask	Specifies the subnet mask of the local IP address of the node, if vIST is configured.
Virtual Ist peer address	Specifies the IP address of the peer node, in the vIST pair.
Virtual Ist cluster-id	Specifies the cluster ID if vIST is configured.
Virtual Ist ISID	Specifies the I-SID if vIST is configured.

## show dvr backbone-entries

Displays the DvR backbone entries.

### Syntax

- **show dvr backbone-entries**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show dvr backbone-entries** command displays the following information:

Output field	Description
IP-ADDRESS	Specifies the IPv4 address of the DvR backbone host.
HOST MAC-ADDRESS	Specifies the MAC address of DvR backbone host.
L3VSN ISID	Specifies the Layer 3 VSN I-SID of the DvR backbone host.
L2VSN ISID	Specifies the Layer 2 VSN I-SID of the DvR backbone host.
DOMAIN ID	Specifies the domain ID of the DvR backbone host.
ADV-CONTROLLER	Specifies the host name of the advertising Controller.
NEXT HOP	Specifies the MAC address of the next hop backbone host in the DvR route.

## show dvr backbone-entries adv-controller

Displays the DvR backbone entries for a specific advertising controller.

### Syntax

- **show dvr backbone-entries adv-controller WORD<1-255>**
- **show dvr backbone-entries adv-controller WORD<1-255> domain-id <1-255>**
- **show dvr backbone-entries adv-controller WORD<1-255> domain-id <1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00**
- **show dvr backbone-entries adv-controller WORD<1-255> domain-id <1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D}**

- `show dvr backbone-entries adv-controller WORD<1-255> domain-id <1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> domain-id <1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> domain-id <1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255>`
- `show dvr backbone-entries adv-controller WORD<1-255> domain-id <1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries adv-controller WORD<1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00`
- `show dvr backbone-entries adv-controller WORD<1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D}`
- `show dvr backbone-entries adv-controller WORD<1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255>`
- `show dvr backbone-entries adv-controller WORD<1-255> host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries adv-controller WORD<1-255> ipv4 {A.B.C.D}`
- `show dvr backbone-entries adv-controller WORD<1-255> ipv4 {A.B.C.D} l2isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255>`
- `show dvr backbone-entries adv-controller WORD<1-255> ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries adv-controller WORD<1-255> l2isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> l2isid <1-16777215> l3isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255>`
- `show dvr backbone-entries adv-controller WORD<1-255> l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac`

- `show dvr backbone-entries adv-controller WORD<1-255> l3isid <1-16777215>`
- `show dvr backbone-entries adv-controller WORD<1-255> l3isid <1-16777215> next-hop WORD<1-255>`
- `show dvr backbone-entries adv-controller WORD<1-255> l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries adv-controller WORD<1-255> next-hop WORD<1-255>`
- `show dvr backbone-entries adv-controller WORD<1-255> next-hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries adv-controller WORD<1-255> nh-as-mac`

## Command Parameters

`domain-id <1-255>`

Specifies the domain ID for advertising controller.

`host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00`

Specifies the host MAC address for advertising controller.

`ipv4 {A.B.C.D}`

Specifies the IPv4 address for advertising controller.

`l2isid <1-16777215>`

Specifies the Layer 2 I-SID for advertising controller.

`l3isid <1-16777215>`

Specifies the Layer 3 I-SID for advertising controller.

`next-hop WORD<1-255>`

Specifies the next hop node for advertising controller.

`nh-as-mac`

Specifies the next hop node with specific MAC address for advertising controller.

`WORD<1-255>`

Specifies the advertising controller.

## Default

None

## Command Mode

User EXEC

## show dvr backbone-entries domain-id

Displays the DvR backbone entries for a specific domain ID.

## Syntax

- `show dvr backbone-entries domain-id<1-255>`
- `show dvr backbone-entries domain-id<1-255> host-mac-address  
0x00:0x00:0x00:0x00:0x00:0x00`
- `show dvr backbone-entries domain-id<1-255> host-mac-address  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D}`
- `show dvr backbone-entries domain-id<1-255> host-mac-address  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>`
- `show dvr backbone-entries domain-id<1-255> host-mac-address  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>  
l3isid <1-16777215>`
- `show dvr backbone-entries domain-id<1-255> host-mac-address  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>  
l3isid <1-16777215> next-hop WORD<1-255>`
- `show dvr backbone-entries domain-id<1-255> host-mac-address  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>  
l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries domain-id<1-255> ipv4 {A.B.C.D}`
- `show dvr backbone-entries domain-id<1-255> ipv4 {A.B.C.D} l2isid  
<1-16777215>`
- `show dvr backbone-entries domain-id<1-255> ipv4 {A.B.C.D} l2isid  
<1-16777215> l3isid <1-16777215>`
- `show dvr backbone-entries domain-id<1-255> ipv4 {A.B.C.D} l2isid  
<1-16777215> l3isid <1-16777215> next-hop WORD<1-255>`
- `show dvr backbone-entries domain-id<1-255> ipv4 {A.B.C.D} l2isid  
<1-16777215> l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries domain-id<1-255> l2isid <1-16777215>`
- `show dvr backbone-entries domain-id<1-255> l2isid <1-16777215> l3isid  
<1-16777215>`
- `show dvr backbone-entries domain-id<1-255> l2isid <1-16777215> l3isid  
<1-16777215>`
- `show dvr backbone-entries domain-id<1-255> l2isid <1-16777215> l3isid  
<1-16777215> next-hop WORD<1-255>`
- `show dvr backbone-entries domain-id<1-255> l2isid <1-16777215> l3isid  
<1-16777215> next-hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries domain-id<1-255> l3isid <1-16777215>`
- `show dvr backbone-entries domain-id<1-255> l3isid <1-16777215> next-  
hop WORD<1-255>`
- `show dvr backbone-entries domain-id<1-255> l3isid <1-16777215> next-  
hop WORD<1-255> nh-as-mac`
- `show dvr backbone-entries domain-id<1-255> next-hop WORD<1-255>`



- **show dvr backbone-entries domain-id<1-255> next-hop WORD<1-255> nh-as-mac**
- **show dvr backbone-entries domain-id<1-255> nh-as-mac**

## Command Parameters

**<1-255>**

Specifies the domain ID.

**host-mac-address 0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the host MAC address for domain ID.

**ipv4 {A.B.C.D}**

Specifies the IPv4 address for domain ID.

**l2isid <1-16777215>**

Specifies the Layer 2 I-SID for domain ID.

**l3isid <1-16777215>**

Specifies the Layer 3 I-SID for domain ID.

**next-hop WORD<1-255>**

Specifies the next hop node for domain ID.

**nh-as-mac**

Specifies the next hop node with specific MAC address for domain ID.

## Default

None

## Command Mode

User EXEC

## show dvr backbone-entries home

---

Display the Distributed Virtual Routing (DvR) backbone entries for the home area.

## Syntax

- **show dvr backbone-entries home**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show dvr backbone-entries home** command displays the following information:

Output field	Description
IP-ADDRESS	Specifies the IPv4 address of the DvR backbone host in home area.
HOST MAC-ADDRESS	Specifies the MAC address of DvR backbone host in home area.
L3VSN ISID	Specifies the Layer 3 VSN I-SID of the DvR backbone host in home area.
L2VSN ISID	Specifies the Layer 2 VSN I-SID of the DvR backbone host in home area.
DOMAIN ID	Specifies the domain ID of the DvR backbone host in home area.
ADV-CONTROLLER	Specifies the host name of the advertising Controller in home area.
NEXT HOP	Specifies the MAC address of the next hop backbone host in the DvR route.
AREA	Specifies the area as home or remote.
AREA-NAME	Specifies the name of the area.

## Example

Displaying the DvR backbone entries for the home area.

```
Switch:1>show dvr backbone-entries home
=====
DVR Backbone-Entries
=====
IP-ADDRESS      HOST          L3VSN  L2VSN  DOMAIN  ADV-CONTROLLER  NEXT HOP  AREA  AREA-NAME
MAC-ADDRESS     ISID   ISID   ID
-----
192.0.2.11      00:19:01:00:00:01  0      551101  9999    area-0.00.70    area-0.00.70  HOME  area-0.00.20
192.0.2.12      00:19:01:00:00:02  0      551101  9999    area-0.00.70    area-0.00.70  HOME  area-0.00.20
192.0.2.13      00:19:01:00:00:03  0      551101  9999    area-0.00.70    area-0.00.70  HOME  area-0.00.20
192.0.2.14      00:19:01:00:00:04  0      551101  9999    area-0.00.70    area-0.00.70  HOME  area-0.00.20
192.0.2.15      00:19:01:00:00:05  0      551101  9999    area-0.00.70    area-0.00.70  HOME  area-0.00.20

Home:    5 out of 5 Total Num of DVR Backbone Routes displayed
=====
```

## show dvr backbone-entries host-mac-address

Displays the DvR backbone entries for a specific host MAC address.

## Syntax

- **show dvr backbone-entries host-mac-address**  
**0x00:0x00:0x00:0x00:0x00:0x00**
- **show dvr backbone-entries host-mac-address**  
**0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D}**

- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>  
l3isid <1-16777215>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>  
l3isid <1-16777215>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>  
l3isid <1-16777215> next-hop WORD<1-255>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 ipv4 {A.B.C.D} l2isid <1-16777215>  
l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 l2isid <1-16777215>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 l2isid <1-16777215> l3isid <1-16777215>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 l2isid <1-16777215> l3isid <1-16777215>  
next-hop WORD<1-255>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 l2isid <1-16777215> l3isid <1-16777215>  
next-hop WORD<1-255> nh-as-mac
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 l3isid <1-16777215>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 l3isid <1-16777215> next-hop WORD<1-255>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 l3isid <1-16777215> next-hop WORD<1-255>  
nh-as-mac
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 next-hop WORD<1-255>
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 next-hop WORD<1-255> nh-as-mac
- `show dvr backbone-entries host-mac-address`  
0x00:0x00:0x00:0x00:0x00:0x00 nh-as-mac

## Command Parameters

0x00:0x00:0x00:0x00:0x00:0x00

Specifies the host MAC address.

ipv4 {A.B.C.D}

Specifies the IPv4 address for host MAC address.

**l2isid <1-16777215>**

Specifies the Layer 2 I-SID for host MAC address.

**l3isid <1-16777215>**

Specifies the Layer 3 I-SID for host MAC address.

**next-hop WORD<1-255>**

Specifies the next hop node for host MAC address.

**nh-as-mac**

Specifies the next hop node with specific MAC address for host MAC address.

## Default

None

## Command Mode

User EXEC

## show dvr backbone-entries ipv4

---

Displays the DvR backbone entries for a specific IPv4 address.

## Syntax

- **show dvr backbone-entries ipv4 {A.B.C.D}**
- **show dvr backbone-entries ipv4 {A.B.C.D} l2isid <1-16777215>**
- **show dvr backbone-entries ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215>**
- **show dvr backbone-entries ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255>**
- **show dvr backbone-entries ipv4 {A.B.C.D} l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac**
- **show dvr backbone-entries ipv4 {A.B.C.D} l3isid <1-16777215>**
- **show dvr backbone-entries ipv4 {A.B.C.D} l3isid <1-16777215> next-hop WORD<1-255>**
- **show dvr backbone-entries ipv4 {A.B.C.D} l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac**
- **show dvr backbone-entries ipv4 {A.B.C.D} next-hop WORD<1-255>**
- **show dvr backbone-entries ipv4 {A.B.C.D} next-hop WORD<1-255> nh-as-mac**
- **show dvr backbone-entries ipv4 {A.B.C.D} nh-as-mac**

## Command Parameters

**{A.B.C.D}**

Specifies the IPv4 address.

**l2isid <1-16777215>**

Specifies the Layer 2 I-SID for IPv4 address.

**l3isid <1-16777215>**

Specifies the Layer 3 I-SID for IPv4 address.

**next-hop WORD<1-255>**

Specifies the next hop node for IPv4 address.

**nh-as-mac**

Specifies the next hop node with specific MAC address for IPv4 address.

## Default

None

## Command Mode

User EXEC

## show dvr backbone-entries l2isid

---

Displays the DvR backbone entries for a specific Layer 2 I-SID.

## Syntax

- **show dvr backbone-entries l2isid <1-16777215>**
- **show dvr backbone-entries l2isid <1-16777215> l3isid <1-16777215>**
- **show dvr backbone-entries l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255>**
- **show dvr backbone-entries l2isid <1-16777215> l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac**
- **show dvr backbone-entries l2isid <1-16777215> next-hop WORD<1-255>**
- **show dvr backbone-entries l2isid <1-16777215> next-hop WORD<1-255> nh-as-mac**
- **show dvr backbone-entries l2isid <1-16777215> nh-as-mac**

## Command Parameters

**<1-16777215>**

Specifies the Layer 2 I-SID.

**l3isid <1-16777215>**

Specifies the Layer 3 I-SID for Layer 2 I-SID.

**next-hop WORD<1-255>**

Specifies the next hop node for Layer 2 I-SID.

**nh-as-mac**

Specifies the next hop node with specific MAC address for Layer 2 I-SID.

## Default

None

## Command Mode

User EXEC

## show dvr backbone-entries l3isid

---

Displays the DvR backbone entries for a specific Layer 3 I-SID.

## Syntax

- **show dvr backbone-entries l3isid <1-16777215>**
- **show dvr backbone-entries l3isid <1-16777215> next-hop WORD<1-255>**
- **show dvr backbone-entries l3isid <1-16777215> next-hop WORD<1-255> nh-as-mac**
- **show dvr backbone-entries l3isid <1-16777215> nh-as-mac**

## Command Parameters

**<1-16777215>**

Specifies the Layer 3 I-SID.

**next-hop WORD<1-255>**

Specifies the next hop node for Layer 3 I-SID.

**nh-as-mac**

Specifies the next hop node with specific MAC address for Layer 3 I-SID.

## Default

None

## Command Mode

User EXEC

## show dvr backbone-entries next-hop

---

Displays the DvR backbone entries for a specific next hop node.

## Syntax

- **show dvr backbone-entries next-hop WORD<1-255>**
- **show dvr backbone-entries next-hop WORD<1-255> nh-as-mac**

## Command Parameters

**nh-as-mac**

Specifies the next hop node with specific MAC address for next-hop.

**WORD<1-255>**

Specifies the next hop node.

## Default

None

## Command Mode

User EXEC

## show dvr backbone-entries nh-as-mac

---

Displays the DvR backbone entries for a specific next hop node with a specific MAC address.

## Syntax

- **show dvr backbone-entries nh-as-mac**

## Default

None

## Command Mode

User EXEC

## show dvr backbone-entries remote

---

Display the Distributed Virtual Routing (DvR) backbone entries for the remote area.

## Syntax

- **show dvr backbone-entries remote**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show dvr backbone-entries remote** command displays the following information:

Output field	Description
IP-ADDRESS	Specifies the IPv4 address of the DvR backbone host in remote area.
HOST MAC-ADDRESS	Specifies the MAC address of DvR backbone host in remote area.
L3VSN ISID	Specifies the Layer 3 VSN I-SID of the DvR backbone host in remote area.
L2VSN ISID	Specifies the Layer 2 VSN I-SID of the DvR backbone host in remote area.
DOMAIN ID	Specifies the domain ID of the DvR backbone host in remote area.
ADV-CONTROLLER	Specifies the host name of the advertising Controller in remote area.
NEXT HOP	Specifies the MAC address of the next hop backbone host in the DvR route.
AREA	Specifies the area as home or remote.
AREA-NAME	Specifies the name of the area.

## Example

Displaying the DvR backbone entries for the home area.

```
Switch:1>show dvr backbone-entries home
=====
                        DVR Backbone-Entries
=====
IP-ADDRESS      HOST          L3VSN  L2VSN  DOMAIN  ADV-CONTROLLER  NEXT HOP  AREA  AREA-NAME
MAC-ADDRESS     ISID   ISID   ID
-----
192.0.2.10      00:19:01:00:00:01  0      551101  9999    area-0.00.90    area-0.00.90  REMOTE  area-0.00.30
192.0.2.20      00:19:01:00:00:02  0      551101  9999    area-0.00.90    area-0.00.90  REMOTE  area-0.00.30
192.0.2.30      00:19:01:00:00:03  0      551101  9999    area-0.00.90    area-0.00.90  REMOTE  area-0.00.30
192.0.2.40      00:19:01:00:00:04  0      551101  9999    area-0.00.90    area-0.00.90  REMOTE  area-0.00.30
192.0.2.50      00:19:01:00:00:05  0      551101  9999    area-0.00.90    area-0.00.90  REMOTE  area-0.00.30

Home:    5 out of 5 Total Num of DVR Backbone Routes displayed
=====
```

## show dvr backbone-members

Display information about the Distributed Virtual Routing (DvR) backbone members. DvR backbone members are either DvR Controllers or non-DvR BEBs that receive redistributed host routes from all other DvR Controllers in the SPB network.



## Syntax

- **show dvr backbone-members**
- **show dvr backbone-members controller**
- **show dvr backbone-members home**
- **show dvr backbone-members non-dvr-beb**
- **show dvr backbone-members remote**

## Command Parameters

### controller

Displays information about DvR backbone members that are Controllers.

### home

Displays information about DvR backbone members in the home area.

### non-dvr-beb

Displays information about DvR backbone members that are non-DvR BEBs.

### none

Displays information about the DvR backbone members. DvR backbone members are either DvR Controllers or non-DvR BEBs that receive redistributed host routes from all other DvR Controllers in the SPB network.

### remote

Displays information about DvR backbone members in the remote area.

## Default

none

## Command Mode

User EXEC

## Command Output

The **show dvr backbone-members** command displays the following information:

Output field	Description
System Name	Specifies the system name of the DvR backbone member.
Nick-Name	Specifies the nick name of the DvR backbone member.
Nodal MAC	Specifies the nodal MAC address of the DvR backbone member.
Role	Specifies the role of the DvR backbone member.
Domain Id	Specifies the domain ID of the backbone member.

Output field	Description
Area	Specifies the area as home or remote.
Area-Name	Specifies the name of the area.

## Example

Display information about the DvR backbone members.

```
Switch:1>show isis multi-area dvr redistribute
=====
DVR BB Members
=====
System Name      Nick-Name      Nodal MAC      Role      Domain Id  Area      Area-Name
-----
area-0.00.30    0.00.30      02:00:30:ff:ff:f0  Controller  9999      HOME      area-0.00.20
area-0.00.70    0.00.70      02:00:70:ff:ff:f0  Controller  9999      HOME      area-0.00.20
area-0.00.80    0.00.80      02:00:80:ff:ff:f0  Controller  9999      HOME      area-0.00.20
area-0.00.20    0.00.20      02:00:20:ff:ff:f0  Controller  9999      REMOTE    area-0.00.30
area-0.00.30    0.60.20      b0:ad:aa:42:dc:84  Controller  30        REMOTE    area-0.00.30

Home:   3 out of 3 Total Num of DVR Backbone Members displayed
Remote: 2 out of 2 Total Num of DVR Backbone Members displayed
=====
```

## show dvr database

Display Distributed Virtual Routing (DvR) database information.

## Syntax

- **show dvr database home**
- **show dvr database ipv4 {A.B.C.D}**
- **show dvr database l3isid <1-16777215>**
- **show dvr database nh-as-mac type <1-2>**
- **show dvr database remote**
- **show dvr database vrf WORD <1-16>**
- **show dvr database vrfids WORD<0-512>**

## Command Parameters

### home

Displays database entries in the home area.

### ipv4 {A.B.C.D}

Displays database entries for a specific net.

### l3isid <1-16777215>

Displays database entries for a particular Layer 3 I-SID.

### nh-as-mac

Displays database entries next hop as mac.

### remote

Displays database entries in the remote area.

**vrf** WORD <1-16>

Specifies a VRF instance by name.

**vrfids** WORD<0-512>

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show dvr database** command displays the following information:

Output field	Description
DEST	Specifies the address type of the IPv4 destination address of the DvR database entry.
MASK	Specifies the destination mask of the DvR database entry.
NEXT HOP	Specifies the MAC address of the next hop BEB, in the DvR database entry.
VRFID	Specifies the VRF ID for the database entry.
L3VSN ISID	Specifies the Layer 3 VSN I-SID of the DvR database entry.
L2VSN ISID	Specifies the Layer 2 VSN I-SID of the DvR database entry.
OUTGOING INTERFACE	Specifies the outgoing interface (port or MLT) of the DvR database entry.
SPB COST	Specifies the SPB cost of the DvR database entry.
PREFIX COST	Specifies the prefix cost of the DvR database entry.
AGE	Specifies the uptime since creation of the DvR database table entry.

## show dvr host-entries

Display DvR host-entries information.

## Syntax

- **show dvr host-entries domain-id <1-255>**
- **show dvr host-entries ipv4 {A.B.C.D}**

- **show dvr host-entries l2isid <1-16777215>**
- **show dvr host-entries l3isid <1-16777215>**
- **show dvr host-entries nh-as-mac type <1-2>**
- **show dvr host-entries type <1-2>**
- **show dvr host-entries vrf WORD <1-16>**
- **show dvr host-entries vrfids WORD<0-512>**

## Command Parameters

**domain-id <1-255>**

Displays host entries for a particular domain-id.

**ipv4 {A.B.C.D}**

Displays host entries for a specific net.

**l2isid <1-16777215>**

Displays host entries for a particular l2isid.

**l3isid <1-16777215>**

Displays host entries for a particular l3isid.

**nh-as-mac**

Displays host entries next hop as mac.

**type <1-2>**

Displays host entries for a particular type - 1= local, 2 = dynamic.

**vrf WORD <1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show dvr host-entries** command displays the following information:

Output field	Description
IP-ADDRESS	Specifies the IP address of the DvR host entry (IPv4 remote ARP).
HOST MAC-ADDRESS	Specifies the MAC address of the DvR host entry (IPv4 remote ARP).
L3VSN ISID	Specifies the Layer 3 VSN I-SID of the DvR host entry.
VRFID	Specifies the VRF ID of the DvR host entry.
L2VSN ISID	Specifies the Layer 2 VSN I-SID of the DvR host entry.
PORT	Specifies the port of the DvR host entry.
DOMAIN ID	Specifies the DvR domain ID of the DvR host entry.
TYPE	Specifies the host type of the DvR host entry.
NEXT HOP	Specifies the next hop system MAC address of the DvR host entry.

## show dvr interfaces

Displays the DvR interfaces on either a Controller or a Leaf node. On Controllers, DvR interfaces are created when you configure IP on a DvR enabled Layer 2 VSN (VLAN, I-SID). Only Controllers display the administrative state of the interfaces because this is where you enable or disable the interfaces. The Leaf nodes display DvR interface information that is pushed from the Controllers, for example, subnet routes or gateway IP addresses for the Layer 2 VSNs.

## Syntax

- **show dvr interfaces**
- **show dvr interfaces l3isid <0-16777215>**
- **show dvr interfaces vrf WORD<1-16>**
- **show dvr interfaces vrfids WORD<0-512>**

## Command Parameters

**l3isid <0-16777215>**

Displays the DvR interfaces for the specified Layer 3 I-SID.

**none**

Displays the DvR interfaces on either a Controller or a Leaf node. On Controllers, DvR interfaces are created when you configure IP on a DvR enabled Layer 2 VSN (VLAN, I-SID). Only Controllers display the administrative state of the interfaces because this is where you enable or disable the interfaces. The Leaf nodes display DvR interface information that is pushed from the Controllers, for example, subnet routes or gateway IP addresses for the Layer 2 VSNs.

**vrf WORD<1-16>**

Displays the DvR interfaces for a specific VRF whose name is specified.

**vrfids WORD<0-512>**

Displays the DvR interfaces for a specific VRF whose VRF ID is specified.

## Default

none

## Command Mode

User EXEC

## Command Output

The **show dvr interfaces** command displays the following information:

Output field	Description
Interface	Specifies the VLAN IP address (IPv4) of the DvR interface.
Mask	Specifies the subnet mask of the VLAN IP address.
L3ISID	Specifies the Layer 3 I-SID of the DvR interface. The range is 0 to 16777215.
VRFID	Specifies the VRF ID of the DvR interface
L2ISID	Specifies the Layer 2 I-SID of the DvR interface. The range is 1 to 16777215.
VLAN	Specifies the VLAN ID of the DvR interface.
GW IPv4	Specifies the DvR gateway IP address (IPv4).
Admin State	Specifies the administrative state of the DvR interface.  <b>Note:</b> This field displays only on a Controller node.
SPBMC State	Specifies the SBPMC state of the DvR interface.
IGMP version	Specifies the version of IGMP running on the DvR interface.

## show dvr l3vsn

Displays VRFs corresponding to Layer 3 (routed) VSN I-SIDs on either a Controller or a Leaf node.

## Syntax

- **show dvr l3vsn**
- **show dvr l3vsn l3isid <0-16777215>**
- **show dvr l3vsn l3isid <0-16777215> nh-as-mac**

- **show dvr l3vsn vrf WORD<1-16>**
- **show dvr l3vsn vrfids WORD<0-512>**

## Command Parameters

**l3isid <0-16777215>**

Displays the Layer 3 VSN information for the specified Layer 3 I-SID.

**none**

Displays the Layer 3 VSN information on either a Controller or a Leaf node.

**vrf WORD<1-16>**

Displays the Layer 3 VSN information for a specific VRF whose name is specified.

**vrfids WORD<0-512>**

Displays the Layer 3 VSN information for a specific VRF whose VRF ID is specified.

## Default

none

## Command Mode

User EXEC

## Command Output

The **show dvr l3vsn** command displays the following information on a Controller:

Output field	Description
VRF ID	Specifies the VRF ID of the VRF corresponding to the Layer 3 VSN I-SID.
L3VSN ISID	Specifies the Layer 3 VSN I-SID.
VRF NAME	Specifies the VRF name of the VRF corresponding to the Layer 3 VSN I-SID.
INJECT-DEFAULT-ROUTE-DISABLE	Specifies whether injection of default routes is disabled.

The **show dvr l3vsn** command displays the following information on a Leaf node:

Output field	Description
VRF ID	Specifies the VRF ID of the VRF corresponding to the Layer 3 VSN I-SID.
L3VSN ISID	Specifies the Layer 3 VSN I-SID.
VRF NAME	Specifies the VRF name of the VRF corresponding to the Layer 3 VSN I-SID.

## show dvr members

Displays the members of all DvR domains, namely the Controllers and Leaf nodes. You can view this information on either a Controller or a Leaf node. Both the Controller and the Leaf node displays those members of the DvR domain to which it belongs.

### Syntax

- **show dvr members**
- **show dvr members controller**
- **show dvr members leaf**

### Command Parameters

#### controller

Displays the members of the DvR domain that the specified Controller is a part of.

#### leaf

Displays the members of the DvR domain that the specified Leaf is a part of.

#### none

Displays the members of all DvR domains, namely the Controllers and Leaf nodes. You can view this information on either a Controller or a Leaf node. Both the Controller and the Leaf node displays those members of the DvR domain to which it belongs.

### Default

none

### Command Mode

User EXEC

### Command Output

The **show dvr members** command displays the following information:

Output field	Description
System Name	Specifies the system name of the DvR member (Controller or Leaf node).
Nick-Name	Specifies the nick name of the DvR member.
Nodal MAC	Specifies the nodal MAC address of the DvR member.
Role	Specifies the role of the DvR member within the DvR domain, that is Controller or Leaf.



## show dvr redistribute

Displays the DvR domain redistribution information on a Controller or a Leaf node.

### Syntax

- **show dvr redistribute**
- **show dvr redistribute vrf WORD<1-16>**
- **show dvr redistribute vrfids WORD<0-512>**

### Command Parameters

#### none

Displays the DvR domain redistribution information on a Controller or a Leaf node.

#### vrf WORD<1-16>

Displays the DvR domain redistribution information for a VRF whose name is specified.

#### vrfids WORD<0-512>

Displays the DvR domain redistribution information for a VRF whose VRF ID is specified.

### Default

none

### Command Mode

User EXEC

### Command Output

The **show dvr redistribute** command displays the following information:

Output field	Description
SOURCE	Specifies the source of the DvR route redistribution.
MET	Specifies the DvR route redistribution metric. The range is 0 to 65535.
MTYPE	Specifies the DvR route redistribution metric type.
ENABLE	Specifies whether DvR route redistribution is enabled on the VRF instance.
RPOLICY	Specifies the route policy for DvR route redistribution.

## show dvr routes

Display dvr routes information.

## Syntax

- **show dvr routes ipv4 {A.B.C.D}**
- **show dvr routes l3isid <1-16777215>**
- **show dvr routes nh-as-mac type <1-2>**
- **show dvr routes vrf WORD <1-16>**
- **show dvr routes vrfids WORD<0-512>**

## Command Parameters

**ipv4 {A.B.C.D}**

Displays routes for a specific net.

**l3isid <1-16777215>**

Displays routes for a particular l3isid.

**nh-as-mac**

Displays routes next hop as mac.

**vrf WORD <1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show dvr routes** command displays the following information:

Output field	Description
DEST	Specifies the IPv4 destination address of the DvR route.
MASK	Specifies the subnet mask of the IPv4 destination address of the DvR route.
NEXT HOP	Specifies the host name of the next hop BEB, in the DvR route.
VRFID	Specifies the VRF ID of the DvR route.
L3VSN ISID	Specifies the Layer 3 VSN I-SID of the DvR route.
L2VSN ISID	Specifies the Layer 2 VSN I-SID of the DvR route.

Output field	Description
TYPE	Specifies the route type of the DvR route.
COST	Specifies the SPB cost of the DvR route.

## show eapol auth-diags interface

Display the Extensible Authentication Protocol (EAPoL) Authenticator diagnostics to manage network performance.

### Syntax

- **show eapol auth-diags interface**
- **show eapol auth-diags interface gigabitethernet**
- **show eapol auth-diags interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **show eapol auth-diags interface vlan <1-4059>**
- **show eapol auth-diags interface vlan <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**

### Command Parameters

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

User EXEC

## show eapol auth-stats interface

Display the Authenticator statistics to manage network performance.

## Syntax

- **show eapol auth-stats interface**
- **show eapol auth-stats interface gigabitEthernet**
- **show eapol auth-stats interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **show eapol auth-stats interface vlan <1-4059>**
- **show eapol auth-stats interface vlan <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**

## Command Parameters

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show eapol auth-stats interface** command displays the following information:

Output field	Description
PORT	Displays the port number in use.
EAP RCVD	Displays the number of EAPoL-EAP frames received by this Authenticator.
AUTH-EAP TX	Displays the number of EAPoL-EAP frames transmitted by the Authenticator.
START RCVD	Displays the number of EAPoL start frames received by this Authenticator.

Output field	Description
LOGOFF RCVD	Displays the number of EAPoL logoff frames received by this Authenticator.
INVALID FRAMES	Displays the number of EAPoL frames received by this Authenticator in which the frame type is not recognized.
LENGTH ERROR	Displays the number of EAPoL frames received by this Authenticator in which the Packet Body Length field is invalid.
LAST-RX VER	Displays the last received version of the EAPoL frame by this Authenticator.
LAST-RX SRC	Displays the source MAC address of the last received EAPoL frame by this Authenticator.

## show eapol multihost non-eap-mac status

Display non-EAP client MAC information on a port.

### Syntax

- **show eapol multihost non-eap-mac status**
- **show eapol multihost non-eap-mac status vlan <1-4059>**
- **show eapol multihost non-eap-mac status verbose**
- **show eapol multihost non-eap-mac status vlan <1-4059> verbose**
- **show eapol multihost non-eap-mac status vlan <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show eapol multihost non-eap-mac status vlan <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} verbose**

### Command Parameters

**{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**verbose**

Displays non-EAPoL client MAC information.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## Command Output

The **show eapol multihost non-eap-mac status** command displays the following information:

Output field	Description
PORT NUM	Displays the port number in use.
MAC	Displays the MAC address of the client.
STATE	Indicates the authentication status of the non EAP host that is authenticated using radius server.
VLAN ID	Indicates the VLAN assigned to the client.

## show eapol port

Display Extensible Authentication Protocol (EAPoL) information for the specified port or interface type.

## Syntax

- **show eapol port {slot/port[sub-port]}**
- **show eapol port interface gigabitEthernet**
- **show eapol port interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show eapol port interface vlan <1-4059>**
- **show eapol port interface <1-4059> [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**{slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show eapol sessions

Display Extensible Authentication Protocol (EAPoL) and non-Extensible Authentication Protocol (NEAP) authentication sessions on the switch.

## Syntax

- **show eapol sessions eap verbose**
- **show eapol sessions eap vlan <1-4059>**
- **show eapol sessions eap {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show eapol sessions neap verbose**
- **show eapol sessions neap vlan <1-4059>**
- **show eapol sessions neap {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**verbose**

Displays non-EAPoL client MAC information.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show eapol session-stats interface

---

Display the port Extensible Authentication Protocol (EAPoL) authenticator session statistics for the specified interface type.

## Syntax

- **show eapol session-stats interface**
- **show eapol session-stats interface gigabitethernet**
- **show eapol session-stats interface gigabitethernet {slot/port[/sub-port]} [-slot/port[/sub-port]] [, ...]**
- **show eapol session-stats interface vlan <1-4059>**
- **show eapol session-stats interface vlan <1-4059> [{slot/port[/sub-port]} [-slot/port[/sub-port]] [, ...]**

## Command Parameters

**gigabitethernet {slot/port[/sub-port]} [-slot/port[/sub-port]] [, ...]**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**



Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show eapol session-stats interface** command displays the following information:

Output field	Description
PORT NUM	Displays the port number in use.
MAC	Displays the MAC address of the client.
USER NAME	Displays the user name of the Supplicant Authenticator Port Access Entity (PAE).
SESSION ID	Displays a unique identifier for the session.
AUTHENTIC METHOD	Displays the authentication method (remote or local RADIUS server) used to establish the session.
SESSION TIME	Displays the duration of the session (in seconds).
TERMINATE CAUSE	Displays the reason the session terminated.

## show eapol status interface

Display the port Extensible Authentication Protocol (EAPoL) operation statistics for the specified interface type.

## Syntax

- **show eapol status interface**
- **show eapol status interface gigabitEthernet**
- **show eapol status interface vlan <1-4059>**
- **show eapol status interface verbose**
- **show eapol status interface gigabitEthernet {slot/port[/sub-port]} [-slot/port[/sub-port]][,...]**
- **show eapol status interface gigabitEthernet {slot/port[/sub-port]} [-slot/port[/sub-port]][,...] verbose**

- **show eapol status interface vlan <1-4059> verbose**
- **show eapol status interface vlan <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show eapol status interface vlan <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} verbose**

## Command Parameters

**gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**verbose**

Displays non-EAPoL client MAC information.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## Command Output

The **show eapol status interface** command displays the following information:

Output field	Description
PORT NUM	Displays the port number in use.
MAC	Displays the MAC address of the client.
PAE STATUS	Indicates the current state of the authenticator PAE state machine.

Output field	Description
VLAN ID	Indicates the VLAN assigned to the client.
PRI	Indicates port priority.

## show eapol system

Display the current Extensible Authentication Protocol (EAPoL) setting on the switch.

### Syntax

- **show eapol system**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show eapol system** command displays the following information:

Output field	Description
eap	Displays whether system authentication control is enabled. EAP is disabled by default.
Eapol Version	Displays the EAP version on the switch.
non-eap-pwd-fmt	Displays the password attribute format for non EAP RADIUS authentication.
non-eap-pwd-fmt key	Displays the attribute key string for non EAP RADIUS password. The range is 0- 32 characters.
non-eap-pwd-fmt padding	Displays whether the padding option is enabled or disabled.

Output field	Description
auto-isid-offset status  <b>Note:</b> Exception: Not supported on VSP 4450 Series, VSP 8600 Series, or XA1400 Series.	Displays the status of the Auto I-SID Offset feature.
auto-isid-offset value  <b>Note:</b> Exception: Not supported on VSP 4450 Series, VSP 8600 Series, or XA1400 Series.	Displays the Auto I-SID Offset value. The range is 0-15995903.

## Examples

The following examples display the EAPoL settings on the switch.

```
Switch:1>show eapol system
```

```
=====
                        Eapol System
=====
```

```

        eap : enabled
        Eapol Version : 3
        non-eap-pwd-fmt : mac-addr
        non-eap-pwd-fmt key : *****
        non-eap-pwd-fmt padding : disabled
        auto-isid-offset status : disabled
        auto-isid-offset value : 15980000
```

```
Switch:1>show eapol system
```

```
=====
                        Eapol System
=====
```

```

        eap : disabled
        Eapol Version : 3
        non-eap-pwd-fmt : mac-addr
        non-eap-pwd-fmt key : *****
        non-eap-pwd-fmt padding : disabled
        auto-isid-offset status : disabled
        auto-isid-offset value : 1000
=====
```

## show endpoint-tracking

Display the global status of Endpoint Tracking on the switch, and the configured I-SID offset value, if applicable.

### Syntax

- **show endpoint-tracking**

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show endpoint-tracking** command displays the following information:

Output field	Description
endpoint tracking status	Specifies whether Endpoint Tracking is globally enabled or disabled on the switch.
auto-isid-offset value	Specifies the configured I-SID offset value used to calculate an I-SID value for a switched UNI when no I-SID value is provided by the RADIUS server.
auto-isid-offset enabled	Specifies whether the I-SID offset value is globally enabled or disabled on the switch.
visibility-mode status	Specifies whether visibility mode is globally enabled or disabled on the switch.

## Example

The following example displays a switch with Endpoint Tracking globally enabled, and an I-SID offset value configured and enabled.

```
Switch:1>show endpoint-tracking
=====
Endpoint Tracking Configuration
=====

endpoint tracking status : ENABLED
auto-isid-offset value  : 15990000
auto-isid-offset enabled : ENABLED
visibility-mode status   : ENABLED
```

## show endpoint-tracking bindings

Display the Endpoint Tracking VLAN:ISID binding information for the switch, for ports, or for MLT or SMLT interfaces.

## Syntax

- **show endpoint-tracking bindings**
- **show endpoint-tracking bindings gigabitEthernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
- **show endpoint-tracking bindings mlt** <1-512>
- **show endpoint-tracking bindings summary**

## Command Parameters

**gigabitEthernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mlt** <1-512>

Specifies the MLT ID.

**summary**

Provides a summary of the total number and status of bindings for all interfaces.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show endpoint-tracking bindings** command displays the following information:

Output field	Description
PORT/MLT	Specifies the port number or MLT ID.
INDEX	Specifies the interface index of the selected port or MLT.
TOTAL	Specifies the total number of bindings for a port or MLT.
ACCEPTED	Specifies the total number of bindings in Accepted status for a port or MLT.

Output field	Description
REJECTED	Specifies the total number of bindings in Rejected status for a port or MLT.
PENDING	Specifies the total number of bindings in Pending status for a port or MLT.
TIMEOUT	Specifies the total number of bindings in Timeout status for a port or MLT.
SERVER-UNREACHABLE	Specifies the total number of bindings in serverNotConfigured status for a port or MLT.
MAC	Specifies the MAC address that corresponds to the VLAN:ISID binding.
STATUS	Specifies the Endpoint Tracking data binding status as follows: <ul style="list-style-type: none"> <li>pending: indicates that a request has been sent to the RADIUS server</li> <li>accept: indicates that the RADIUS server has successfully returned the request</li> <li>reject: indicates that the RADIUS server has rejected the request</li> <li>timeout: indicates that the RADIUS server request has timed out. The entry is deleted if it remains in this state for 15 minutes.</li> <li>serverNotConfigured: indicates that the RADIUS server is not configured for Endpoint Tracking. The entry is deleted if it remains in this state for 15 minutes.</li> </ul>
VLAN ID	Specifies the VLAN ID.
ISID	Specifies the I-SID value, either provided by the RADIUS server, or calculated using the VLAN ID plus the configured I-SID offset value.
SOURCE	Specifies how the I-SID value is provided, as follows: <ul style="list-style-type: none"> <li>radius: provided by the RADIUS server</li> <li>autoconfig: calculated using the VLAN ID plus the configured endpoint-tracking offset value</li> <li>config: from MAC addresses learned on a static S-UNI</li> </ul>
TIMEOUT	Specifies the timeout period that is applied to the MAC in the bindings table when the MAC is aged out. If the MAC is in timeout state (there is no response from the RADIUS server), the timeout triggers immediately with a 15 minute period. Otherwise, the default timeout is one day, and triggers the moment the MAC ages out from the VLAN/I-SID bridge forwarding database (FDB) table. The default timeout of one day can be overridden by the RADIUS server if the Session-Timeout attribute is configured and returned.
TIME REMAINING	Specifies the time remaining until the Endpoint Tracking data binding entry expires.

## Examples

The following example displays the global data binding information for Endpoint Tracking ports and MLT interfaces on a switch.

```
Switch:1>show endpoint-tracking bindings
```

```

Endpoint Tracking Bindings
=====
PORT/MLT  INDEX  MAC                STATUS  VLAN ID  ISID    SOURCE          TIMEOUT          TIME REMAINING
-----
1/10      201    00:00:00:00:1b:01  accept  27       15990027 autoconfig  0 day(s), 00:01:40  0 day(s), 00:00:00
1/10      201    00:00:00:00:1b:02  accept  27       15990027 autoconfig  0 day(s), 00:01:40  0 day(s), 00:00:00
1/10      201    00:00:00:00:1b:03  accept  27       15990027 autoconfig  0 day(s), 00:01:40  0 day(s), 00:00:00
1/10      201    00:00:00:00:1b:04  accept  27       15990027 autoconfig  0 day(s), 00:01:40  0 day(s), 00:00:00
1/10      201    00:00:00:00:1b:05  accept  27       15990027 autoconfig  0 day(s), 00:01:40  0 day(s), 00:00:00

5 out of 5 Total Num of Endpoint Tracking bindings displayed.

```

The following example displays a summary of the binding information for Endpoint Tracking ports and MLT interfaces on a switch.

```

Switch:1>show endpoint-tracking bindings summary
=====
Endpoint Tracking Bindings
=====
PORT/MLT  INDEX  TOTAL  ACCEPTED  REJECTED  PENDING  TIMEOUT  SERVER-UNREACHABLE
-----
1/10      201    5       5         0         0         0         0

```

## show endpoint-tracking interfaces

Display the status of Endpoint Tracking on interfaces. Only interfaces on which Endpoint Tracking has been created are shown.

### Syntax

- **show endpoint-tracking interfaces**
- **show endpoint-tracking interfaces gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show endpoint-tracking interfaces mlt <1-512>**

### Command Parameters

**gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mlt <1-512>**

Specifies the MLT ID.

### Default

None



## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show endpoint-tracking interfaces** command displays the following information:

Output field	Description
PORT NUM	Specifies the slot and port number, or the MLT ID.
INDEX	Specifies the interface index of the port or MLT.
STATUS	Specifies whether Endpoint Tracking is enabled or disabled on the port or MLT. Disabled specifies that Endpoint Tracking has been created but not enabled, and Enabled specifies that Endpoint Tracking has been created and enabled.

## Example

The following example displays the Endpoint Tracking status of ports and MLT interfaces. In this example, two ports have Endpoint Tracking created and enabled, one MLT has Endpoint Tracking created and enabled, and one MLT has Endpoint Tracking created but not yet enabled.

```
Switch:1>show endpoint-tracking interfaces
=====
Endpoint Tracking Interfaces
=====
PORT
NUM      INDEX      STATUS
-----
1/1      192        Enabled
1/10     201        Enabled
MLT-2    6145       Enabled
MLT-5    6148       Disabled
-----
4 out of 4 Total Num of Endpoint Tracking interfaces displayed
=====
```

## show energy-saver eee statistics

Display Energy Efficient Ethernet (EEE) statistics for all ports, or for a specific port.

## Syntax

- **show energy-saver eee statistics**

- **show energy-saver eee statistics** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

## Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show energy-saver eee statistics** command displays the following information:

Output field	Description
PortId	Specifies the port number.
EEE Status	Specifies whether EEE is enabled or disabled on the port.
Tx LPI Events	Specifies the number of times EEE has triggered Low Power Idle (LPI) on the transmitting side.
Tx Idle Duration	Specifies the total amount of time, in microseconds, during which the transmitting side was in Low Power Idle (LPI).
Rx LPI Events	Specifies the number of times EEE has triggered Low Power Idle (LPI) on the receiving side.
Rx Idle Duration	Specifies the total amount of time, in microseconds, during which the receiving side was in Low Power Idle (LPI).

## Example

```
Switch:1>show energy-saver eee statistics
```

```
=====
EEE Port Status
=====
```

PortId	EEE Status	Tx LPI Events	Tx Idle Duration (micro seconds)	Rx LPI Events	Rx Idle Duration (micro seconds)
1/1	enabled	847	963657920	115	965100020

## show fa

Display the Fabric Attach configuration status.

### Syntax

- **show fa**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show fa** command displays the following information:

Output field	Description
FA Service	Specifies whether Fabric Attach is enabled or disabled.
FA Element Type	Specifies the Fabric Attach element type.
FA Assignment Timeout	Specifies the Fabric Attach assignment time-out in seconds.
FA Discovery Timeout	Specifies the Fabric Attach discovery time-out in seconds.
FA Provision Mode	Specifies the Fabric Attach provision mode.

### Example

The following example displays the Fabric Attach configuration.

```
Switch:1>show fa

=====
                          Fabric Attach Configuration
=====
                          FA Service : enabled
                          FA Element Type : server
                          FA Assignment Timeout : 240
                          FA Discovery Timeout : 240
                          FA Provision Mode : spbm
```

## show fa agent

Display Fabric Attach agent information.

### Syntax

- **show fa agent**

### Command Parameters

**config**

Display Fabric Attach agent information.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show fa agent** command displays the following information:

Output field	Description
FA Service	Specifies whether Fabric Attach is enabled or disabled.
FA Element Type	Specifies the Fabric Attach element type.
FA Assignment Timeout	Specifies the Fabric Attach assignment time-out in seconds.
FA Discovery Timeout	Specifies the Fabric Attach discovery time-out in seconds.
FA Provision Mode	Specifies the Fabric Attach provision mode.

### Example

The following example displays the Fabric Attach agent information.

```
Switch:1>show fa agent
```

```
=====
                          Fabric Attach Configuration
=====
                          FA Service : enabled
                           FA Element Type : server
FA Assignment Timeout : 240
FA Discovery Timeout : 240
                           FA Provision Mode : spbm
```

## show fa assignment

Display Fabric Attach ISID-to-VLAN assignments.

### Syntax

- **show fa assignment**
- **show fa assignment {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show fa assignment** command displays the following information:

Output field	Description
Interface	Specifies the interface identifier of the I-SID-to-VLAN assignment.
I-SID	Specifies the I-SID value of the I-SID-to-VLAN assignment.
Vlan	Specifies the VLAN ID component of the I-SID-to-VLAN assignment.
State	Specifies the current state of the I-SID-to-VLAN assignment as one of the following values: <ul style="list-style-type: none"> <li>• Other</li> <li>• Pending</li> <li>• Active</li> <li>• Rejected</li> </ul>
Origin	Specifies the origin information of the I-SID-to-VLAN assignment.
I-SID Name	Specifies the I-SID name.

## Example

The following example displays the Fabric Attach assignment information.

```
Switch:>en
Switch:1#show fa assignment
=====
                          Fabric Attach Assignment Map
=====
Interface  I-SID      Vlan      State      Origin      I-SID Name
-----
1/1        2          2         active     proxy       ISID-2
1/2        3          3         active     proxy       ISID-3
1/2        4          4         active     proxy       ISID-4
1/3        5          5         reject     proxy       ISID-5
-----

4 out of 4 Total Num of fabric attach assignment mappings displayed
-----
```

## show fa elements

Display Fabric Attach discovery elements.

### Syntax

- **show fa elements**
- **show fa elements {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

User EXEC

## show fa interface

Display Fabric Attach configuration on all interfaces.

## Syntax

- **show fa interface**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show fa interface** command displays the following information:

Output field	Description
INTERFACE	Specifies the interface (port or MLT) on which Fabric Attach is configured.
SERVER STATUS	Specifies the current state of the Fabric Attach port. It is either enabled or disabled.
MGMT ISID	Specifies the Fabric Attach management I-SID for the associated port. A zero value indicates that the management I-SID is not specified for the interface.
MGMT CVID	Specifies the Fabric Attach management customer VLAN ID (C-VID) for the interface. A zero value indicates that no C-VID is specified for the interface.
MSG AUTH STATUS	Specifies the Fabric Attach message authentication status on the port.
MSG AUTH KEY	Specifies the Fabric Attach message authentication key for the associated port.
ORIGIN <b>Note:</b> Exception: Not supported on VSP 8600 Series and XA1400 Series.	Specifies the origin of the Fabric Attach port, either manually configured through CLI or EDM or dynamically configured through Auto-sense.

## Example

The following example displays the Fabric Attach configuration on all interfaces.

```
Switch:1>show fa interface

=====
                          Fabric Attach Interfaces
=====
INTERFACE      SERVER   MGMT    MGMT    MSG AUTH  MSG AUTH  ORIGIN
                STATUS  ISID    CVID    STATUS    KEY
```

```
-----  
Port2/10    enabled  0      0      enabled  ****  
Port4/6     enabled  0      0      enabled  ****  
Port4/11    enabled  0      0      enabled  ****  
Mlt2        enabled  0      0      enabled  ****  
-----
```

```
4 out of 4 Total Num of fabric attach interfaces displayed  
-----
```

## show fa interface disabled-auth

---

Display Fabric Attach interfaces with authentication disabled.

### Syntax

- **show fa interface disabled-auth**

### Default

None

### Command Mode

User EXEC

## show fa interface enabled-auth

---

Display Fabric Attach interfaces with authentication enabled.

### Syntax

- **show fa interface enabled-auth**

### Default

None

### Command Mode

User EXEC

## show fa interface mlt

---

Display Fabric Attach interfaces on an MLT.

### Syntax

- **show fa interface mlt**



- **show fa interface mlt <1-512>**

## Command Parameters

<1-512>

Display Fabric Attach interfaces on an MLT.

## Default

None

## Command Mode

User EXEC

---

## show fa interface port

Display Fabric Attach interfaces on a port.

## Syntax

- **show fa interface port**
- **show fa interface port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

---

## show fa statistics

Display global level Fabric Attach statistics.

## Syntax

- **show fa statistics**
- **show fa statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show fa statistics summary**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### summary

Display global level Fabric Attach statistics.

## Default

None

## Command Mode

User EXEC

---

## show fa zero-touch-client

Display fabric attach zero touch client information

## Syntax

- **show fa zero-touch-client**

## Default

None

## Command Mode

User EXEC

---

## show fdb-filter

Show forwarding database filter information. This command does not apply to all hardware platforms.

## Syntax

- **show fdb-filter**

## Default

None

## Command Mode

User EXEC

## show ftp-access

---

Show the maximum FTP sessions.

## Syntax

- **show ftp-access**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ftp-access** command displays the following information:

Output field	Description
max ipv4 sessions	Displays the maximum number of permitted IPv4 FTP sessions.
max ipv6 sessions	Displays the maximum number of permitted IPv6 FTP sessions.

## Example

The following example displays the command output.

```
Switch:1#show ftp-access
max ipv4 sessions : 4
max ipv6 sessions : 4
```

## show fulltech

---

Display the output of all show commands and, optionally, capture the output to a file. You can limit the display to Key Health Indicator (KHI) show commands.

The command output includes a recursive listing of filesystem contents.

## Syntax

- **show fulltech**
- **show fulltech file WORD<1-99>**
- **show fulltech khi**
- **show fulltech khi file WORD<1-99>**

## Command Parameters

**file WORD<1-99>**

Specifies the file name in the form /intflash/<file> or /usb/<file> {string length {1..99} }.

**khi**

Display output only from KHI show commands.

## Default

None

## Command Mode

User EXEC

## show ha-state

---

Show detailed information on the High Availability-CPU (HA-CPU) state of the system.



### Note

Use the **show sys-info** command to view the slots of the primary CPU and the standby CPU. You can also check whether the standby CPU is running in hot standby mode or warm standby mode.

## Syntax

- **show ha-state**

## Default

None.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show ha-state** command displays the following information:

Output field	Description
Current CPU State	Displays the HA-CPU state.

## Example

The following example shows sample command output.

```
Switch:1>show ha-state
Current CPU State : Initialization state.
```

## show hosts

Query the DNS host for information about host addresses. You can enter either a hostname or an IP address. If you enter the hostname, this command shows the IP address corresponding to the hostname and if you enter an IP address, this command shows the hostname for the IP address.

## Syntax

- **show hosts WORD<0-256>**

## Command Parameters

**WORD<0-256>**

Specifies one of the following: the name of the host DNS server as a string of 0-256 characters, the IP address of the host DNS server in a.b.c.d format, or the IPv6 address of the host DNS server in hexadecimal format (string length 0-46).

## Default

None

## Command Mode

User EXEC

## show ike certificate-identity

Display the X.509 V3 digital certificate subject name.

## Syntax

- **show ike certificate-identity**

## Command Parameters

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command is not supported on VSP 8600 Series.

---

## show ike policy

Display the configured IKE policies

## Syntax

- **show ike policy**
- **show ike policy WORD<1-32> laddr WORD<1-256>**
- **show ike policy WORD<1-32> laddr WORD<1-256> raddr WORD<1-256>**

## Command Parameters

**laddr WORD<1-256>**

Specifies the local IPv4 or IPv6 address.

**raddr WORD<1-256>**

Specifies the remote IPv4 or IPv6 address.

**WORD<1-32>**

Specifies the name of the policy to be displayed.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ike policy** command displays the following information:

Output field	Description
Policy Name	Specifies the name of the policy that is displayed.
Addr Type	Specifies whether the IP address is an IPv4 or IPv6 address.
Local Address	Specifies the local IPv4 or IPv6 address.
Remote Address	Specifies the remote IPv4 or IPv6 address.
Profile Name	Specifies the name of the profile.
Profile version	Specifies the version of the profile, version 1 or version 2.
Auth-Method	Specifies the authentication method. The supported values are digital-certificate and pre-shared-key.
Pre-Shared Key	Specifies the pre-shared key value.
Revocation-Check Method	Specifies the revocation check method as OCSP, CRL or none.
Peer-identity name	Specifies peer identity name for IKE phase 1.
DPD Timeout	Specifies the Dead-peer detection timeout in seconds. The supported value ranges from 1 to 4294967295 seconds.
Admin State	Specifies whether the IKE admin state is enabled or disabled.
Oper State	Specifies whether the policy is operational or not. The values are up and down.
P2 PFS	Specifies whether Phase 2 perfect forward secrecy is enabled or not.
Use IKE DH Grp	Specifies whether IKE can use the DH group or not. The values are enable and disable.
DH Group	Specifies the type of DH group selected. The supported values are modp768, modp1024, and modp2048.
Intfld	Specifies the ID of the interface on which the policy is applied.

## show ike profile

Display IKEv2 profiles.

### Syntax

- **show ike profile**
- **show ike profile WORD<1-32>**

### Command Parameters

**WORD<1-32>**

Specifies the name of the profile to be displayed.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ike profile** command displays the following information:

Output field	Description
<i>Name</i>	Specifies the name of the IKE Phase 1 profile.
<i>Hash Algo</i>	Specifies the hash authorization algorithm. The supported values are md5, sha, and sha256.
<i>Encrypt Algo</i>	Specifies the cryptographic algorithm. The supported values are desCbc, 3DesCbc, and aesCbc.
<i>Encrypt Key Len</i>	Specifies the length of the encryption key. The supported values are 128, 192 and 256.
<i>DH Group</i>	Specifies the Diffie-Hellman (DH) group. The supported values are modp768, modp1024, and modp2048.
<i>Exchange Mode</i>	Specifies the IKE mode. The supported mods are main mode and aggressive mode.
<i>Lifetime seconds</i>	Specifies the lifetime value in seconds.

## show ike sa

Display security associations.

## Syntax

- **show ike sa**
- **show ike sa version v1 WORD<1-32> laddr WORD<1-256> raddr WORD<1-256>**
- **show ike sa version v2 WORD<1-32> laddr WORD<1-256> raddr WORD<1-256>**

## Command Parameters

**laddr WORD<1-256>**

Specifies the local IPv4 or IPv6 address.

**raddr WORD<1-256>**

Specifies the remote IPv4 or IPv6 address.

**version v1 WORD<1-32>**

Specifies the local IPv4 or IPv6 address for IKE Phase 1, version 1 SA.



**version v2 WORD<1-32>**

Specifies the local IPv4 or IPv6 address for IKE Phase 1, version 2 SA.

**Default**

None

**Command Mode**

User EXEC

**show ike v2-profile**

Display IKE profiles.

**Syntax**

- **show ike v2-profile**
- **show ike v2-profile WORD<1-32>**

**Command Parameters**

**WORD<1-32>**

Specifies the name of the profile to be displayed.

**Default**

None

**Command Mode**

User EXEC

**Command Output**

The **show ike v2-profile** command displays the following information:

Output field	Description
Name	Specifies the name of the IKEv2 profile.
Hash Algo	Specifies the hash authorization algorithm. The supported values are MD5, SHA1, and SHA256.
Encrypt Algo	Specifies the cryptographic algorithm. The supported values are DES, 3DES, and AES.
Encrypt Key Length	Specifies the length of the encryption key. The supported values are 128, 192, and 256.

Output field	Description
DH Group	Specifies the Diffe-Hellman (DH) group. The supported values are modp768, modp024, and modp048.
Integrity Algorithm	Specifies IKE SA integrity algorithms supported in IKEv2.
Exchange Mode	Specifies the IKE mode. The supported mods are main mode and aggressive mode.
Lifetime seconds	Specifies the lifetime value in seconds.

## show io

Shows IO information.

### Syntax

- **show io control**
- **show io cpu-cosq-counters [file WORD<1-99>]**
- **show io filter-tables [file WORD<1-99>]**
- **show io ipsec logs [file WORD<1-99>]**
- **show io ipsec stats [file WORD<1-99>]**
- **show io l2-tables [file WORD<1-99>]**
- **show io l3-tables [file WORD<1-99> | verbose]**
- **show io logical-intf-ipsec [file WORD<1-99>]**
- **show io logical-intf-tables [file WORD<1-99>]**
- **show io nic-counters [file WORD<1-99>]**
- **show io performance-vcpu**
- **show io spb-tables [file WORD<1-99>]**
- **show io tunnel-stats**

### Command Parameters

#### control

Shows IO internal control statistics. Only run this command when requested by GTAC (Global Technical Assistance Center).

#### cpu-cosq-counters [file WORD<1-99>]

Shows the CPU cosq counters. Specify an optional filename to view the contents of a specific file.

#### filter-tables [file WORD<1-99>]

Shows the filter tables. Specify an optional filename to view the contents of a specific file.

#### ipsec logs [file WORD<1-99>]

Shows the IPsec logs. Specify an optional filename to view the contents of a specific log file. Use the **debug-ipsec level** command to determine how much information is logged. For more information, see [debug-ipsec level <-1-5>](#) on page 1061.

**ipsec stats [file WORD<1-99>]**

Shows the ipsec statistics. Specify an optional filename to view the contents of a specific file.

**I2-tables [file WORD<1-99>]**

Shows the Layer 2 tables. Specify an optional filename to view the contents of a specific file.

**I3-tables [file WORD<1-99>]**

Shows the Layer 3 tables. Specify an optional filename to view the contents of a specific file.

**logical-intf-ipsec [file WORD<1-99>]**

Shows the logical interface ipsec status. Specify an optional filename to view the contents of a specific file.

**logical-intf-tables [file WORD<1-99>]**

Shows the logical interface tables. Specify an optional filename to view the contents of a specific file.

**nic-counters [file WORD<1-99>]**

Shows the network interface card counters. Specify an optional filename to view the contents of a specific file.

**performance-vcpu**

Shows the CPU performance.

**spb-tables [file WORD<1-99>]**

Shows the Shortest Path Bridging tables. Specify an optional filename to view the contents of a specific file.

**tunnel-stats**

Shows the tunnel statistics.

**verbose**

Specifies verbose mode (detailed output).

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The parameters *cpu-cosq-counters*, *filter-tables*, *ipsec logs*, *ipsec stats*, *logical-intf-ipsec*, *logical-intf-tables*, *nic-counters*, *performance-vcpu*, *spb-tables*, and *tunnel-stats* only apply to XA1400 Series.

---

## show io resources

---

Shows IO resources information.

### Syntax

- `show io resources filter`
- `show io resources interface`
- `show io resources l3-defip-count`
- `show io resources l3-entry-count`
- `show io resources l3-kaps-count`
- `show io resources l3-lem-count`
- `show io resources mirror`
- `show io resources model`
- `show io resources model-dnx-stats`
- `show io resources nlb`
- `show io resources qos-group`
- `show io resources spbm-uni-detail`
- `show io resources spbm-uni-show`
- `show io resources verbose`
- `show io resources vxlan-vtep-count`

### Command Parameters

#### filter

Shows the IO resource manager filter.

#### interface

Shows the IO resource manager interface.

#### l3-defip-count

Shows the IO resource manager Layer3 defip count.

#### l3-entry-count

Shows the IO resource manager Layer3 entry count.

#### l3-kaps-count

Shows the IO resource manager Layer3 kaps count.

#### l3-lem-count

Shows the IO resource manager Layer3 lem count.

#### mirror

Shows the IO resource manager mirror.

#### model

Shows the IO resource manager slice statistics summary.

**model-dnx-stats**

Shows the IO resource manager dnx statistics summary.

**nlb**

Shows the IO resource manager NLB table.

**qos-group**

Shows the IO resource manager QoS group usage.

**spbm-uni-detail**

Shows the IO resource manager SPBM unicast detail.

**spbm-uni-show**

Shows the IO resource manager SPBM unicast.

**verbose**

Shows the IO resource manager additional Layer3 information (detailed output).

**vxlan-vtep-count**

Shows the IO resource manager VXLAN VTEP table.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The parameters *l3-kaps-count*, *l3-lem-count*, and *model-dnx-stats* only apply to VSP 8600 Series.

## show i-sid

---

Show all configured service instance identifiers (I-SID) along with their types, ports/mlt.

## Syntax

- **show i-sid [<1-16777215>]**

## Command Parameters

<1-16777215>

Specifies a service instance identifier (I-SID).

## Default

None

## Command Mode

User EXEC

## Command Output

The **show i-sid** command displays the following information:

Output field	Description
I-SID ID	Indicates the I-SID IDs.
I-SID TYPE	Indicated the I-SID type. <ul style="list-style-type: none"> <li>• T-UNI: Transparent Port UNI service.</li> <li>• ELAN: any to any service (switched service).</li> <li>• CVLAN: CVLAN based service.</li> </ul>
VLANID	Indicates the VLAN IDs.
PORT INTERFACES	Indicates the port interface.
MLT INTERFACES	Indicates the MLT interface.
ORIGIN	Indicates how the I-SID is discovered.
ISID NAME	Indicates the I-SID names.

## Example

View I-SID information.

```
Switch:1#show i-sid
=====
                                Isid Info
=====
ISID      ISID      VLANID    PORT      MLT        ORIGIN      ISID
ID        TYPE      VLANID    INTERFACES INTERFACES          NAME
-----
15999999  ELAN      4048      -         -         C --- - --- - -   Onboarding I-SID
16777001  ELAN      N/A       -         -         C --- - --- - -   FAN-ISID

c: customer vid    u: untagged-traffic

All 2 out of 2 Total Num of i-sids displayed

ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
M: FA management; E: discovered by EAP; A: auto-sense; R: multi-area redist
l: discover by local switch  r: discover by remote VIST switch
```

## show i-sid elan

Show the elan (Switched UNI) based service instance identifiers (I-SID).

## Syntax

- **show i-sid elan**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show i-sid elan** command displays the following information:

Output field	Description
I-SID ID	Indicates the I-SID IDs.
I-SID TYPE	Indicated the I-SID type. <ul style="list-style-type: none"> <li>T-UNI: Transparent Port UNI service.</li> <li>ELAN: any to any service (switched service).</li> <li>CVLAN: CVLAN based service.</li> </ul>
VLANID	Indicates the VLAN IDs.
PORT INTERFACES	Indicates the port interface.
MLT INTERFACES	Indicates the MLT interface.
ORIGIN	Indicates how the I-SID is discovered.
ISID NAME	Indicates the I-SID names.

## Example

View I-SID elan information.

```
Switch:1>show i-sid elan

=====
                        Isid Info
=====
ISID   ISID   VLANID  PORT      MLT      ORIGIN      ISID
ID     TYPE   ID       INTERFACES INTERFACES              NAME
-----
27     ELAN   N/A     c4000:1/1,2/11  -        C --- - --- -   ISID-27
38     ELAN   N/A     c4000:1/2,2/22  -        C --- - --- -   ISID-38
270    ELAN   N/A     c4001:1/1,2/11  -        C --- - --- -   ISID-270
307    ELAN   N/A     c307:1/5,2/5    -        C --- - --- -   ISID-307
308    ELAN   N/A     c308:1/6,2/6    -        C --- - --- -   ISID-308
309    ELAN   N/A     c309:1/1,2/1    -        C --- - --- -   ISID-309
310    ELAN   N/A     c310:1/2,2/2    -        C --- - --- -   ISID-310
311    ELAN   N/A     c311:1/3,2/3    -        C --- - --- -   ISID-311
312    ELAN   N/A     c312:1/4,2/4    -        C --- - --- -   ISID-312
317    ELAN   N/A     c317:1/7,2/7    -        C --- - --- -   ISID-317
318    ELAN   N/A     c318:1/8,2/8    -        C --- - --- -   ISID-318
319    ELAN   N/A     c319:1/9,2/9    -        C --- - --- -   ISID-319
320    ELAN   N/A     c320:1/10,2/10  -        C --- - --- -   ISID-320

--More-- (q = quit)

c: customer vid    u: untagged-traffic

13 out of 77 Total Num of Elan displayed

ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
```

M: FA management; E: discovered by EAP; A: auto-sense  
 l: discover by local switch r: discover by remote VIST switch

## show i-sid elan-transparent

Show the elan-transparent (Transparent UNI) based service instance identifiers (I-SID).

### Syntax

- **show i-sid elan-transparent**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show i-sid elan-transparent** command displays the following information:

Output field	Description
I-SID ID	Indicates the I-SID IDs.
I-SID TYPE	Indicated the I-SID type. <ul style="list-style-type: none"> <li>• T-UNI: Transparent Port UNI service.</li> <li>• ELAN: any to any service (switched service).</li> <li>• CVLAN: CVLAN based service.</li> </ul>
VLANID	Indicates the VLAN IDs.
PORT INTERFACES	Indicates the port interface.
MLT INTERFACES	Indicates the MLT interface.
ISID NAME	Indicates the I-SID names.

### Example

View I-SID elan-transparent information.

```
Switch:1 (config)#show i-sid elan-transparent
=====
                          Isid Info
=====
ISID      ISID      VLANID    PORT      MLT      ISID
ID        TYPE          ID        INTERFACES INTERFACES NAME
-----
2         ELAN_TR    N/A       -         -         ExtremeServer2
25        ELAN_TR    N/A       1/2-1/8,8/11 25       ExtremeServer4
```



```
All 1 out of 1 Total Num of elan-tp i-sids displayed
```

## show i-sid limit-fdb-learning

---

Displays the maximum MAC learning limit configured for an I-SID.

### Syntax

- **show i-sid limit-fdb-learning**

### Command Parameters

#### limit-fdb-learning

Shows the I-SID based max MAC limit information.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

### Command Output

The **show i-sid limit-fdb-learning** command displays the following information:

Output field	Description
ISID ID	Specifies the service interface identifier (I-SID)
MAC-LIMIT STATUS	Specifies whether the MAC learning limit is enabled or disabled
MAXMAC COUNT	Specifies the MAC learning limit

## show i-sid mac-address-entry

---

Display all C-MACs learnt on T-UNI ports for a given I-SID.

## Syntax

- **show i-sid mac-address-entry** [**<1-16777215>**] [**home**] [**mac <0x00:0x00:0x00:0x00:0x00:0x00>**] [**non-local**] [**port <{slot/port[/sub-port]}[-slot/port[/sub-port]][, ...]>**] [**remote**]

## Command Parameters

**<1-16777215>**

Specifies a service instance identifier (I-SID).

**home**

Filters the command output to show only MAC addresses learned in the home area.

**mac <0x00:0x00:0x00:0x00:0x00:0x00>**

Specifies a MAC address.

**non-local**

Filters the command output to show only MAC addresses learned from other nodes; not local nodes.

**port {slot/port[/sub-port]}[-slot/port[/sub-port]][, ...]**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**remote**

Filters the command output to show only MAC addresses learned in the remote area.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show i-sid mac-address-entry** command displays the following information:

Output field	Description
I-SID	Specifies the service interface identifier (I-SID).
STATUS	Specifies the learning status of the associated MAC.
MAC-ADDRESS	Specifies the MAC address of the port assigned to the specific I-SID or MAC learned on the specific I-SID.
INTERFACE	Specifies the port or MLT on which the MAC is learned for the specific I-SID.

Output field	Description
TYPE	Specifies if the MAC address is learned locally or on an NNI port from a remote destination.
DEST-MAC	Specifies the virtual B-MAC address or system ID, in MAC format, of the destination node.
BVLAN	Specifies the B-VLAN on which the destination node is discovered for the I-SID.
DEST-SYSNAME	Specifies the destination system name.
AREA-ROLE	Indicates the area role of the system.
AREA-NAME	Indicates the area name of the system.

## show i-sid name

Shows the global I-SID name to I-SID mapping.

### Syntax

- **show i-sid name [name WORD<1-64>]**

### Command Parameters

**name WORD<1-64>**

Specifies the global I-SID name to I-SID mapping.

By default, the service is named ISID-x, where x correlates to the I-SID number of the service.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command is not supported on VSP 8600 Series or XA1400 Series.

## Command Output

The **show i-sid name** command displays the following information:

Output field	Description
I-SID	Indicates the I-SID IDs.
ISID NAME	Indicates the I-SID names.
TYPE	<p>Shows the I-SIDs that are in use as services and the I-SIDs that the administrator names.</p> <p>An I-SID can have one base type or a combination of base types. You can use the combination of base types so that multiple services can use the same I-SID at the same time. Following are some of the combinations of the base types:</p> <ul style="list-style-type: none"> <li>• config—Shows the SUNI (elan) or TUNI (elan-transparent) in use.</li> <li>• discoverLocal—Shows the information that is discovered locally. For example, fabric attach and endpoint tracking information that is received from the local box.</li> <li>• discoverRemote—Shows the information that is discovered remotely. For example, SMLT peer communicates on fabric attached or EPT discovery.</li> <li>• mgmt—Shows the fabric attach management details.</li> <li>• l2vsn—Shows the layer 2 VSN details, such as VLAN I-SID for port based or private VLAN for etree.</li> <li>• l3vsn—Shows the layer 3 VSN details, such as IPVPN and IPv6 IPVPN.</li> <li>• adminName—Shows the user names service details.</li> <li>• eapDiscoverLocal—Shows the information that is discovered by EAP.</li> <li>• eapDiscoverRemote—Shows the information that is discovered by an EAP IST peer.</li> <li>• autoSense—Shows the onboarding I-SID, discovered by Zero Touch Fabric Configuration.</li> </ul>

## Example

View I-SID names.

```
Switch:1(config)#show i-sid name
=====
                        I-SID Name
=====
I-SID      I-SID NAME      TYPE
-----
1          ExtremeServer1  adminName
2          ExtremeServer2  adminName
3          ExtremeServer3  config adminName
4          ISID-4          config
23         ISID-23         config
25         ExtremeServer4  config adminName

Total number of I-SID Name entries: 6.
```

---

## show ip arp

---

Show ARP information to view the configuration information in the ARP table.

### Syntax

- **show ip arp**
- **show ip arp {A.B.C.D}**
- **show ip arp gigabitEthernet {{slot/port[sub-port]}}**
- **show ip arp gigabitEthernet {{slot/port[sub-port]} vrfids WORD<0-512>**
- **show ip arp gigabitEthernet{{slot/port[sub-port]} vrf WORD<1-16>**
- **show ip arp -s {A.B.C.D} {A.B.C.D}**
- **show ip arp spbm-tunnel-as-mac**
- **show ip arp vlan <1-4059>**
- **show ip arp vrf WORD<1-16>**
- **show ip arp vrfids WORD<0-512>**

### Command Parameters

**{A.B.C.D}**

Specifies the network IP address for the table.

**{slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the subport in the format slot/port/sub-port.

**gigabitEthernet {slot/port[sub-port]} vrfids WORD<0-512>**

Specifies the VRF ID. The total number of ARPs listed in the summary line of the show ip arp display represents the total number of ARPs on the chassis, including all VRFs (which includes the Mgmt Router VRF). {{slot/port[sub-port]} identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the subport in the format slot/port/sub-port.

**interface**

Displays ARP interface configuration information.

**-s {A.B.C.D} {A.B.C.D}**

Specifies the network IP address for the table.

**spbm-tunnel-as-mac**

Displays the remote host name in the TUNNEL column for the SPBM ARP entry.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the name of the VRF. The total number of ARPs listed in the summary line of the show ip arp display represents the total number of ARPs on the chassis including all VRFs (which includes the Mgmt Router VRF).

**vrfids WORD<0-512>**

Specifies the VRF ID. The total number of ARPs listed in the summary line of the show ip arp display represents the total number of ARPs on the chassis, including all VRFs (which includes the Mgmt Router VRF).

**vrfids WORD<0-512>**

Specifies the VRF ID. The total number of ARPs listed in the summary line of the show ip arp display represents the total number of ARPs on the chassis, including all VRFs (which includes the Mgmt Router VRF).

## Default

None

## Command Mode

User EXEC

## show ip arp gigabitethernet

---

Display ARP entries for a particular brouter port.

## Syntax

- **show ip arp gigabitethernet {slot/port[/sub-port]}**
- **show ip arp gigabitEthernet**
- **show ip arp gigabitethernet {slot/port[/sub-port]} vrf WORD<1-16>**
- **show ip arp gigabitethernet {slot/port[/sub-port]} vrfids WORD<0-512>**

## Command Parameters

**{slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the subport in the format slot/port/sub-port.

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## show ip arp interface

---

Show ARP port information to display data about the specified port, all ports, or the VLAN.

## Syntax

- **show ip arp interface**
- **show ip arp interface gigabitethernet**
- **show ip arp interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show ip arp interface vlan <1-4059>**

## Command Parameters

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show ip arp spbm-tunnel-as-mac

---

Display SPBM ARP entry tunnel as BMAC.

## Syntax

- **show ip arp spbm-tunnel-as-mac**

## Default

None

## Command Mode

User EXEC

---

## show ip arp-inspection

Displays DAI information.

## Syntax

- **show ip arp-inspection**
- **show ip arp-inspection vlan <1-4059>**
- **show ip arp-inspection vrf WORD<1-16>**
- **show ip arp-inspection vrfids WORD<0-512>**

## Command Parameters

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the name of the VRF. The total number of ARPs listed in the summary line of the show ip arp display represents the total number of ARPs on the chassis including all VRFs (which includes the Mgmt Router VRF).

**vrfids WORD<0-512>**

Specifies the VRF ID. The total number of ARPs listed in the summary line of the show ip arp display represents the total number of ARPs on the chassis, including all VRFs (which includes the Mgmt Router VRF).

## Default

None



## Command Mode

User EXEC

## show ip arp-inspection interface

---

Displays DAI interface configuration.

### Syntax

- **show ip arp-inspection interface**
- **show ip arp-inspection interface vlan**
- **show ip arp-inspection interface vlan <1-4059>**
- **show ip arp-inspection interface vrf WORD<1-16>**
- **show ip arp-inspection interface vrfids WORD<0-512>**

### Command Parameters

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Displays DAI configuration for a particular VRF.

**vrfids WORD<0-512>**

Displays DAI configuration for a particular VRF ID.

### Default

None

## Command Mode

User EXEC

## show ip arp-inspection interface gigabitEthernet

---

Displays DAI configuration on the port.

## Syntax

- `show ip arp-inspection interface gigabitEthernet`
- `show ip arp-inspection interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} vrf WORD<1-16>`
- `show ip arp-inspection interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} vrfids WORD<0-512>`
- `show ip arp-inspection interface gigabitEthernet <1-4059> vrf WORD<1-16>`
- `show ip arp-inspection interface gigabitEthernet <1-4059> vrfids WORD<0-512>`
- `show ip arp-inspection interface gigabitEthernet vrf WORD<1-16>`
- `show ip arp-inspection interface gigabitEthernet vrfids WORD<0-512>`

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]][,...]}

Displays DAI configuration for a particular port.

<1-4059>

Displays the DAI VLAN configuration.

vrf WORD<1-16>

Displays DAI configuration for a particular VRF.

vrfids WORD<0-512>

Displays DAI configuration for a particular VRF ID.

## Default

None

## Command Mode

User EXEC

## show ip as-list

Show the AS path lists on the Global Router.

## Syntax

- `show ip as-list [<1-1024>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

## Command Parameters

<1-1024>

Specifies the list ID.

**vrf WORD<1-16>**

Specifies the name of the VRF.

**vrfids WORD<0-512>**

Specifies the VRF ID in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

## show ip bfd

Display global Bidirectional Forwarding Detection (BFD) configuration information for IPv4 interfaces.

## Syntax

- **show ip bfd**
- **show ip bfd vrf**
- **show ip bfd vrfids**

## Command Parameters

**vrf**

Specifies a VRF instance by VRF name.

**vrfids**

Specifies a VRF or range of VRFs by ID.

## Command Mode

User EXEC

## Command Output

The **show ip bfd** command displays the following information:

Output field	Description
BFD Version	Specifies the current BFD version.
Admin Status	Specifies whether BFD is enabled globally.
Trap Enable	Specifies whether traps are enabled.
Total session number	Specifies the total number of BFD sessions.

Output field	Description
UP	Specifies whether a BFD session is in UP state.
DOWN	Specifies whether a BFD session is in DOWN state.
AdminDown	Specifies whether a BFD session is in AdminDown state.
Init	Specifies whether a BFD session is in Init state.

## Example

The following example displays global configuration information for BFD on an IPv4 interface.

```
Switch:1>show ip bfd
=====
                        BFD information - GlobalRouter
=====
                        BFD Version : 1
                        Admin Status : TRUE
                        Trap Enable  : FALSE
-----
Total session number : 1

UP: 1, DOWN: 0, AdminDown: 0, Init: 0
-----
```

## show ip bfd interfaces

Display Bidirectional Forwarding Detection (BFD) configuration for a port, VLAN, or loopback on an IPv4 interface.

### Syntax

- **show ip bfd interfaces gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ip bfd interfaces gigabitethernet vrf WORD<1-16>**
- **show ip bfd interfaces gigabitethernet vrfids WORD<0-512>**
- **show ip bfd interface loopback <1-256>**
- **show ip bfd interfaces vlan <1-4059>**
- **show ip bfd interfaces vlan vrf WORD<1-16>**
- **show ip bfd interfaces vlan vrfids WORD<0-512>**

### Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

```
vlan <1-4059>
```

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF instance by VRF name.

**vrfids WORD<0-512>**

Specifies a VRF or range of VRFs by ID.

**<1-256>**

Specifies the loopback interface ID value.

This parameter does not apply to all hardware platforms.

## Command Mode

User EXEC

## Command Output

The **show ip bfd interfaces** command displays the following information:

Output field	Description
VLAN	Specifies the VLAN ID. This field displays only in output for VLAN interfaces.
PORT	Specifies the port number. This field displays only in output for GigabitEthernet interfaces.
INTF ID	Specifies the loopback interface ID. This field displays only in output for Loopback interfaces. This parameter does not apply to all hardware platforms.
STATUS	Specifies whether BFD is enabled on the interface.
MIN_RX	Specifies the receive interval in milliseconds.
INTERVAL	Specifies the transmit interval in milliseconds.
MULTIPLIER	Specifies the multiplier used to calculate the amount of time BFD waits before declaring a receive timeout.
VRF-ID	Specifies a VRF ID.

## Examples

The following example displays VLAN interface configuration information for BFD.

```
Switch:1>show ip bfd interfaces vlan 11
=====
                        Vlan Bfd
=====
VLAN      STATUS    MIN_RX    INTERVAL  MULTIPLIER  VRF-ID
=====
```

```
11          enable      200      200      3          0
```

The following example displays Loopback interface configuration information for BFD:

```
Switch:1>enable
Switch:1#show ip bfd interfaces loopback
=====
                        Circuitless IP Interface Bfd
=====
INTF ID   STATUS   MIN_RX   INTERVAL  MULTIPLIER  VRF-ID
-----
1         enable  200     200       3           0
2         enable  200     200       3           2
```

## show ip bfd neighbors

Display Bidirectional Forwarding Detection (BFD) session information for IPv4 neighbors.

### Syntax

- **show ip bfd neighbors**
- **show ip bfd neighbors next-hop**
- **show ip bfd neighbors vrf**
- **show ip bfd neighbors vrfids**

### Command Parameters

#### next-hop

Specifies the next-hop IP address in the format a.b.c.d.

#### vrf

Specifies a VRF instance by VRF name.

#### vrfids

Specifies a VRF or range of VRFs by ID.

### Command Mode

User EXEC

### Command Output

The **show ip bfd neighbors** command displays the following information:

Output Field	Description
MY_DISC	Specifies the local discriminator for the BFD session.
YOUR_DISC	Specifies the remote discriminator for the BFD session.

Output Field	Description
NEXT_HOP	Specifies the next-hop IP address.
STATE	Specifies the BFD session state. Possible values are Down, Up, Init, and AdminDown.
MULTI	Specifies the multiplier used to calculate the amount of time BFD waits before declaring a receive timeout.
MIN_TX	Specifies, in microseconds, the minimum interval that the local system prefers to use when transmitting BFD control packets.
MIN_RX	Specifies, in microseconds, the minimum interval between received BFD control packets.
ACT_TX	Specifies, in microseconds, the actual transmission interval.
DETECT_TIME	Specifies the period of time without receiving BFD packets, after which the session is determined to have failed.
REMOTE_STATE	Specifies the BFD session state of the remote system.
APP	Specifies the application configured on the BFD session.
RUN	Specifies the application running on the BFD session.

## Example

The following example displays BFD session information for an IPv4 neighbor.

```
Switch:1>show ip bfd neighbors
-----
                        BFD Session - GlobalRouter
-----
MY_DISC   YOUR_DISC  NEXT_HOP      STATE      MULTI  MIN_TX  MIN_RX  ACT_TX  DETECT_TIME  REMOTE_STATE  APP  RUN
-----
1          0          192.0.2.11    Down       3      200    200    1000   600          Down         O    0
-----
1 out of 1 BFD session displayed
-----
APP and RUN Legend:
      B=BGP, O=OSPF, S=Static Route
-----
```

## show ip bfd stats

Display Bidirectional Forwarding Detection (BFD) statistics for IPv4 interfaces.

## Syntax

- **show ip bfd stats**
- **show ip bfd stats vrf WORD<1-16>**
- **show ip bfd stats vrfids WORD<0-512>**

## Command Parameters

### vrf

Specifies a VRF instance by VRF name.

### vrfids

Specifies a VRF or range of VRFs by ID.

## Command Mode

User EXEC

## Command Output

The **show ip bfd stats** command displays the following information:

Output field	Description
MY_DISC	Specifies the local discriminator for the BFD session.
YOUR_DISC	Specifies the remote discriminator for the BFD session.
NEXT_HOP	Specifies the next-hop IPv4 address.
PACKT_IN	Specifies the total number of BFD messages received for this BFD session.
PACKET_OUT	Specifies the total number of BFD messages sent for this BFD session.
LAST_UP	The value of sysUpTime on the most recent occasion at which the session came up. If no such up event exists this object contains a zero value.
LAST_DOWN	The value of sysUpTime on the most recent occasion at which the last time communication was lost with the neighbor. If no such down event exist this object contains a zero value

## Example

The following example displays BFD statistics for IPv4 interfaces.

```
Switch:1>show ip bfd stats
=====
BFD staticstics - GlobalRouter
=====
MY_DISC    YOUR_DISC  NEXT_HOP    PACKT_IN    PACKET_OUT  LAST_UP    LAST_DOWN
-----
1          0          192.0.2.10  4661750     4620630    Mon Sep  6 15:31:15 2021  Mon Sep  6
15:28:08 2021
-----
```



## show ip bgp aggregates

---

Display information about current aggregate addresses.

### Syntax

- **show ip bgp aggregates** [**<prefix/len>**] [**vrf WORD<1-16>**] [**vrfids WORD<0-255>**]

### Command Parameters

**<prefix/len>**

Specifies the IP address and the mask length (the length can be 0 to 32).

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD <0-512>**

Specifies a range of VRFs by ID number.

### Default

None

### Command Mode

User EXEC

## show ip bgp cidr-only

---

Display information about classless interdomain routing (CIDR) routes.

### Syntax

- **show ip bgp cidr-only** [**<prefix/len>**] [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]

### Command Parameters

**<prefix/len>**

Specifies an exact match of the prefix. This is an IP address and an integer value between 0 and 32 in the format a.b.c.d/xx.

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip bgp cidr-only** command displays the following information:

Output field	Description
NETWORK/MASK	Specifies the network IP address and exact mask length (must be an integer value from 0-32).
PEER REM ADDR	Specifies the IP address of the remote peer.
NEXTHOP ADDRESS	Specifies the IP address of the next hop.
ORG	Specifies the source of a route: <ul style="list-style-type: none"> <li>• IGP — the route is interior to the originating AS that inserts this route into the BGP table (0 = IGP).</li> <li>• EGP — the route is learned through an Exterior Gateway Protocol (EGP) before it is inserted into the BGP table (1 = BGP).</li> <li>• Incomplete — the origin of the route is unknown or learned by some other means. For example, the router learns these routes through RIP, OSPF, or static routes (2 = Incomplete).</li> </ul>
LOC PREF	Specifies the local preference.

## show ip bgp confederation

View BGP confederation information on the switch.

## Syntax

- **show ip bgp confederation**

## Default

None

## Command Mode

User EXEC

## show ip bgp dampened-paths

Display information about flap-dampened routes to determine unreliable routes.

## Syntax

- **show ip bgp dampened-paths** <A.B.C.D> [<prefix/len>] [longer-prefixes] [vrf WORD<1-16>] [vrfids WORD<0-512>]

## Command Parameters

**{A.B.C.D}**

Specifies the source IP address in the format a.b.c.d.

**<prefix/len>**

Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).

**longer-prefixes**

Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip bgp dampened-paths** command displays the following information:

Output field	Description
NETWORK/MASK	Specifies the network IP address and exact mask length (must be an integer value from 0-32).
PEER REM ADDR	Specifies the IP address of the remote peer.
NEXTHOP ADDRESS	Specifies the IP address of the next hop.

Output field	Description
ORG	Specifies the source of a route: <ul style="list-style-type: none"> <li>IGP — the route is interior to the originating AS that inserts this route into the BGP table (0 = IGP).</li> <li>EGP — the route is learned through an Exterior Gateway Protocol (EGP) before it is inserted into the BGP table (1 = BGP).</li> <li>Incomplete — the origin of the route is unknown or learned by some other means. For example, the router learns these routes through RIP, OSPF, or static routes (2 = Incomplete).</li> </ul>
LOC PREF	Specifies the local preference.

## show ip bgp flap-damp-config

Display global information about flap-dampening.

### Syntax

- show ip bgp flap-damp-config** [**<prefix/len>**] [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]

### Command Parameters

**<prefix/len>**

Specifies the exact match the prefix {a,b,c,d/len}.

**vrf WORD <1-16>**

Displays BGP configuration for a particular VRF.

**vrfids WORD<0-512>**

Specifies the VRF ID in the range of 0 to 512.

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ip bgp flap-damp-config** command displays the following information:

Output field	Description
Status	Indicates the global state of the route flap dampening feature. Valid values are enable or disable.
PolicyName	This field does not apply to the switch.
CutoffThreshold	Indicates the penalty level that causes route suppression.
ReuseThreshold	Specifies the system-configured time for route reuse.
Decay	Indicates the decay rate based on the decay algorithm.
MaxHoldDown	Indicates the maximum length of time, in seconds, to suppress the route.

## show ip bgp imported-routes

Display information about BGP imported routes.

### Syntax

- **show ip bgp imported-routes** [**<prefix/len>**][**longer-prefixes**] [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]

### Command Parameters

**<prefix/len>**

Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).

**longerprefixes**

Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ip bgp imported-routes** command displays the following information:

Output field	Description
ROUTE	Specifies the IP address of the route.
METRIC	Specifies the route metric.
COMMUNITY	Specifies the BGP community.
LOCALPREF	Specifies the local preference.
NEXTHOP	Specifies the IP address of the next hop.
ORIGIN	Specifies the source of a route: <ul style="list-style-type: none"> <li>IGP — the route is interior to the originating AS that inserts this route into the BGP table (0 = IGP).</li> <li>EGP — the route is learned through an Exterior Gateway Protocol (EGP) before it is inserted into the BGP table (1 = BGP).</li> <li>Incomplete — the origin of the route is unknown or learned by some other means. For example, the router learns these routes through RIP, OSPF, or static routes (2 = Incomplete).</li> </ul>

## show ip bgp neighbors

Display information about BGP peer advertised routes, peer routes, and IP VPN BGP peers.

### Syntax

- **show ip bgp neighbors** [{A.B.C.D}] [advertised-routes] [<prefix/len>] [vrf WORD<1-16>] [vrfids WORD<0-512>]
- **show ip bgp neighbors** [{A.B.C.D}] [vrf WORD<1-16>] [vrfids WORD<0-512>]
- **show ip bgp neighbors** {A.B.C.D} routes [<prefix/len>] [community <disable|enable>] [longerprefixes] [vrf WORD<1-16>] [vrfids WORD<0-512>]
- **show ip bgp neighbors** {A.B.C.D} stats [vrf WORD<1-16>] [vrfids WORD<0-512>]
- **show ip bgp neighbors** {A.B.C.D} vpnv4 [<prefix/len>] [community <disable|enable>] [extcommunity] [longer-prefixes] [vrf WORD<1-16>] [vrfids WORD<0-512>]

### Command Parameters

{A.B.C.D}

Specifies the IP address.

<prefix/len>

Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).

advertised-routes

Displays information about BGP peer advertised routes.

**community**

Enables the display of community attributes.

**ext-community**

Enables the display of extended community attributes.

**longer-prefixes**

Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c.d/32).

**routes**

Displays information about BGP peer routes.

**stats**

Displays statistics information for BGP peers.

**vpn4**

Displays information about IP VPN BGP peers.

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## show ip bgp networks

---

Display information about BGP network configurations.

## Syntax

- **show ip bgp networks** [**<prefix/len>**] [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]

## Command Parameters

**<prefix/len>**

Shows networks with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## show ip bgp peer-group

---

Display information about BGP peer groups.

## Syntax

- **show ip bgp peer-group [WORD<0-1536>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

**WORD<0-1536>**

Specifies the name of the peer group.

## Default

None

## Command Mode

User EXEC

## show ip bgp redistributed-routes

---

View BGP redistribution information on the switch.

## Syntax

- **show ip bgp redistributed-routes <prefix/len> vrf WORD<1-16> vrfids WORD<0-512>**



## Command Parameters

**<prefix/len>**

Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip bgp redistributed-routes** command displays the following information:

Output field	Description
SRC-VRF	Indicates the redistribution source VRF instance.
SRC	Indicates the redistribution source: RIP, Local, Static, or OSPF.
MET	Indicates the metric value.
MET-TYPE	Indicates the redistribution metric type.
ENABLE	Indicates whether the redistribution policy is enabled (T) true or disabled (F) false.
RPOLICY	The route policy currently assigned to the redistribution.

## show ip bgp route

Display information about BGP routes.

## Syntax

- show ip bgp route** [**<prefix/len>**] [**longer-prefixes**] [**community <enable|disable>**] [**ip <A.B.C.D>**] [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]

## Command Parameters

**<prefix/len>**

Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).

**community <enable|disable>**

Enables or disables the display of community attributes.

**ip <A.B.C.D>**

Specifies an IP address.

**longer-prefixes**

Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).

**vrf WORD<1-16>**

Specifies a VRF instance by name.

**vrfids WORD<0-512>**

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip bgp route** command displays the following information:

Output field	Description
NETWORK/MASK	Specifies the path prefix address.
PEER REM ADDR	Specifies the remote peer address.
NEXTHOP ADDRESS	Specifies the BGP next hop address.
ORG	Specifies the source of a route: <ul style="list-style-type: none"> <li>IGP — the route is interior to the originating AS that inserts this route into the BGP table (0 = IGP).</li> <li>EGP — the route is learned through an Exterior Gateway Protocol (EGP) before it is inserted into the BGP table (1 = BGP).</li> <li>Incomplete — the origin of the route is unknown or learned by some other means. For example, the router learns these routes through RIP, OSPF, or static routes (2 = Incomplete).</li> </ul>
LOCAL PREF	Specifies the local preference.

## show ip bgp stats

View Border Gateway Protocol (BGP) statistics.

## Syntax

- `show ip bgp stats`
- `show ip bgp stats vrf WORD<1-16>`
- `show ip bgp stats vrf WORD<1-16> vrfids WORD<0-512>`
- `show ip bgp stats vrfids WORD<0-512>`

## Command Parameters

`vrf WORD<1-16>`

Specifies a VRF instance by name.

`vrfids WORD<0-512>`

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## show ip bgp summary

---

Display summarized information about Border Gateway Protocol (BGP).

## Syntax

- `show ip bgp summary [vrf WORD<1-16>] [vrfids WORD<0-512>]`

## Command Parameters

`vrf WORD <1-16>`

Specifies a VRF instance by name.

`vrfids WORD <0-512>`

Specifies a range of VRFs by ID number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip bgp summary** command displays the following information:

Output field	Description
BGP version	Specifies the version of BGP that runs on the router.
local-as	Specifies the local autonomous system number.
Identifier	Specifies the BGP identifier.
Decision state	Specifies the BGP process state.
NEIGHBOR	Specifies the IP address of the remote peer.
RMTAS	Specifies the AS number of the remote peer.
STATE	Specifies the peer operating state: Idle, Accept, Connect, Open, Open-sent, and Established.
HLDTM	Specifies the negotiated hold time timer.
KPALV	Specifies the keep alive timer.
HLDCFG	Specifies the configured hold time timer.
KPCFG	Specifies the configured keep alive timer.
WGHT	Specifies the weight value assigned to the peer.
CONRTY	Specifies the retry timer.
ADVINT	Specifies the advertisement interval.
UPTime	Specifies how long (in seconds) this peer has been in the established state, or how long since this peer was last in the established state. It is set to zero when a new peer is configured or when the router is booted. If the peer never reaches the established state, the value remains zero.

## show ip community-list

Show the community lists on the Global Router.

### Syntax

- show ip community-list** [**<1-1024>**] [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]

### Command Parameters

**<1-1024>**

Specifies the list ID.

**vrf WORD<1-16>**

Specifies the name of the VRF.

**vrfids WORD<0-512>**

Specifies the VRF ID in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

# show ip dhcp-relay counters

---

Display information about the Dynamic Host Configuration Protocol (DHCP) relay counters.

## Syntax

- **show ip dhcp-relay counters**
- **show ip dhcp-relay counters [option82]**
- **show ip dhcp-relay counters [option82] [vrf WORD<1-16>]**
- **show ip dhcp-relay counters [option82] [vrf WORD<1-16>] [vrfids <0-512>]**
- **show ip dhcp-relay counters [option82] [vrfids <0-512>]**
- **show ip dhcp-relay counters [vrf WORD<1-16>]**
- **show ip dhcp-relay counters [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip dhcp-relay counters [vrfids WORD<0-512>]**

## Command Parameters

### option82

Shows statistics for the relay agent option.

### vrf WORD<1-16>

Specifies the name of the VRF.

### vrfids <0-512>

Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip dhcp-relay counters option82** command displays the following information:

Output field	Description
INTERFACE	Shows the VLAN or port associated with the respective relay interface.
IP ADDR	Shows the IP address of the respective relay interface.
FOUND OPT82	Shows the number of packets received that included option82. This number increases every time a valid DHCP packet that contains option82 arrives on the respective relay interface.
DROP PKT	Shows the number of packets the interface did not forward. This number increases every time a DHCP packet that has option82 arrives on a relay interface but is not forwarded on the interface towards the server; the path towards the relay can include additional DHCP relays. To determine the cause of the drop, you must enable trace on level 170.
CIRC ID	Show the circuit ID associated with the respective interface.
ADD CIRC	Shows on how many packets the circuit ID was inserted for that interface. This number increases every time the relay adds a circuit id sub-option in a generated option82 packet to send on an interface towards the server. If you expect this value to increase but it does not, and the interface does not drop a packet, it is possible the packet does not have enough space to insert the option. You must enable trace on level 170 to determine the cause.
DEL CIRC	Shows on how many packets the circuit id was removed for that interface. This number increases every time the relay removes a circuit id sub-option from an option82 packet received on a interface towards the server.
REMOTE ID	Shows the remote ID associated with the respective interface. The value is the MAC address of the interface.
ADD REMID	Shows on how many packets the remote ID was inserted for that interface. This number increases every time the relay adds a remote id sub-option in a generated option82 packet to send through an interface towards a server. If you expect this value to increase but it does not, and the interface does not drop a packet, it is possible the packet does not have enough space to insert the option. You must enable trace on level 170 to determine the cause.
DEL REMID	Shows on how many packets the remote ID was removed for that interface. This number increases every time the relay removes a remote id sub-option from an option82 packet received on an interface towards a server.

```
Switch:1>show ip dhcp-relay counters option82
=====
```

DHCP Counters Option82 - GlobalRouter									
INTERFACE	IP ADDR	FOUND OP82	DROP PKT	CIRC ID	ADD CIRC	DEL CIRC	REMOTE ID	ADD REMID	DEL REMID
Port 1/12	192.0.1.10	0	0	395	0	0	00:24:7f:9d:0a:00	0	0
Vlan40	192.0.1.20	0	0	2088	0	0	00:24:7f:9d:0a:01	0	0

## show ip dhcp-relay fwd-path

Display information about Dynamic Host Configuration Protocol (DHCP) relay forward paths.

### Syntax

- **show ip dhcp-relay fwd-path**
- **show ip dhcp-relay fwd-path [vrf WORD<1-16>]**
- **show ip dhcp-relay fwd-path [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip dhcp-relay fwd-path [vrfids WORD<0-512>]**

### Command Parameters

**vrf WORD<1-16>**

Specifies the name of the VRF.

**vrfids <0-512>**

Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

### Default

None.

### Command Mode

User EXEC

### Command Output

The **show ip dhcp-relay fwd-path** command displays the following information:

Output field	Description
INTERFACE	Shows the VLAN or port associated with the respective relay interface.
SERVER	Specifies the server address.
ENABLE	Specifies if the DHCP-relay forwarding path from the client to the server is enabled on the switch.

Output field	Description
MODE	Indicates the configured mode of this interface.
SRC PORT 67  <b>Note:</b> Exception: not supported on VSP 8600 Series.	Specifies that the UDP source port is 67 for BOOTP/DHCP relay request. The default is 68.

## Example

The following example displays information about DHCP Relay forward paths.

```
Switch:1> show ip dhcp-relay fwd-path
```

```
=====
                        DHCP Fwd-path - GlobalRouter
=====
INTERFACE          SERVER          ENABLE    MODE          SRC PORT 67
-----
3.3.3.3            4.4.4.1        FALSE    DHCP & BOOTP  TRUE
```

## show ip dhcp-relay interface

Display information about the Dynamic Host Configuration Protocol (DHCP) relay configuration for specific interface(s).

## Syntax

- **show ip dhcp-relay interface**
- **show ip dhcp-relay interface [gigabitethernet]**
- **show ip dhcp-relay interface [gigabitethernet] <1-4059>**
- **show ip dhcp-relay interface [gigabitethernet] <1-4059> [vrf WORD<1-16>]**
- **show ip dhcp-relay interface [gigabitethernet] <1-4059> [vrfids WORD<0-512>]**
- **show ip dhcp-relay interface [gigabitethernet] <1-4059> {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **show ip dhcp-relay interface [gigabitethernet] [vrf WORD<1-16>]**
- **show ip dhcp-relay interface [gigabitethernet] [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip dhcp-relay interface [gigabitethernet] [vrfids WORD<0-512>]**
- **show ip dhcp-relay interface [gigabitethernet] {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **show ip dhcp-relay interface [gigabitethernet] {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} [vrf WORD<1-16>]**



- `show ip dhcp-relay interface [gigabitethernet] {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} [vrf WORD<1-16>] [vrfids WORD<0-512>]`
- `show ip dhcp-relay interface [gigabitethernet] {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} [vrfids WORD<0-512>]`
- `show ip dhcp-relay interface [vlan]`
- `show ip dhcp-relay interface [vlan] [<1-4059>]`
- `show ip dhcp-relay interface [vrf WORD<1-16>]`
- `show ip dhcp-relay interface [vrf WORD<1-16>] [vrfids WORD<0-512>]`
- `show ip dhcp-relay interface [vrfids WORD<0-512>]`

## Command Parameters

`gigabitethernet` {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

`vlan` <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

`vrf WORD<1-16>`

Specifies the name of the VRF.

`vrfids <0-512>`

Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip dhcp-relay interface** command displays the following information:

Output field	Description
PORT NUM	Indicates the port number.
VRF NAME	Identifies the VRF name of the DHCP relay interface.
ENABLE	Specifies if the DHCP-relay interface from the client to the server is enabled on the switch
MAX HOP	Configures the maximum number of hops before a DHCP packet is discarded (1 to 16). The default is 4. To configure this option to the default value, use the default operator with this command.
MIN SEC	Configures the minimum seconds count for DHCP. If the secs field in the DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped (0 to 65535). The default is 0 seconds. To configure this option to the default value, use the default operator with this command.
MODE	Configures DHCP mode to forward DHCP messages only.
ALWAYS BCAST	specifies the dhcp-relay interface instance is located on bcast.
CIRCUIT ID	Show the circuit ID associated with the respective interface.
REMOTE ID	Shows the remote ID associated with the respective interface.
TRUST CIRC	Configures the DHCP circuit as trusted.

## show ip dhcp-snooping

Displays DHCP Snooping global configuration.

### Syntax

- **show ip dhcp-snooping**
- **show ip dhcp-snooping vlan <1-4059>**
- **show ip dhcp-snooping vrf WORD<1-16>**
- **show ip dhcp-snooping vrfids WORD<0-512>**

### Command Parameters

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the name of the VRF.

**vrfids <0-512>**

Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

---

## show ip dhcp-snooping binding

Displays DHCP Snooping binding table information.

## Syntax

- **show ip dhcp-snooping binding**
- **show ip dhcp-snooping binding vlan <1-4059>**
- **show ip dhcp-snooping binding vrf WORD<1-16>**
- **show ip dhcp-snooping binding vrfids WORD<0-512>**

## Command Parameters

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the name of the VRF.

**vrfids <0-512>**

Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

---

## show ip dhcp-snooping binding address

---

Displays DHCP Snooping binding table information based on address type.

### Syntax

- **show ip dhcp-snooping binding address {A.B.C.D}**
- **show ip dhcp-snooping binding address 0x00:0x00:0x00:0x00:0x00:0x00**

### Command Parameters

{A.B.C.D}

Displays DHCP Snooping binding table information for the specified IP address.

0x00:0x00:0x00:0x00:0x00:0x00

Displays DHCP Snooping binding table information for the specified MAC address.

### Default

None

### Command Mode

User EXEC

---

## show ip dhcp-snooping binding interface

---

Displays DHCP Snooping binding table information based on interface type.

### Syntax

- **show ip dhcp-snooping binding interface**
- **show ip dhcp-snooping binding interface gigabitEthernet**
- **show ip dhcp-snooping binding interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show ip dhcp-snooping binding interface vlan <1-4059>**
- **show ip dhcp-snooping binding interface vrf vrfids WORD<0-512>**
- **show ip dhcp-snooping binding interface vrf WORD<1-16>**

### Command Parameters

gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Displays DHCP Snooping binding table information for the specified port number.

vlan <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Displays DHCP Snooping binding table information for the specified VRF name.

**vrfids WORD<0-512>**

Displays DHCP Snooping binding table information for the specified VRF ID.

## Default

None

## Command Mode

User EXEC

## show ip dhcp-snooping binding summary

---

Displays DHCP Snooping binding table summary.

## Syntax

- **show ip dhcp-snooping binding summary**
- **show ip dhcp-snooping binding summary {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ip dhcp-snooping binding summary <1-4059>**
- **show ip dhcp-snooping binding summary vrf WORD<1-16>**
- **show ip dhcp-snooping binding summary vrfids WORD<0-512>**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Displays DHCP Snooping binding table summary for the specified port number.

<1-4059>

Displays DHCP Snooping binding table summary for the specified VLAN.

**vrf WORD<1-16>**

Displays DHCP Snooping binding table summary for a particular VRF.

**vrfids WORD<0-512>**

Displays DHCP Snooping binding table summary for a particular VRF ID.

## Default

None

## Command Mode

User EXEC

---

## show ip dhcp-snooping binding type

Displays DHCP Snooping binding table information based on entry type.

## Syntax

- **show ip dhcp-snooping binding type dynamic**
- **show ip dhcp-snooping binding type static**

## Command Parameters

### dynamic

Displays DHCP Snooping binding table information for dynamic entries.

### static

Displays DHCP Snooping binding table information for static entries.

## Default

None

## Command Mode

User EXEC

---

## show ip dhcp-snooping interface

Displays DHCP Snooping interface configuration.

## Syntax

- **show ip dhcp-snooping interface**
- **show ip dhcp-snooping interface vlan**
- **show ip dhcp-snooping interface vlan <1-4059>**
- **show ip dhcp-snooping interface vrf WORD<1-16>**
- **show ip dhcp-snooping interface vrfids WORD<0-512>**

## Command Parameters

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf** WORD<1-16>

Displays DHCP Snooping configuration for a particular VRF.

**vrfids** WORD<0-512>

Displays DHCP Snooping configuration for a particular VRF ID.

## Default

None

## Command Mode

User EXEC

## show ip dhcp-snooping interface gigabitEthernet

---

Displays DHCP Snooping configuration on the port.

## Syntax

- **show ip dhcp-snooping interface gigabitEthernet**
- **show ip dhcp-snooping interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} vrf WORD<1-16>**
- **show ip dhcp-snooping interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} vrfids WORD<0-512>**
- **show ip dhcp-snooping interface gigabitEthernet <1-4059> vrf WORD<1-16>**
- **show ip dhcp-snooping interface gigabitEthernet <1-4059> vrfids WORD<0-512>**
- **show ip dhcp-snooping interface gigabitEthernet vrf WORD<1-16>**
- **show ip dhcp-snooping interface gigabitEthernet vrfids WORD<0-512>**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]][,...]}

Displays DHCP Snooping configuration for a particular port.

<1-4059>

Displays the DHCP Snooping VLAN configuration.

**vrf WORD<1-16>**

Displays DHCP Snooping configuration for a particular VRF.

**vrfids WORD<0-512>**

Displays DHCP Snooping configuration for a particular VRF ID.

## Default

None

## Command Mode

User EXEC

## show ip directed-broadcast

---

Show the interface status for direct broadcast.

## Syntax

- **show ip directed-broadcast interface**
- **show ip directed-broadcast interface GigabitEthernet**
- **show ip directed-broadcast interface GigabitEthernet {slot/port[sub-port]}**
- **show ip directed-broadcast interface GigabitEthernet {slot/port[sub-port]}**

## Command Parameters

**interface GigabitEthernet {slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the subport in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## show ip directed-broadcast vlan

---

Displays Vlan IDs with directed broadcast enabled.



## Syntax

- **show ip directed-broadcast vlan**

## Default

None

## Command Mode

User EXEC

## show ip dns

---

View the DNS client system status.

The **show sys dns** command returns the same output.

## Syntax

- **show ip dns**

## Default

None

## Command Mode

User EXEC

## show ip ecmp

---

Display the prefix list of routes with number of ECMP paths.

## Syntax

- **show ip ecmp max-path**
- **show ip ecmp max-path vrf WORD<1-16>**
- **show ip ecmp max-path vrfids WORD<0-512>**
- **show ip ecmp pathlist-1**
- **show ip ecmp pathlist-1 vrf WORD<1-16>**
- **show ip ecmp pathlist-1 vrfids WORD<0-512>**
- **show ip ecmp pathlist-2**
- **show ip ecmp pathlist-2 vrf WORD<1-16>**
- **show ip ecmp pathlist-2 vrfids WORD<0-512>**
- **show ip ecmp pathlist-3**

- `show ip ecmp pathlist-3 vrf WORD<1-16>`
- `show ip ecmp pathlist-3 vrfids WORD<0-512>`
- `show ip ecmp pathlist-4`
- `show ip ecmp pathlist-4 vrf WORD<1-16>`
- `show ip ecmp pathlist-4 vrfids WORD<0-512>`
- `show ip ecmp pathlist-5`
- `show ip ecmp pathlist-5 vrf WORD<1-16>`
- `show ip ecmp pathlist-5 vrfids WORD<0-512>`
- `show ip ecmp pathlist-6`
- `show ip ecmp pathlist-6 vrf WORD<1-16>`
- `show ip ecmp pathlist-6 vrfids WORD<0-512>`
- `show ip ecmp pathlist-7`
- `show ip ecmp pathlist-7 vrf WORD<1-16>`
- `show ip ecmp pathlist-7 vrfids WORD<0-512>`
- `show ip ecmp pathlist-8`
- `show ip ecmp pathlist-8 vrf WORD<1-16>`
- `show ip ecmp pathlist-8 vrfids WORD<0-512>`

## Command Parameters

### max-path

Configures the maximum number of Equal Cost Multipath (ECMP) paths.

### vrf WORD<1-16>

Displays the prefix list of routes for a particular VRF. WORD<1-16> specifies the VRF name.

### vrfids WORD<0-512>

Displays the prefix list of routes for a particular VRF ID. WORD<0-512> specifies the VRF ID.

## Default

None

## Command Mode

User EXEC

## show ip extcommunity-list

---

Show extended community list information.

## Syntax

- `show ip extcommunity-list`
- `show ip extcommunity-list <1-1024>`
- `show ip extcommunity-list <1-1024> vrf WORD<1-16>`
- `show ip extcommunity-list <1-1024> vrfids WORD<0-512>`
- `show ip extcommunity-list vrf WORD<1-16>`
- `show ip extcommunity-list WORD<0-512>`

## Command Parameters

`<1-1024>`

Specifies the extended community list ID.

`vrf WORD<1-16>`

Displays extended community list for a particular VRF.

`vrfids WORD<0-512>`

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip forward-protocol udp

---

Display the UDP protocol table with the UDP port numbers for each supported or designated protocol.

## Syntax

- `show ip forward-protocol udp`
- `show ip forward-protocol udp [vrf WORD<1-16>] [vrfids <0-512>]`
- `show ip forward-protocol udp interface`
- `show ip forward-protocol udp interface {A.B.C.D}`
- `show ip forward-protocol udp interface vrf WORD<1-16>`
- `show ip forward-protocol udp interface vrfids WORD<0-512>`
- `show ip forward-protocol udp vrf WORD<1-16>`
- `show ip forward-protocol udp vrfids WORD<0-512>`

## Command Parameters

`interface <A.B.C.D>`

Displays information about the UDP interface for all IP addresses or a specified IP address.

**portfwd**

Displays the UDP port forwarding table.

**portfwdlist <1-1000>**

Displays the UDP port forwarding list table for the specified list or all lists on the switch. <1-1000> specifies the port forward list ID.

**vrf WORD<1-16>**

Specifies the name of the VRF in the range of 0 to 16 characters.

**vrfids <0-512>**

Specifies the ID of the port and is an integer in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

## show ip forward-protocol udp portfwd

---

View and confirm the port forward entry configuration.

## Syntax

- **show ip forward-protocol udp portfwd**
- **show ip forward-protocol udp portfwd [vrf WORD<1-16>] [vrfids <0-512>]**

## Command Parameters

**vrf WORD<1-16>**

Specifies the name of the VRF in the range of 0 to 16 characters.

**vrfids <0-512>**

Specifies the ID of VRF and is an integer between 0 and 512.

## Default

None

## Command Mode

User EXEC

## show ip forward-protocol udp portfwddlist

---

View and confirm the configuration setting on the IP forwarding list.

### Syntax

- `show ip forward-protocol udp portfwddlist`
- `show ip forward-protocol udp portfwddlist <1-1000>`
- `show ip forward-protocol udp portfwddlist <1-1000> [vrf WORD<1-16>]  
[vrfids <0-512>]`
- `show ip forward-protocol udp portfwddlist vrf WORD<1-16>`
- `show ip forward-protocol udp portfwddlist vrfids WORD<0-512>`

### Command Parameters

`<1-1000>`

Specifies the port forward list id which is an integer in the range of 1 to 1000.

`vrf WORD<1-16>`

Specifies the name of the VRF in the range of 0 to 16 characters.

`vrfids <0-512>`

Specifies the ID of the port and is an integer in the range of 0 to 512.

### Default

None

### Command Mode

User EXEC

## show ip global

---

Display the global IPv4 configuration information.

### Syntax

- `show ip global`
- `show ip global vrf WORD<1-16>`
- `show ip global vrfids WORD<0-512>`

### Command Parameters

`vrf WORD<1-16>`

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Examples

The following example displays information of ICMP drop packet filtering for IPv4 network:

```
Switch:1>show ip global
```

```
=====
                                     IPv4 Global Information - GlobalRouter
                                     =====
icmp-drop-fragments                   : disable
```

## show ip icmp statistics

Show the collective IPv4 ICMP statistics for all VRF instances.

## Syntax

- **show ip icmp statistics**

## Default

None

## Command Mode

User EXEC

## show ip interface

Shows the IP configuration for an interface.

## Syntax

- **show ip interface**
- **show ip interface gigabitethernet**
- **show ip interface gigabitethernet <1-4059>**
- **show ip interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**
- **show ip interface vrf WORD<1-16>**
- **show ip interface vrfids WORD<0-512>**

## Command Parameters

**<1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the name of the VRF.

**vrfids WORD <0-512>**

Specifies the VRF ID in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip interface** command displays the following information:

Output field	Description
INTERFACE	Indicates the slot and port for the management port.
IP ADDRESS	Indicates the IP address for the management port.
NET MASK	Indicates a subnet mask of an IP address.
BCASTADDR FORMAT	Indicates the broadcast address format for the management port.
REASM MAXSIZE	Indicates the size of the largest IP packet that can be reassembled from IP fragmented packets received on the management port.
VLAN ID	Indicates the VLAN ID of the management port.

Output field	Description
BROUTER PORT	Indicates whether the management port is a brouter port or a routeable VLAN.
IPSEC STATE	Indicates whether the IPsec policy is enabled on the interface.
IP NAME	Indicates the IP name given to the IP address.

## Example

The following example displays the command output.

```
Switch:1>show ip interface
=====
                        IP Interface - GlobalRouter
=====
INTERFACE  IP          NET          BCASTADDR  REASM      VLAN  BROUTER  IPSEC  IP
ADDRESS    MASK                FORMAT      MAXSIZE    ID    PORT    STATE  NAME
-----
Clip1      1.2.3.4    255.255.0.0  ones        1500      --    false    disable testing123
Clip2      2.3.4.5    255.255.255.0 ones        1500      --    false    disable testing451

All 2 out of 2 Total Num of IP interfaces displayed
```

## show ip ipfix

Display IPFIX global status.

### Syntax

- **show ip ipfix**

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show ip ipfix collector

Display information about the IPFIX collector.



## Syntax

- **show ip ipfix collector <1-1>**

## Command Parameters

<1-1>

Specifies the IPFIX collector ID.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## show ip ipfix flows

Display information about IPFIX flows.

## Syntax

- **show ip ipfix flows**
- **show ip ipfix flows source-addr {A.B.C.D} dest-addr {A.B.C.D} source-port <1-65535> dest-port <1-65535> protocol { udp | tcp } in-port { rx-nni | {slot/port[/sub-port]}}**
- **show ip ipfix flows source-addr {A.B.C.D} dest-addr {A.B.C.D} source-port <1-65535> dest-port <1-65535> protocol { udp | tcp } in-vrf <0-511> {in-vlan <1-4095> | untagged} ip-ttl <0-255>**

## Command Parameters

**dest-addr {A.B.C.D}**

Specifies an IP address for the flow destination.

**dest-port <1-65535>**

Specifies a value for the destination port.

**in-port <rx-nni | {slot/port[/sub-port]}>**

Identifies the port that learns the flow.

**in-vlan <1-4095> >**

Specifies an ingress VLAN ID for the flow.

**in-vrf <0-511> >**

Specifies the IP time-to-live (TTL) for the flow.

**ip-ttl <0-255>**

Specifies the IP time-to-live (TTL) for the flow.

**protocol {udp | tcp}**

Specifies the transport protocol.

**source-addr {A.B.C.D}**

Specifies an IP address for the flow source.

**source-port <1-65535>**

Specifies a value for the source port.

**untagged**

Specifies ingress untagged flows.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

The *in-port* parameter is only supported on VSP 7400 Series.

The *in-vlan*, *in-vrf*, *ip-ttl*, and *untagged* parameters are only supported on 5420 Series and 5520 Series.

## show ip ipvpn

---

Display the configuration for IP VPN enabled VRFs.

## Syntax

- **show ip ipvpn [vrf WORD<1-16>] [vrfids WORD<0-512>]**

## Command Parameters

vrf WORD<1-16>

Specifies a VRF.

**vrfids WORD<0-512>**

Specifies the VRF ID.

## Default

None

## Command Mode

User EXEC

## Example

The following example displays the command output.

```
Switch:1#show ip ipvpn
=====
                                     IPv4  IPVPN
-----
VRF Name          VRF ID   IPv4  IPVPN   IPv6  IPVPN   I-SID   I-SID Name
-----
green              1        enabled  disabled  109   ExtremeServer1
-----
1 out of 1 Total IPv4 L3 VSN, 1 active IPv4 and 0 active IPv6 displayed.
```

## show ip isid-list

Displays I-SID list information.

## Syntax

- **show ip isid-list**
- **show ip isid-list vrf WORD<1-16>**
- **show ip isid-list WORD<1-32>**
- **show ip isid-list WORD<1-32> vrf WORD<1-16>**

## Command Parameters

**vrf WORD<1-16>**

Displays I-SID list information for a particular VRF by name.

**WORD<1-32>**

Displays I-SID list information for a particular I-SID list by name.

## Default

None

## Command Mode

User EXEC

## show ip isis redistribute

---

Display the redistribution configuration.

### Syntax

- **show ip isis redistribute**
- **show ip isis redistribute vrf WORD<1-16>**
- **show ip isis redistribute vrf WORD<1-16> vrfids WORD<0-512>**
- **show ip isis redistribute vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a particular VRF. Type a name between 0-16 characters in length.

**vrfids WORD<0-512>**

Specifies the VRF ID.

### Default

None

## Command Mode

User EXEC

## show ip mroute hw-resource-usage

---

View multicast hardware resource usage. The range of values depends on the hardware platform.

### Syntax

- **show ip mroute hw-resource-usage**
- **show ip mroute hw-resource-usage vrf WORD<1-16>**
- **show ip mroute hw-resource-usage vrf WORD<1-32>**
- **show ip mroute hw-resource-usage vrfids WORD<0-255>**
- **show ip mroute hw-resource-usage vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-32> | vrf WORD<1-16>**

Specifies a VRF by name. Range depends on hardware platform.

**vrfids WORD <0-255> | vrfids WORD <0-512>**

Specifies a VRF by ID. Range depends on hardware platform.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command is not supported on a node configured as the DVR Leaf within a DVR domain.

## Command Output

The **show ip mroute hw-resource-usage** command displays the following information:

Output field	Description
EGRESS REC IN-USE	Displays the number of egress records traversing the switch.
INGRESS REC IN-USE	Displays the number of ingress records (source or group) traversing the switch.
EGRESS THRESHOLD	Displays the configured egress threshold level. A notification message is sent if this value is exceeded. The default is 0.
INGRESS THRESHOLD	Displays the configured ingress threshold level. A notification message is sent if this value is exceeded. The default is 0.
LOG MSG ONLY	Displays whether only log notification messages are sent after the threshold level is exceeded. The default is false (disabled).
SEND TRAP ONLY	Displays whether only trap notification messages are sent after the threshold level is exceeded. The default is false (disabled).
SENT TRAP AND LOG	Displays whether both trap and log notification messages are sent after the threshold level is exceeded. The default is false (disabled).

## Example

The following example displays the hardware resource usage.

```
Switch:1>show ip mroute hw-resource-usage
=====
Multicast Hardware Resource Usage
=====
```

EGRESS	INGRESS	EGRESS	INGRESS	LOG MSG	SEND TRAP	SEND TRAP
REC IN-USE	REC IN-USE	THRESHOLD	THRESHOLD	ONLY	ONLY	AND LOG
0	0	0	0	false	false	false

## show ip mroute interface

Display information about the interface for the multicast routes set up on the switch. The range of values depends on the hardware platform.

### Syntax

- **show ip mroute interface**
- **show ip mroute interface gigabitethernet**
- **show ip mroute interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show ip mroute interface vrf WORD<1-16>**
- **show ip mroute interface vrf WORD<1-32>**
- **show ip mroute interface vrfids WORD<0-255>**
- **show ip mroute interface vrfids WORD<0-512>**

### Command Parameters

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vrf WORD<1-32> | vrf WORD<1-16>**

Specifies a VRF by name. Range depends on hardware platform.

**vrfids WORD <0-255> | vrfids WORD <0-512>**

Specifies a VRF ID. Range depends on hardware platform.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command is not supported on a node configured as the DvR Leaf within a DvR domain.

The following message displays if the system shuts down the port due to excessive multicast streams:

```
Shutdown port <port> due to excessive multicast streams <# of streams
ingressed>; Configured limit max streams <configured limit> in
<configured sampling interval> sec. Please disable and re-enable the
port.
```

## Command Output

The **show ip mroute interface** command displays the following information:

Output field	Description
INTERFACE	Indicates the interface.
TTL	Indicates the datagram TTL threshold for the interface. IP multicast datagrams with a TTL less than this threshold are not forwarded out of the interface. The default value of 0 means all multicast packets are forwarded out of the interface.
PROTOCOL	Indicates the routing protocol running on this interface.
PORT	Shows the slot and port location.
MROUTE STR LIMIT	Indicates the maximum number of multicast streams that can enter the CPU through this port.
MROUTE STR LIMIT TMR	Indicates the sampling period (in seconds) to check number of multicast streams that enter the CPU through this port.
ENABLE	Indicates the status of the mroute stream limit on the port.

## show ip mroute next-hop

Display information about the next hop for the multicast routes set up on the switch. The range of values depends on the hardware platform.

### Syntax

- **show ip mroute next-hop**
- **show ip mroute next-hop vrf WORD<1-16>**
- **show ip mroute next-hop vrf WORD<1-32>**
- **show ip mroute next-hop vrfids WORD<0-255>**
- **show ip mroute next-hop vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-32> | vrf WORD<1-16>**

Specifies a VRF by name. Range depends on hardware platform.

**vrfids WORD <0-255> | vrfids WORD <0-512>**

Specifies a VRF by ID. Range depends on hardware platform.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip mroute next-hop** command displays the following information:

Output field	Description
INTERFACE	Indicates the interface identity.
GROUP	Indicates the IP multicast group for which this entry specifies a next-hop PIM neighbor toward receivers for a specific outgoing interface.
SOURCE	Indicates the network address, which when combined with the corresponding value of SRCMASK, identifies the sources for which this entry specifies a next-hop PIM neighbor toward receivers for a specific outgoing interface.
SRCMASK	Indicates the network mask, which when combined with the corresponding value of SOURCE, identifies the sources for which this entry specifies a next-hop PIM neighbor toward receivers for a specific outgoing interface.
ADDRESS	Indicates the address of the next hop specific to this entry. The next hop must be the address of a PIM neighbor. This table does not represent local receivers.
STATE	Indicates whether the outgoing interface and next hop represented by this entry currently forward IP datagrams. The value forwarding indicates the information is currently used; the value pruned indicates it is not used.
EXPTIME	Indicates the minimum amount of time that remains before this entry ages out. The value 0 indicates that the entry is not subject to aging.
CLOSEHOP	Indicates the minimum number of hops between this router and members of this IP multicast group reached through this next hop on this outgoing interface. IP multicast datagrams for the group that use a time-to-live less than this number of hops are forwarded to the next hop
PROTOCOL	Indicates the routing mechanism through which the switch learned this next hop.
L2ISID	Indicates the I-SID associated with the Layer 2 interface.

## show ip mroute route

Display information about the multicast routes set up on the switch. The range of values depends on the hardware platform.



## Syntax

- **show ip mroute route**
- **show ip mroute route vrf WORD<1-16>**
- **show ip mroute route vrf WORD<1-32>**
- **show ip mroute route vrfids WORD<0-255>**
- **show ip mroute route vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-32> | vrf WORD<1-16>**

Specifies a VRF by name. Range depends on hardware platform.

**vrfids WORD <0-255> | vrfids WORD <0-512>**

Specifies a VRF by ID. Range depends on hardware platform.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command is not supported on a node configured as the DvR Leaf within a DvR domain.

In this output, every stream uses one (\*,G) entry and x (S,G) entries, depending on how many servers forward traffic to the same group.

The 0.0.0.0 mask is always tied to a (\*,G) entry.

Every time a new stream comes in, Protocol Independent Multicast (PIM) creates two entries in the table; one is a (\*,G) entry that points toward the rendezvous point (RP) router, and the other is an (S,G) entry that points toward the source.

## Command Output

The **show ip mroute route** command displays the following information:

Output field	Description
GROUP	Indicates the IP multicast group for this multicast route.
SOURCE	Indicates the network address that, when combined with the corresponding value of SRCMASK, identifies the sources for this multicast route.

Output field	Description
SRCMASK	Indicates the network mask that, when combined with the corresponding value of SOURCE, identifies the sources for this multicast route.
UPSTREAM_NBR	Indicates the address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received, or 0.0.0.0 if the (S,G) source is local or if the RP for this the (*,G) group is an address on this router.
IF	Indicates the value of ifIndex for the interface that receives IP datagrams sent by these sources to this multicast address. A value of 0 in a (*,G) route indicates that datagrams are not subject to an incoming interface check, but datagrams can be received on any interface.
EXPIR	Indicates the minimum amount of time remaining before this entry ages out. The value 0 indicates that the entry is not subject to aging.  <b>Note:</b> The value you configure for fwd-cache-timeout applies only to the locally learned sender; it does not apply to SMLT synchronized sender records.
PROT	Indicates the multicast protocol through which the switch learned this route.

## Example

The following example displays information about the multicast routes on the switch.

```
Switch:1>show ip mroute route

=====
Mroute Route - GlobalRouter
=====
GROUP          SOURCE          SRCMASK          UPSTREAM_NBR    IF      EXPIR  PROT
-----
233.252.0.1    0.0.0.0         0.0.0.0         0.0.0.0         V3      30     spb-access
233.252.0.1    192.0.2.102    255.255.255.0   0.0.0.0         -       0      spb-network
233.252.0.2    0.0.0.0         0.0.0.0         0.0.0.0         V2      30     pimsm
225.1.1.1      198.51.100.99  255.255.255.0   0.0.0.0         V3      173    spb-pim-gw

Total 4
```

## show ip mroute static-source-group

Display information about the static source groups on the current interface. The range of values depends on the hardware platform.

## Syntax

- **show ip mroute static-source-group**
- **show ip mroute static-source-group <A.B.C.D>**
- **show ip mroute static-source-group <A.B.C.D> vrf WORD<1-16>**

- **show ip mroute static-source-group <A.B.C.D> vrf WORD<1-32>**
- **show ip mroute static-source-group <A.B.C.D> vrfids WORD<0-255>**
- **show ip mroute static-source-group <A.B.C.D> vrfids WORD<0-512>**

## Command Parameters

<A.B.C.D>

Specifies the group IP address.

vrf WORD<1-32> | vrf WORD<1-16>

Specifies a VRF by name. Range depends on hardware platform.

vrfids WORD <0-255> | vrfids WORD <0-512>

Specifies a VRF by ID. Range depends on hardware platform.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command is not supported on a node configured as the DvR Leaf within a DvR domain.

You can use this command to see all valid entries that were created. If an entry is created with a x bit mask, it shows as a x bit in the output.

## Command Output

The **show ip mroute static-source-group** command displays the following information:

Output field	Description
Group Address	Indicates the IP multicast group address.
Source Address	Indicates the network address.
Subnet Mask	Indicates the network mask.

## show ip mroute stats

Display IP multicast route statistics.

## Syntax

- **show ip mroute stats**

- **show ip mroute stats** [WORD<3-160> {A.B.C.D[,E.F.G.H][,...]}]

## Command Parameters

WORD<3-160> {A.B.C.D[,E.F.G.H][,...]}

Displays the IP multicast route statistics.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip mroute stats** command displays the following information:

Output field	Description
GroupAddress	Specifies the multicast group IP address for which to show statistics.
SourceCounter	Specifies the number of sources associated with the multicast route record.
IngressPackets	Specifies the number of packets received for the associated IP address.
IngressBytes	Specifies the number of bytes received for the associated IP address.
AverageSize	Specifies the average packet length for the associated group IP address. This information indicates only the ingress packet length and is calculated using the formula: ingress packet/ingress byte.

## show ip ospf accept

Display information about the configured OSPF entries.

## Syntax

- **show ip ospf accept**
- **show ip ospf accept vrf** WORD<1-16>
- **show ip ospf accept vrfids** WORD<0-512>

## Command Parameters

vrf ids WORD<0-512>

Specifies the ID of the VRF.

**vrf WORD<1-16>**

Specifies the name of the VRF.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip ospf accept** command displays the following information:

Output field	Description
ADV_RTR	Indicates the router advancing the packets.
MET_TYPE	Indicates the metric type for the routes to import into OSPF routing protocol, which passed the matching criteria configured in this route policy. Options include: local, internal, external, externaltype1, and externaltype2.
ENABLE	Indicates if the policy is enabled.
POLICY	Indicates the type of policy.

## Example

The following example displays information about the configured OSPF entries.

```
Switch:1#show ip ospf accept
=====
                        Ospf Accept - GlobalRouter
=====
ADV_RTR      MET_TYPE  ENABLE  POLICY
-----
192.0.2.11   type1    true    test1
```

## show ip ospf area

Display OSPF area information to ensure accuracy.

## Syntax

- **show ip ospf area**
- **show ip ospf area vrf WORD<1-16>**
- **show ip ospf area vrfids WORD<0-512>**

## Command Parameters

**vrf WORD <1-16>**

Specifies a VRF by name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip ospf area-range

---

Display OSPF area range configuration information to ensure accuracy.

## Syntax

- **show ip ospf area-range**
- **show ip ospf area-range vrf <WORD 1-16>**
- **show ip ospf area-range vrfids <WORD 0-512>**

## Command Parameters

**vrf <WORD 1-16>**

Specifies a VRF by name.

**vrfids <WORD 0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip ospf ase

---

View the link-state database to determine externally learned routing information.

## Syntax

- **show ip ospf ase**
- **show ip ospf ase metric-type**
- **show ip ospf ase metric-type <1-2>**
- **show ip ospf ase vrf WORD<1-16>**
- **show ip ospf ase vrfids WORD<0-512>**

## Command Parameters

**metric-type <1-2>**

Specifies the metric type as a string of 1 to 2 characters.

**vrf WORD<1-16>**

Identifies the VRF by name.

**vrfids WORD<0-512>**

Specifies a VRF by ID.

## Default

None

## Command Mode

User EXEC

# show ip ospf authentication

---

Display OSPF authentication information to ensure accuracy.

## Syntax

- **show ip ospf authentication interface**
- **show ip ospf authentication interface gigabitethernet**
- **show ip ospf authentication interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show ip ospf authentication interface vlan**
- **show ip ospf authentication interface vlan <1-4059>**

## Command Parameters

**interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

---

## show ip ospf default-cost

Display OSPF default cost information to ensure accuracy.

## Syntax

- **show ip ospf default-cost**
- **show ip ospf default-cost vrf** WORD<1-16>
- **show ip ospf default-cost vrfids** WORD<0-512>

## Command Parameters

**vrf** WORD<1-16>

Specifies a VRF by name.

**vrfids** WORD<0-512>

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

---

## show ip ospf host-route

Display the host route OSPF information to ensure accuracy.



## Syntax

- **show ip ospf host-route**
- **show ip ospf host-route vrf WORD<1-16>**
- **show ip ospf host-route vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip ospf ifstats

---

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

## Syntax

- **show ip ospf ifstats**
- **show ip ospf ifstats detail [vrf WORD <1-16>] [vrfids WORD<0-512>]**
- **show ip ospf ifstats mismatch [vrf WORD <1-16>] [vrfids WORD<0-512>]**
- **show ip ospf ifstats vlan <1-4059>**
- **show ip ospf ifstats vrf WORD<1-16>**
- **show ip ospf ifstats vrfids WORD<0-512>**

## Command Parameters

**detail**

Displays the details of the OSPF.

**mismatch**

Specifies the number of times the area ID is not matched.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags,

the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF instance by VRF name.

**vrfids WORD<0-512>**

Specifies a VRF or range of VRFs by ID.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip ospf ifstats** command displays the following information:

Field	Description
INTERFACE	Indicates the IP address of the host.
HELLOS RX	Indicates the number of hello packets received by this interface.
HELLOS TX	Indicates the number of hello packets transmitted by this interface.
DBS RX	Indicates the number of database descriptor packets received by this interface.
DBS TX	Indicates the number of database descriptor packets transmitted by this interface.
LS REQ RX	Indicates the number of link state request packets received by this interface.
LS REQ TX	Indicates the number of link state request packets transmitted by this interface.
LS UDP RX	Indicates the number of link state update packets received by this interface.
LS UDP TX	Indicates the number of link state update packets transmitted by this interface.
LS ACK RX	Indicates the number of link state acknowledge packets received by this interface.
LS ACK TX	Indicates the number of link state acknowledge packets transmitted by this interface.
VERSION	Indicates the OSPF version.
AREA	Indicates the OSPF area.
AUTHTYPE	Indicates the OSPF authentication type.
AUTHFAIL	The count of authentication fail messages.

Field	Description
NETMASK	Indicates the net mask.
HELLO	The count of Hello messages.
DEADTRR OPTION	The dead TRR option.

## Example

```
Switch:1#show ip ospf ifstats
=====
                        OSPF Interface Statistics - GlobalRouter
=====
---HELLOS---  ---DBS---  -LS REQ--  --LS UPD---  --LS ACK---
INTERFACE      RX      TX      RX  TX      RX  TX      RX  TX      RX  Tx
-----
192.0.2.3      76035  76355  33  32      4   9      2483  2551  2525  1247
192.0.2.8      76038  76349  0   0       0   0       0     0     0     0
```

## show ip ospf int-auth

Display OSPF authentication information to ensure accuracy.

### Syntax

- **show ip ospf int-auth**
- **show ip ospf int-auth [vrf WORD <1-16>] [vrfids WORD<0-512>]**
- **show ip ospf int-auth vrf WORD<1-16>**
- **show ip ospf int-auth vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Displays ospf authentication configuration for a particular VRF.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

### Default

None

### Command Mode

User EXEC

## show ip ospf interface

Display OSPF information on a particular interface to ensure accuracy.

## Syntax

- **show ip ospf interface**
- **show ip ospf interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ip ospf interface vlan**
- **show ip ospf interface vlan <1-4059>**
- **show ip ospf interface vrf WORD<1-16>**
- **show ip ospf interface vrfids WORD<0-512>**

## Command Parameters

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Displays ospf configuration for a particular VRF.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

---

## show ip ospf int-timers

Display OSPF timers information to ensure accuracy.

## Syntax

- **show ip ospf int-timers**
- **show ip ospf int-timers [vrf WORD<1-16>] [vrfids WORD<0-512>]**

- **show ip ospf int-timers vrf WORD<1-16>**
- **show ip ospf int-timers vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Displays ospf timer configuration for a particular VRF.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip ospf lsdb

---

View the area advertisements and other information contained in the link-state database (LSD) to ensure correct OSPF operations.

## Syntax

- **show ip ospf lsdb**
- **show ip ospf lsdb [area <A.B.C.D>] [lsa-type <1-11>] [lsid <A.B.C.D>] [adv-rtr <A.B.C.D>] [vrf WORD<1-16>] [vrfids WORD<0-512>] [detail]**
- **show ip ospf lsdb adv-rtr {A.B.C.D}**
- **show ip ospf lsdb adv-rtr {A.B.C.D} vrf WORD<1-16>**
- **show ip ospf lsdb adv-rtr {A.B.C.D} vrfids WORD<0-512>**
- **show ip ospf lsdb area {A.B.C.D}**
- **show ip ospf lsdb area {A.B.C.D} vrf WORD<1-16>**
- **show ip ospf lsdb area {A.B.C.D} vrfids WORD<0-512>**
- **show ip ospf lsdb detail**
- **show ip ospf lsdb detail vrf WORD<1-16>**
- **show ip ospf lsdb detail vrfids WORD<0-512>**
- **show ip ospf lsdb lsa-type <1-11>**
- **show ip ospf lsdb lsa-type <1-11> vrf WORD<1-16>**
- **show ip ospf lsdb lsa-type <1-11> vrfids WORD<0-512>**
- **show ip ospf lsdb lsid {A.B.C.D}**
- **show ip ospf lsdb lsid {A.B.C.D} vrf WORD<1-16>**

- **show ip ospf lsdb lsid {A.B.C.D} vrfids WORD<0-512>**
- **show ip ospf lsdb vrf WORD<1-16>**
- **show ip ospf lsdb vrfids WORD<0-512>**

## Command Parameters

**adv-rtr <A.B.C.D>**

Specifies the advertising router.

**area <A.B.C.D>**

Specifies the OSPF area.

**detail**

Provides detailed output.

**lsa-type <1-11>**

Specifies the link-state advertisement type in the range of 1 to 11.

**lsid <A.B.C.D>**

Specifies the link-state ID.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip ospf neighbor

---

Displays OSPF NBMA neighbor information.

## Syntax

- **show ip ospf neighbor**
- **show ip ospf neighbor [vrf WORD<1-16>] [vrfids WORD <0-512>]**
- **show ip ospf neighbor vrf WORD<1-16>**
- **show ip ospf neighbor vrfids WORD<0-512>**

## Command Parameters

**vrf WORD <1-16>**

Specifies a VRF by name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

# show ip ospf port-error

---

Check OSPF errors for administrative and troubleshooting purposes.

## Syntax

- **show ip ospf port-error**
- **show ip ospf port-error [port <portList>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip ospf port-error port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**
- **show ip ospf port-error port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} vrf WORD<1-16>**
- **show ip ospf port-error port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} vrfids WORD<0-512>**
- **show ip ospf port-error vrf WORD<1-16>**
- **show ip ospf port-error vrfids WORD<0-512>**

## Command Parameters

**port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

# show ip ospf redistribute

---

Displays the OSPF redistribution configuration information.

## Syntax

- **show ip ospf redistribute**
- **show ip ospf redistribute [vrf WORD <1-16>] [vrfids WORD<1-512>]**
- **show ip ospf redistribute vrf WORD<1-16>**
- **show ip ospf redistribute vrfids WORD<0-512>**

## Command Parameters

**vrf WORD <1-16>**

Specifies a VRF by name.

**vrfids WORD <0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

# show ip ospf stats

---

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

## Syntax

- **show ip ospf stats**
- **show ip ospf stats [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip ospf stats vrf WORD<1-16>**
- **show ip ospf stats vrfids WORD<0-512>**



## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF instance by VRF name.

**vrfids WORD<0-512>**

Specifies a VRF or range of VRFs by ID.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip ospf stats** command displays the following information:

Output field	Description
NumBufAlloc	Indicates the number of buffers allocated for OSPF.
NumBufFree	Indicates the number of buffers that are freed by the OSPF.
NumBufAllocFail	Indicates the number of times that OSPF failed to allocate buffers.
NumBufFreeFail	Indicates the number of times that OSPF failed to free buffers.
NumTxPkt	Indicates the number of packets transmitted by OSPF.
NumRxPkt	Indicates the number of packets received by OSPF.
NumTxDropPkt	Indicates the number of packets dropped before transmission by OSPF.
NumRxDropPkt	Indicates the number of packets dropped before reception by OSPF.
NumRxBadPkt	Indicates the number of packets received by OSPF that are bad.
NumSpfRun	Indicates the total number of SPF calculations performed by OSPF, which also includes the number of partial route table calculation for incremental updates.
LastSpfRun	Indicates the time (SysUpTime) since the last SPF calculated by OSPF.
LsdbTblSize	Indicates the number of entries in the link state database table.
NumAllocBdDDP	Indicates the number of times buffer descriptors were allocated for OSPF database description packets.
NumFreeBdDDP	Indicates the number of times buffer descriptors were freed after use as OSPF database description packets.
NumBadLsReq	Indicates the number of bad LSDB requests.
NumSeqMismatch	Indicates the number of mismatches for sequence numbers.
NumOspfRoutes	The count of OSPF routes.

Output field	Description
NumOspfAreas	The count of all OSPF areas.
NumOspfAdjacencies	The count of adjacencies.
NumOspfNbrs	The count of OSPF neighbors.
NumEnabledOspfAreas	The count of OSPF areas with at least one enabled OSPF interface. This number counts against the scaling maximum when you add a new area.

## Example

The following example displays the OSPF performance statistics.

```
Switch:1#show ip ospf stats

=====
                        OSPF Statistics - GlobalRouter
=====
      NumBufAlloc: 1138
      NumBufFree: 1138
NumBufAllocFail: 0
NumBufFreeFail: 0
      NumTxPkt: 1144
      NumRxPkt: 2287
NumTxDropPkt: 0
NumRxDropPkt: 0
NumRxBadPkt: 0
      NumSpfRun: 19
      LastSpfRun: 0 day(s), 00:26:15
      LsdbTblSize: 7
NumAllocBdDDP: 5
NumFreeBdDDP: 5
NumBadLsReq: 0
NumSeqMismatch: 0
NumOspfRoutes: 7
NumOspfAreas: 0
NumOspfAdjacencies: 3
      NumOspfNbrs: 3
NumEnabledOspfAreas:0
```

## show ip ospf virtual-link

Displays the OSPF virtual link information to ensure accuracy.

## Syntax

- **show ip ospf virtual-link {A.B.C.D} {A.B.C.D}**
- **show ip ospf virtual-link {A.B.C.D} {A.B.C.D} [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip ospf virtual-link {A.B.C.D} {A.B.C.D} vrf WORD<1-16>**
- **show ip ospf virtual-link {A.B.C.D} {A.B.C.D} vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D} {A.B.C.D}**

Specifies the area ID and the virtual interface ID. The first IP address specifies the area ID and the second specifies the virtual interface ID.

**vrf WORD<1-16>**

Specifies a VRF by name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip ospf vrf

---

Displays the OSPF configuration for a particular VRF.

## Syntax

- **show ip ospf vrf WORD<1-16>**
- **show ip ospf vrf WORD<1-16> vrfids WORD<0-512>**

## Command Parameters

**vrfids WORD<0-512>**

Specifies the VRF ID.

**WORD<1-16>**

Specifies the VRF name.

## Default

None

## Command Mode

User EXEC

---

## show ip ospf vrfids

---

Displays the OSPF configuration for VRFs by VRF ID.

### Syntax

- **show ip ospf vrfids WORD<0-512>**

### Command Parameters

WORD<0-512>

Specifies the VRF ID.

### Default

None

### Command Mode

User EXEC

---

## show ip pim

---

Display the global status of PIM on the switch.

### Syntax

- **show ip pim**

### Default

None

### Command Mode

User EXEC

### Example

```
Switch:1#show ip pim
=====
                          Pim General Group - GlobalRouter
=====
PimStat           : disabled
Mode              : sparse
StaticRP          : disabled
FastJoinPrune     : disabled
SptInfiniteThreshold : enabled
BootstrapPeriod   : 60
CRPAdvTimeout     : 60
```

```

DiscDataTimeout      : 60
FwdCacheTimeout      : 210
RegSupprTimeout      : 60
UniRouteChangeTimeout : 5
JoinPruneInt         : 60

```

## show ip pim active-rp

Displays information about the active rendezvous point (RP) for all groups or a specific group.

### Syntax

- **show ip pim active-rp**
- **show ip pim active-rp group <A.B.C.D>**

### Command Parameters

**group <A.B.C.D>**

Specifies the multicast group address.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show ip pim active-rp** command displays the following information:

Output field	Description
GRPADDR	Shows the IP address of the multicast group.
RP-ADDR	Shows the IP address of the RP router. This address must be one of the local PIM-SM enabled interfaces.
RP-PRIORITY	Shows the priority of the RP.

### Example

The following example displays information about the active rendezvous point (RP) for all groups or a specific group. If you do not specify an IP address, you receive information about the active RP for all the running multicast groups on the switch.

```

Switch:1>show ip pim active-rp
=====
                        Pim Grp->RP Active RP Table - GlobalRouter
=====
GRPADDR      RP-ADDR      RP-PRIORITY

```

```

-----
239.0.0.1      20.0.0.90      0
239.0.0.2      20.0.0.90      0
239.0.0.3      20.0.0.90      0
239.0.0.4      20.0.0.90      0
239.0.0.5      20.0.0.90      0
239.255.255.250 20.0.0.90      0

```

## show ip pim bsr

Displays information about the bootstrap router (BSR) for this PIM-SM domain.

### Syntax

- **show ip pim bsr**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show ip pim bsr** command displays the following information:

Output field	Description
Current BSR address	Shows the IP address of the current BSR for the local PIM domain.
Current BSR priority	Shows the priority of the current BSR. The C-BSR with the highest BSR priority and address (referred to as the preferred BSR) is elected as the BSR for the domain.
Current BSR HaskMask	Shows the mask used in the hash function to map a group to one of the C-RPs from the RP set. The hash-mask allows a small number of consecutive groups (for example, 4) to always hash to the same RP.
Current BSR Fragment	Shows a randomly generated number that distinguishes fragments that belong to different bootstrap messages. Fragments that belong to the same bootstrap message carry the same fragment tag.
Pim Bootstrap Timer	Shows the bootstrap timer. After the bootstrap timer expires, the BSR sends out bootstrap messages.

### Example

The following example displays information about the bootstrap router (BSR) for this PIM-SM domain.

```

Switch:1>show ip pim bsr
-----
Current Bootstrap Router Info - GlobalRouter

```

```
=====
Current BSR address: 0.0.0.0
Current BSR priority: -1
Current BSR HashMask: 255.255.255.252
Current BSR Fragment Tag: 0
Pim Bootstrap Timer : 0
```

## show ip pim interface

Displays information about the PIM-SM interface setup on the switch.

### Syntax

- **show ip pim interface** [gigabitethernet [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}]
- **show ip pim interface** [gigabitethernet [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}] [vlan <1-4059>]
- **show ip pim interface** vlan [<1-4059>]

### Command Parameters

**gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** [<1-4059>]

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ip pim interface** command displays the following information:

Output field	Description
IF	Indicates the slot and port number or VLAN ID of the interface where PIM is enabled.
ADDR	Shows the IP address of the PIM interface.
MASK	Shows the network mask for the IP address of the PIM interface.
MODE	Indicates the configured mode of this interface. The valid modes are SSM and Sparse.
DR	Shows the designated router (DR) for this interface.
HLINT	Specifies how long to wait (in seconds) before the PIM router sends out the next hello message to neighboring switches. The default hello interval is 30 seconds.
JPINT	Specifies how long to wait (in seconds) before the PIM router sends out the next join or prune message to its upstream neighbors. The default join and prune interval is 60 seconds.
CBSR	Specifies the preference for this local interface to become a C-BSR. The C-BSR with the highest BSR priority and address the preferred BSR. The default is -1, which indicates that the current interface is not a C-BSR.
OPSTAT	Indicates the status of PIM on this interface: up or down.
INTF TYPE	Indicates whether the PIM interface is active or passive.
VLAN-ID or PORT-NUM	Indicates the slot and port number or VLAN ID of the interface where PIM is enabled.
PIM ENABLE	Indicates the administrative status of PIM.
MODE	Indicates the configured mode of this interface. The valid modes are SSM and Sparse.
HELLOINT	Specifies how long to wait (in seconds) before the PIM router sends out the next hello message to neighboring switches. The default hello interval is 30 seconds.
JPINT	Specifies how long to wait (in seconds) before the PIM router sends out the next join or prune message to its upstream neighbors. The default join and prune interval is 60 seconds.
CBSRPREF	Specifies the preference for this local interface to become a C-BSR. The C-BSR with the highest BSR priority and address the preferred BSR. The default is -1, which indicates that the current interface is not a C-BSR.
INTF TYPE	Indicates whether the PIM interface is active or passive.

## Examples

The following example displays information about the PIM-SM interface configuration on the switch.

```
Switch:1>show ip pim interface
=====
Pim Interface - GlobalRouter
```



```

=====
IF          ADDR          MASK          MODE          DR          HLINT  JPINT  CBSR          OPSTAT INTF TYPE
Port1/4    10.1.1.1      255.255.255.0 ssm          10.1.1.1    30     60     -1 (disabled) up     active
Clip1     111.10.10.10 255.255.255.255 ssm          111.10.10.10 30     60     11 (enabled)  up     passive
Vlan300   21.0.0.206   255.255.255.0 ssm          21.0.0.206  30     60     -1 (disabled) up     active
Vlan400   41.0.0.206   255.255.255.0 ssm          41.0.0.206  30     60     -1 (disabled) up     active
Vlan500   31.0.0.206   255.255.255.0 ssm          31.0.0.206  30     60     -1 (disabled) up     active
Vlan700   62.0.0.206   255.255.255.0 ssm          62.0.0.206  30     60     -1 (disabled) up     active
Vlan701   62.0.1.206   255.255.255.0 ssm          62.0.1.206  30     60     -1 (disabled) up     active
Vlan702   62.0.2.206   255.255.255.0 ssm          62.0.2.206  30     60     -1 (disabled) up     active
Vlan703   62.0.3.206   255.255.255.0 ssm          62.0.3.206  30     60     -1 (disabled) up     active
=====

```

The following example displays information about the PIM-SM configuration for a specific VLAN.

```

Switch:1>show ip pim interface vlan 10
=====
                                Vlan Ip Pim
=====
VLAN-ID  PIM-ENABLE MODE  HELLOINT  JPINT  CBSRPF  INTF TYPE
-----
10        enable   sparse  30        60     -1 (disabled) active
=====

```

## show ip pim mode

Show the PIM mode (SM or SSM) configuration on the switch.

### Syntax

- **show ip pim mode**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show ip pim mode** command displays the following information:

Output field	Description
Mode	Indicates the PIM mode as SM or SSM.

### Example

The following example displays the PIM mode (SM or SSM).

```

Switch:1>show ip pim mode
=====
                                Pim Global Mode - GlobalRouter
=====
Mode      : sparse
=====

```

## show ip pim mroute

---

Displays PIM multicast route information from the route table.

### Syntax

- **show ip pim mroute group {A.B.C.D}**
- **show ip pim mroute source {A.B.C.D}**
- **show ip pim mroute terse**
- **show ip pim mroute terse [group {A.B.C.D}] [source {A.B.C.D}]**
- **show ip pim mroute terse group {A.B.C.D}**
- **show ip pim mroute terse source {A.B.C.D}**

### Command Parameters

**group {A.B.C.D}**

Specifies the multicast group address.

**source {A.B.C.D}**

Specifies the source IP address.

**terse**

Excludes the VLAN timers from the command output.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

In a PIM-SM or PIM-SSM Layer 3 MLT/SMLT multicast environment, when an SMLT link down or SMLT link up event occurs, or when an individual port in an (S)MLT goes down or comes back up, traffic can be re-hashed (switched over) either to another port in the (S)MLT or to any of the IST's MLT ports. This is valid, as the nature of the (S)MLT environment is that traffic can ingress on any one of these ports and be successfully forwarded to receivers. However, the Incoming Port record might not accurately reflect which port the data is arriving on at a given time. This issue does not cause traffic loss. Check traffic statistics on the ports of the (S)MLT/ IST to determine the ingress port.

## Command Output

The **show ip pim mroute** command displays the following information:

Output field	Description
Src	Displays the IP address of the source that sends the multicast stream. A nonzero value indicates that a source sends multicast traffic. 0.0.0.0 indicates that this entry is created in response to a receiver that wants to receive this traffic.
Grp	Displays the IP multicast group address.
RP	Displays the IP address of the RP router.
Upstream	Displays the IP address of the next hop that a multicast packet takes when received on the correct port as listed on the incoming interface.
Flags	Displays the flags configured based on the condition of the receivers, the RP, and the senders. Use the legend at the bottom of the output to explain the flag values.
Incoming Port	Lists the port through which a multicast packet can ingress. If the port is a member of a Multi-Link Trunk (MLT), the packets can ingress on any port of the MLT.
Outgoing Ports	Lists all ports through which traffic that enters on incoming ports exit.
Joined Ports	Lists all ports that received PIM join messages.
Pruned Ports	List all ports that received PIM prune messages.
Leaf Ports	Lists multicast receivers that directly connect to the router.
Asserted Ports	Lists all ports that received assert messages. The router uses assert messages to help determine the best path to the source.
Prune Pending Ports	Lists all ports currently in the prune-pending state.
Assert Winner Ifs	Lists interfaces elected the assert winner. The winner continues to forward multicast traffic to the LAN.
Assert Loser Ifs	Lists interfaces not elected as the assert winner. The loser interface is pruned.
Timers	Displays the up time and expiration time for the entry in the routing table.
AssertVifTimer	Displays the time after which the assert winner state refreshes.

## Example

The following example displays information from the route table.

```
Switch:1>show ip pim mroute
=====
                          Pim Multicast Route - GlobalRouter
=====
Src: 10.1.1.3      Grp: 232.2.1.1      RP: 0.0.0.0      Upstream: 70.70.70.4
Flags: SPT CACHE SG
Incoming  Port: Vlan70-MLT-4(1/24),
Outgoing  Ports: Vlan2-1/8,1/40,
Joined    Ports: Vlan2-1/8,
Pruned    Ports:
```

```

Leaf      Ports: Vlan2-1/40,
Asserted  Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
Entry   JP   RS   Assert
207     9    0     0
VLAN-Id:  2    3    4    70
Join-P:   191  0    0    0
Assert:   0    0    0    0
-----
Src: 10.1.1.4      Grp: 232.2.1.1    RP: 0.0.0.0    Upstream: 70.70.70.4
Flags:
SPT CACHE SG
Incoming Port: Vlan70-MLT-4(1/24),
Outgoing Ports: Vlan2-1/8,1/40,
Joined Ports: Vlan2-1/8,
Pruned Ports:
Leaf      Ports: Vlan2-1/40,
Asserted  Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
Entry   JP   RS   Assert
230     19  0     0
VLAN-Id:  2    3    4    70
Join-P:   203  0    0    0
Assert:   0    0    0    0
-----
Total Num of Entries Displayed 2/2

```

## show ip pim neighbor

Displays information about the neighboring routers configured with PIM-SM.

### Syntax

- **show ip pim neighbor**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ip pim neighbor** command displays the following information:

Output field	Description
INTERFACE	Indicates the interface number.
ADDRESS	Indicates the IP address of the PIM neighbor.
UPTIME	Indicates the elapsed time since this PIM neighbor last became a neighbor of the local router.
EXPIRE	Indicates the time that remains before this PIM neighbor times out.

## show ip pim rp-candidate

Displays information about the candidate rendezvous points for the PIM-SM domain.

### Syntax

- **show ip pim rp-candidate**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ip pim rp-candidate** command displays the following information:

Output field	Description
GRPADDR	Displays the IP address of the multicast group. When combined with the group mask, this value identifies the prefix that the local router uses to advertise itself as a C-RP router.
GRPMASK	Displays the address mask of the multicast group. When combined with the group address, this value identifies the prefix that the local router uses to advertise itself as a C-RP router.
RPADDR	Displays the IP address of the C-RP router. This address must be one of the local PIM-SM enabled interfaces.

## show ip pim rp-hash

Displays information about the rendezvous points (RPs) for this PIM-SM domain.

## Syntax

- **show ip pim rp-hash**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip pim rp-hash** command displays the following information:

Output field	Description
GRPADDRESS	Shows the IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP router.
GRPMASK	Shows the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP router.
ADDRESS	Shows the IP address of the C-RP router.
HOLDTIME	Shows the time specified in a C-RP advertisement that the BSR uses to time out the RP. After the BSR receives an advertisement for the RP, it restarts the timer. If no advertisement arrives before the timer expires, the BSR removes that RP from the RP set.
EXPTIME	Shows the time that remains before this C-RP router times out.

## show ip pim static-rp

Displays the static rendezvous point (RP) table.

## Syntax

- **show ip pim static-rp**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip pim static-rp** command displays the following information:

Output field	Description
GRPADDR	Indicates the IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a static RP.
GRPMASK	Indicates the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a static RP.
RPADDR	Indicates the IP address of the static RP. This address must be one of the local PIM-SM enabled interfaces.
STATUS	Indicates the status of static RP.

## Example

The following example displays the static RP table.

```
Switch:1>show ip pim static-rp
=====
                        Pim Static RP Table - GlobalRouter
=====
GRPADDR      GRPMASK      RPADDR      STATUS
-----
239.0.0.0    255.0.0.0    20.0.0.90   valid
```

## show ip pim virtual-neighbor

Display the virtual neighbor.

### Syntax

- **show ip pim virtual-neighbor**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ip pim virtual-neighbor** command displays the following information:

Output field	Description
INTERFACE	Indicates the interface.
ADDRESS	Indicates the IP address of the virtual neighbor.

## show ip prefix-list

Display the prefix list.

### Syntax

- **show ip prefix-list**
- **show ip prefix-list [WORD<1-64>] [prefix <A.B.C.D>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip prefix-list prefix {A.B.C.D}**
- **show ip prefix-list vrf WORD<1-16>**
- **show ip prefix-list vrfids WORD<0-512>**
- **show ip prefix-list WORD<1-64>**

### Command Parameters

**prefix {A.B.C.D}**

Adds a prefix entry to the prefix list. {A.B.C.D} is the IP address.

**vrf WORD<1-16>**

Shows prefix list for particular VRF ids. The ID of the VRF and is an integer in the range of 0 to 512.

**vrfids WORD<0-512>**

Renames the specified prefix list. The name length is from 1 to 64 characters.

**WORD <1-64>**

Renames the specified prefix list. The name length is from 1 to 64 characters.

### Default

None

### Command Mode

User EXEC



---

## show ip rip

---

Display RIP configuration information to ensure the configuration is accurate.

### Syntax

- `show ip rip`
- `show ip rip [vrf WORD<1-16>] [vrfids WORD<0-512>]`
- `show ip rip vrf WORD<1-16>`
- `show ip rip vrfids WORD<0-512>`

### Command Parameters

`vrf WORD<1-16>`

Specifies a VRF by name.

`vrfids WORD<0-512>`

Specifies a range of VRF IDs.

### Default

None

### Command Mode

User EXEC

---

## show ip rip interface

---

Display Routing Information Protocol (RIP) information for each interface.

### Syntax

- `show ip rip interface`
- `show ip rip interface {A.B.C.D}`
- `show ip rip interface ports`
- `show ip rip interface ports {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}`
- `show ip rip interface ports {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} [vlan <1-4059>] [vrf WORD<1-16>] [vrfids WORD<0-512>] [{A.B.C.D}]`
- `show ip rip interface vlan`
- `show ip rip interface vlan <1-4059>`
- `show ip rip interface vrf WORD<1-16>`
- `show ip rip interface vrfids WORD<0-512>`

## Command Parameters

**{A.B.C.D}**

Shows configurations based on an IP address assigned to a VLAN.

**ports {slot/port[/sub-port][/-slot/port[/sub-port]][...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip rip redistribute

---

Display the RIP redistribution configuration information.

## Syntax

- **show ip rip redistribute**
- **show ip rip redistribute [vrf WORD<1-16>] [vrfids WORD<1-512>]**
- **show ip rip redistribute vrf WORD<1-16>**
- **show ip rip redistribute vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip rip vrf

---

Shows RIP information for a particular VRF by ID.

## Syntax

- **show ip rip vrf WORD<1-16>**
- **show ip rip vrf WORD<1-16> vrfids WORD<0-512>**

## Command Parameters

**vrfids WORD<0-512>**

Specifies the VRF ID.

**WORD<1-16>**

Specifies the VRF name.

## Default

None

## Command Mode

User EXEC

## show ip rip vrfids

---

Shows RIP information for a particular VRF by ID.

## Syntax

- **show ip rip vrfids WORD<0-512>**

## Command Parameters

WORD<0-512>

Specifies the VRF ID.

## Default

None

## Command Mode

User EXEC

## show ip route

---

Display the IP route information.

## Syntax

- `show ip route`
- `show ip route {A.B.C.D}`
- `show ip route alternative protocol {bgp|isis|local|ospf|rip|static|}`
- `show ip route alternative spbm-nh-as-mac`
- `show ip route alternative vrf WORD<1-16>`
- `show ip route alternative vrfids WORD<0-512>`
- `show ip route count-summary vrf WORD<1-16>`
- `show ip route count-summary vrfids WORD<0-512>`
- `show ip route preference vrf WORD<1-16>`
- `show ip route preference vrfids WORD<0-512>`
- `show ip route protocol [bgp|isis|local|ospf|rip|static|]`
- `show ip route -s {A.B.C.D/X}`
- `show ip route -s default`
- `show ip route spbm-nh-as-mac`
- `show ip route static`
- `show ip route static {A.B.C.D}`
- `show ip route static {A.B.C.D} -s {A.B.C.D} {A.B.C.D}`
- `show ip route static {A.B.C.D} vrf WORD<1-16>`
- `show ip route static {A.B.C.D} vrfids WORD<0-512>`
- `show ip route static -s {A.B.C.D} {A.B.C.D}`
- `show ip route static -s {A.B.C.D} {A.B.C.D} vrf WORD<1-16>`
- `show ip route static -s {A.B.C.D} {A.B.C.D} vrfids WORD<0-512>`
- `show ip route static vrf WORD<1-16>`

- **show ip route static vrfids WORD<0-512>**
- **show ip route vrf WORD<1-16>**
- **show ip route vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D}**

Specifies the IP address of the route to the network.

**alternative**

Displays the alternative routes.

**count-summary**

Displays ip route count summary.

**preference**

Displays the route preference information.

**-s <A.B.C.D/X>**

Indicates the IP address and subnet mask for which to display routes.

**-s default**

Specifies the default subnet.

**spbm-nh-as-mac**

show spbm route next hop as mac

**static**

Shows static route information.

**static -s {A.B.C.D} {A.B.C.D} vrf WORD<1-16>**

Shows static route information.

**vrf WORD<1-16>**

Specifies a VRF instance by VRF name.

**vrfids WORD<0-512>**

Specifies a VRF instance by VRF number.

## Default

None

## Command Mode

User EXEC

## show ip routing

Display the ip routing configuration information.

## Syntax

- **show ip routing**
- **show ip routing [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip routing vrf WORD<1-16>**
- **show ip routing vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Display the ip routing configuration information.

**vrfids WORD<0-512>**

Specifies a VRF instance by VRF number.

## Default

None

## Command Mode

User EXEC

## show ip rsmplt

---

Show IP Routed Split MultiLink Trunking (RSMLT) information to view data about all RSMLT interfaces.

## Syntax

- **show ip rsmplt**
- **show ip rsmplt [<local|peer>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip rsmplt local**
- **show ip rsmplt peer**
- **show ip rsmplt vrf WORD<1-16>**
- **show ip rsmplt vrfids WORD<0-512>**

## Command Parameters

**edge-support**

Displays RSMLT edge support and peer information.

**local**

Displays values for the local switch.

**peer**

Specifies values for the peer switch.

**vrf WORD<1-16>**

Specifies a VRF instance by VRF name.

**vrfids WORD<0-512>**

Specifies a VRF instance by VRF number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip rsmlt** command displays the following information:

Output field	Description
VID	Indicates the VLAN ID.
IP	Indicates the IP address of the VLAN.
MAC	Indicates the MAC address assigned.
ADMIN	Indicates the administrative status of RSMLT on the VLAN.
OPER	Indicates the operational status of RSMLT on the VLAN.
HDTMR	Indicates the hold-down timer value in the range of 0 to 3600 seconds.
HUTMR	Indicates the hold-up timer value in the range of 0 to 3600 seconds or 9999. 9999 means infinity.
HDT REMAIN	Indicates the time remaining of the hold-down timer.
HUT REMAIN	Indicates the time remaining of the hold-up timer.
SMLT ID	Indicates the Split MultiLink Trunk ID.

## Example

The following example shows the output of the **show ip rsmlt** command.

```
Switch:1>show ip rsmlt

=====
                          Ip Rsmlt Local Info - GlobalRouter
=====

VID   IP           MAC           ADMIN  OPER  HDTMR  HUTMR
-----
101   101.1.1.32    00:24:7f:9e:da:01  Enable Up    100    200
102   102.1.1.32    00:24:7f:9e:da:02  Enable Up     60    180

VID   SMLT ID
-----
101   101
```

```

102    102

VID   IPv6           MAC                ADMIN  OPER  HDTMR  HUTMR
-----
101           00:24:7f:9e:da:01  Enable  Up    100    200
    1010:0:0:0:0:0:0/64
    1010:0:0:0:0:0:0:32/64
    fe80:0:0:0:224:7fff:fe9e:da01/128
102           00:24:7f:9e:da:02  Enable  Up    60     180
    1020:0:0:0:0:0:0/64

    1020:0:0:0:0:0:0:32/64
    fe80:0:0:0:224:7fff:fe9e:da02/128

VID   SMLT ID
-----
101    101
102    102

=====
                          Ip Rsmлт Peer Info - GlobalRouter
=====

VID   IP             MAC                ADMIN  OPER  HDTMR  HUTMR
-----
101   101.1.1.33      00:24:7f:9e:ea:01  Enable  Up    100    200
102   102.1.1.33      00:24:7f:9e:ea:00  Enable  Up    60     180

VID   HDT REMAIN  HUT REMAIN  SMLT ID
-----
101   60          180         101
102   60          180         102

VID   IPv6           MAC                ADMIN  OPER  HDTMR  HUTMR
-----
101           00:24:7f:9e:ea:01  Enable  Up    100    200
    1010:0:0:0:0:0:0/64
    1010:0:0:0:0:0:0:33/64
    fe80:0:0:0:224:7fff:fe9e:ea01/128
102           00:24:7f:9e:ea:00  Enable  Up    60     180
    1020:0:0:0:0:0:0/64
    1020:0:0:0:0:0:0:33/64
    fe80:0:0:0:224:7fff:fe9e:ea00/128

VID   HDT REMAIN  HUT REMAIN  SMLT ID
-----
101   60          180
101
102   60          180
102

```

## show ip rsmлт edge-support

Display Routed Split MultiLink Trunking (RSMLT)-edge status information.



## Syntax

- **show ip rsmult edge-support**

## Default

None

## Command Mode

User EXEC

## show ip source binding

---

Displays the IPv4 addresses that are allowed on all IP Source Guard enabled ports or for a specified port.

## Syntax

- **show ip source binding**
- **show ip source binding {A.B.C.D}**
- **show ip source binding interface gigaBiteEthernet**
- **show ip source binding interface gigaBiteEthernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**
- **show ip source binding vlan <1-4059>**
- **show ip source binding vrf WORD<1-16>**
- **show ip source binding vrfids WORD<0-512>**

## Command Parameters

**{A.B.C.D}**

Displays the IP Source Guard address bindings for the specified IPv4 address.

**interface gigaBiteEthernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**

Displays the IPv4 addresses that are allowed on the specified IP Source Guard port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Displays the IP Source Guard address bindings list for a specific vrf.

**vrfids WORD<0-512>**

Displays the IP Source Guard address bindings list for a specific vrf id.

## Default

None

## Command Mode

User EXEC

## show ip source verify

---

Displays IP Source Guard configuration on all ports or for a specified port, for IPv4 addresses.

## Syntax

- **show ip source verify interface gigabitethernet**

## Command Parameters

**interface gigabitethernet**

Displays IP Source Guard configuration on all ports on the switch, for IPv4 addresses.

**interface gigabitethernet** [{slot/port[/sub-port] [-slot/port[/sub-port]] [...]]

Displays IP Source Guard configuration on the specified port(s), for IPv4 addresses.

## Default

None

## Command Mode

User EXEC

## show ip spb-pim-gw

---

Display the default values used for the SPB-PIM Gateway interface HELLO and JOIN PRUNE intervals unless specifically configured on the individual interface

## Syntax

- **show ip spb-pim-gw**
- **show ip spb-pim-gw interface gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [...]}
- **show ip spb-pim-gw interface gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [...]} vrf WORD<0-16>
- **show ip spb-pim-gw interface gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [...]} vrfids WORD<0-512>

## Default

None

## Command Mode

User EXEC

# show ip spb-pim-gw foreign-source

---

Displays the foreign source information.

## Syntax

- `show ip spb-pim-gw foreign-source`
- `show ip spb-pim-gw foreign-source controller`
- `show ip spb-pim-gw foreign-source vrf WORD<1-16>`
- `show ip spb-pim-gw foreign-source vrfids WORD<0-512>`
- `show ip spb-pim-gw foreign-source all`
- `show ip spb-pim-gw foreign-source gateway`
- `show ip spb-pim-gw foreign-source group {A.B.C.D}`
- `show ip spb-pim-gw foreign-source msdp`
- `show ip spb-pim-gw foreign-source source {A.B.C.D}`
- `show ip spb-pim-gw foreign-source spb-node-as-mac`
- `show ip spb-pim-gw foreign-source static`

## Command Parameters

### all

Displays information for all the VRF IDs from the Controller and Gateway foreign source database.

### controller

Displays information from the Controller foreign source database. Only displays information on nodes configured as Controller.

### gateway

Displays information from the Gateway foreign source database. Only displays information on nodes configured as Gateway.

### group {A.B.C.D}

Displays information for the specific multicast group IP address from the Controller foreign source database.

### msdp

Displays information from the Controller foreign source database that is learned through MSDP.

### source {A.B.C.D}

Displays information for the specific source IP address from the Controller foreign source database.

**spb-node-as-mac**

Displays the MAC address for the assigned SPB-PIM Gateway.

**static**

Displays information from the Controller foreign source database that is configured statically.

**vrf WORD<1-16>]**

Displays information from the Controller foreign source database for a specific VRF name.

**vrfids WORD<0-512>**

Displays information from the Controller foreign source database for a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip spb-pim-gw interface

---

Display the SPB-PIM Gateway VLAN interface information

## Syntax

- **show ip spb-pim-gw interface vlan <1-4059>**

## Command Parameters

**{slot/port[/sub-port][/-slot/port[/sub-port]][,...]}**

Identifies the slot and port. {slot/port[/sub-port][/-slot/port[/sub-port]][,...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the SPB-PIM Gateway interface neighbor information for a specific VRF.

**vrfids WORD<0-512>**

Specifies the SPB-PIM Gateway interface neighbor information for a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip spb-pim-gw neighbor

---

Display the SPB-PIM Gateway interfaces neighbor information.

## Syntax

- **show ip spb-pim-gw neighbor**
- **show ip spb-pim-gw neighbor vrf WORD<1-16>**
- **show ip spb-pim-gw neighbor vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies the SPB-PIM Gateway interface information for a specific VRF.

**vrfids WORD<0-512>**

Specifies the SPB-PIM Gateway interface information for a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip spb-pim-gw node

---

Displays the active Controllers and Gateways in the SPBM domain.

## Syntax

- **show ip spb-pim-gw node controller**
- **show ip spb-pim-gw node gateway**
- **show ip spb-pim-gw node spb-node-as-mac**

## Command Parameters

### controller

Displays only the controller nodes.

### gateway

Displays only the gateway nodes.

### spb-node-as-mac

Displays the node list with mac address.

## Default

None

## Command Mode

User EXEC

## show ip spb-pim-gw spbmc-source

---

Displays all the SPB Multicast over Fabric Connect sources distributed to MSDP.

## Syntax

- **show ip spb-pim-gw spbmc-source group {A.B.C.D}**
- **show ip spb-pim-gw spbmc-source originator WORD<1-32>**
- **show ip spb-pim-gw spbmc-source source {A.B.C.D}**
- **show ip spb-pim-gw spbmc-source spb-node-as-mac**
- **show ip spb-pim-gw spbmc-source vrf WORD<1-16>**
- **show ip spb-pim-gw spbmc-source WORD<0-512>**

## Command Parameters

### group {A.B.C.D}

Displays information for a specific multicast group IP address from SPB originated sources database.

### originator WORD<1-32>

Displays information for a specific originator host name from SPB originated sources database.

### source {A.B.C.D}

Displays information for a specific source IP address from SPB originated sources database.

### spb-node-as-mac

Displays the originator of SPB originated sources as a MAC address rather than a nickname.

### vrf WORD<1-16>

Displays SPB originated sources for a specific VRF.

**vrfids WORD<0-512>**

Displays SPB originated sources for a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

# show ip spb-pim-rw mroute

---

Display the SPB-PIM Gateway multicast routes.

## Syntax

- **show ip spb-pim-rw mroute**
- **show ip spb-pim-rw mroute**
- **show ip spb-pim-rw mroute group {A.B.C.D}**
- **show ip spb-pim-rw mroute source {A.B.C.D}**
- **show ip spb-pim-rw mroute vrf WORD<1-16>**
- **show ip spb-pim-rw mroute vrfids WORD<0-512>**

## Command Parameters

**group {A.B.C.D}**

Displays mroute information specific to a group IP address.

**source {A.B.C.D}**

Displays mroute information specific to a source IP address.

**vrf WORD<1-16>**

Specifies the SPB-PIM Gateway mroute information for a specific VRF.

**vrfids WORD<0-512>**

Specifies the SPB-PIM Gateway mroute information for a range of VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ip tcp adjust-mss

Displays the configuration of the TCP maximum segment size (MSS) adjustment functionality on the switch.

### Syntax

- **show ip tcp adjust-mss**

### Default

None.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show ip tcp adjust-mss** command displays the following information:

Output field	Description
ENABLE	Displays if the MSS adjustment functionality is enabled on the switch.
STATUS	Displays the activation status of the MSS adjustment functionality. The MSS adjustment functionality only activates when at least one FE tunnel with a maximum transmission unit (MTU) less than or equal to 1500 is configured.
TCP MSS TYPE	Displays if the MSS adjustment value is manually configured or auto-derived.
TCP MSS VALUE	Displays the MSS adjustment value.

### Example

The following example displays the TCP MSS adjustment configuration.

```
Switch:1>show ip tcp adjust-mss
=====
                        IP TCP Adjust MSS
=====
ENABLE          STATUS          TCP MSS          TCP MSS
                        TYPE          VALUE
-----
TRUE            ACTIVE          MANUAL-CONFIG    1200
```



## show ip tcp connections

---

Displays the information on the TCP connections.

### Syntax

- **show ip tcp connections [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ip tcp connections vrf WORD<1-16>**
- **show ip tcp connections vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF instance by VRF name.

**vrfids WORD<0-512>**

Specifies a VRF instance by VRF number.

### Default

None

### Command Mode

User EXEC

## show ip tcp properties

---

Displays global properties.

### Syntax

- **show ip tcp properties**

### Default

None

### Command Mode

User EXEC

## show ip tcp statistics

---

View TCP statistics to manage network performance.

## Syntax

- **show ip tcp statistics**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ip tcp statistics** command displays the following information:

Field	Description
ActiveOpens	The count of transitions by TCP connections to the SYN-SENT state from the CLOSED state.
PassiveOpens	The count of transitions by TCP connections to the SYN-RCVD state from the LISTEN state.
AttemptFails	The count of transitions by TCP connections to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the count of transitions to the LISTEN state from the SYN-RCVD state.
EstabResets	The count of transitions by TCP connections to the CLOSED state from the ESTABLISHED or CLOSE-WAIT state.
CurrEstab	The count of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
InSegs	The total count of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
RetransSegs	The total count of TCP segments transmitted containing one or more previously transmitted octets.
InErrs	The count of segments received in error.
OutRsts	The count of TCP segments sent containing the RST flag.

```
Switch:1#show ip tcp statistics
show ip tcp global statistics:
-----
ActiveOpens:          0
```

```
PassiveOpens:      37
AttemptFails:      0
EstabResets:       34
CurrEstab:         1
InSegs:            6726
OutSegs:           7267
RetransSegs:       10
InErrs:            0
OutRsts:           10
```

---

## show ip udp endpoints

---

Displays ip udp endpoints information.

### Syntax

- **show ip udp endpoints**

### Default

None

### Command Mode

User EXEC

---

## show ip udp statistics

---

Display UDP statistics information.

### Syntax

- **show ip udp statistics**

### Default

None

### Command Mode

User EXEC

---

## show ip vrf

---

View VRF configuration by VRF name.

## Syntax

- **show ip vrf**
- **show ip vrf ipv6-max-routes** [vrf WORD <1-16>] [vrfids WORD <0-512>]
- **show ip vrf max-routes**
- **show ip vrf max-routes** [vrf WORD <1-16>] [vrfids WORD <0-512>]
- **show ip vrf vrf** WORD <1-16>
- **show ip vrfids** WORD <0-512>

## Command Parameters

### ipv6-max-routes

Displays ipv6 max routes for VRF.

### max-routes

Displays max routes for vrf.

### mvpn

Displays mvpn information for vrf.

### vrfids WORD<0-512>

Displays configuration information for a VRF ID.

### WORD<1-16>

Specifies a VRF instance by VRF name.

## Default

None

## Command Mode

User EXEC

## show ip vrf mvpn

---

Displays information about all VRFS with MVPN enabled.

## Syntax

- **show ip vrf mvpn**

## Default

None

## Command Mode

User EXEC

## show ip vrrp

---

Display the global Virtual Router Redundancy Protocol (VRRP) configuration.

### Syntax

- **show ip vrrp**
- **show ip vrrp vrf WORD <1-16>**
- **show ip vrrp vrfids WORD<0-512>**

### Default

None

## Command Mode

User EXEC

## show ip vrrp address

---

Display basic Virtual Router Redundancy Protocol (VRRP) configuration information about the specified port, all ports, or the VLAN.

### Syntax

- **show ip vrrp address**
- **show ip vrrp address [addr {A.B.C.D}] [vrid <1-255>] [addr <A.B.C.D>] [vrf WORD<1-16>] [vrfids WORD<0-512>] [version <2-3>]**
- **show ip vrrp address [version <2-3>]**
- **show ip vrrp address addr {A.B.C.D}**
- **show ip vrrp address vrf WORD<1-16>**
- **show ip vrrp address vrfids WORD<0-512>**
- **show ip vrrp address vrid <1-255>**

### Command Parameters

[version <2|3>

Displays the VRRP version configured.

addr {A.B.C.D}

Specifies the IP address of the master VRRP.

vrf WORD<1-16>

Specifies the name of the VRF.

**vrfids WORD<0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

**vrid <1-255>**

Specifies a unique integer value that represents the virtual router ID in the range 1 to 255. The virtual router acts as the default router for one or more assigned addresses.

## Default

None

## Command Mode

User EXEC

## show ip vrrp interface

---

Display Virtual Router Redundancy Protocol (VRRP) information about the interface.

## Syntax

- **show ip vrrp interface**
- **show ip vrrp interface**
- **show ip vrrp interface [versin <2-3>]**
- **show ip vrrp interface [version <2-3>]**
- **show ip vrrp interface verbose**
- **show ip vrrp interface vrf WORD<1-16>**
- **show ip vrrp interface vrfids WORD<0-512>**
- **show ip vrrp interface vrid <1-255>**

## Command Parameters

**[version <2|3>**

Displays the VRRP version configured.

**gigabitEthernet {slot/port[/sub-port]][-slot/port[/sub-port]][,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**verbose**

Shows all available information about the VRRP interfaces.

**vlan <1-4059>**

Shows the VRRP interface gigabitEthernet configurations. Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Shows all available information about the VRRP interfaces.

**vrfids WORD<0-512>**

Specifies the ID of the VRF.

## Default

None

## Command Mode

User EXEC

## show ip vrrp interface gigabitEthernet

---

Display the Virtual Router Redundancy Protocol (VRRP) interface gigabitEthernet configurations.

## Syntax

- **show ip vrrp interface gigabitEthernet**
- **show ip vrrp interface gigabitEthernet <1-4059>**
- **show ip vrrp interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show ip vrrp interface gigabitEthernet verbose**

## Command Parameters

**{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**<1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**verbose**

Displays all available information about the VRRP interface gigabitEthernet configurations.

## Default

None

## Command Mode

User EXEC

# show ip vrrp interface gigabitEthernet statistics

---

Display statistics for Virtual Router Redundancy Protocol (VRRP) ports.

## Syntax

- **show ip vrrp interface gigabitEthernet statistics**
- **show ip vrrp interface gigabitEthernet statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ip vrrp interface gigabitEthernet statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} verbose**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**verbose**

Displays all available information about the VRRP interface gigabitEthernet configurations.

## Default

None

## Command Mode

User EXEC

# show ip vrrp interface vlan

---

Show the extended Virtual Router Redundancy Protocol (VRRP) configuration for all VLANs on the switch or for the specified VLAN.

## Syntax

- **show ip vrrp interface vlan**
- **show ip vrrp interface vlan <1-4059>**



- **show ip vrrp interface vlan {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ip vrrp interface vlan verbose**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### verbose

Displays all available information about the VRRP interface VLAN configurations.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf** WORD<1-16>

Specifies the name of the VRF.

**vrfids** WORD<0-512>

Specifies the ID of the VRF.

## Default

None

## Command Mode

User EXEC

## show ip vrrp statistics

Display Virtual Router Redundancy Protocol (VRRP) statistics.

## Syntax

- **show ip vrrp statistics**
- **show ip vrrp statistics [address {A.B.C.D}] [vrf WORD<1-16>] [vrfids WORD<0-512>] [vrid<1-255>] [version <2-3>]**
- **show ip vrrp statistics [version <2-3>]**
- **show ip vrrp statistics address {A.B.C.D}**

- **show ip vrrp statistics vrf WORD<1-16>**
- **show ip vrrp statistics vrfids WORD<0-512>**
- **show ip vrrp statistics vrid <1-255>**

## Command Parameters

**[version <2|3>**

Displays the VRRP version configured.

**address {A.B.C.D}**

Specifies the address of the backup VRRP.

**vrf WORD<1-16>**

Specifies the VRF name.

**vrfids WORD<0-512>**

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

**vrid WORD<1-255>**

Specifies a unique integer value that represents the virtual router ID in the range of 1 to 255. The virtual router acts as the default router for one or more assigned addresses.

## Default

None

## Command Mode

User EXEC

## show ipsec interface (for a port)

---

Display the Internet Protocol Security (IPsec) information on an Ethernet interface. The command only works on an interface where you enable IPv6. If you do not enable IPv6 on the interface, the command displays as an error to the user.

## Syntax

- **show ipsec interface**
- **show ipsec interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipsec interface gigabitethernet** command displays the following information:

Output field	Description
Interface	Specifies the interface.
Policy Name	Specifies the IPsec policy that associates with the specific port or ports.
IPsec State	Specifies whether the IPsec policy is enabled on the interface.
Direction	Specifies the policy direction.

## show ipsec interface (for a VLAN)

Display the Internet Protocol Security (IPsec) information on an VLAN interface. The command only works on an interface where you enable IPv6. If you do not enable IPv6 on the interface, the command displays as an error to the user.

## Syntax

- **show ipsec interface**
- **show ipsec interface vlan <1-4059>**

## Command Parameters

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipsec interface vlan** command displays the following information:

Output field	Description
Vlan Interface	Specifies the VLAN interface.
Policy Name	Specifies the IPsec policy that associates with the specific VLAN or VLANs.
IPsec State	Specifies whether the IPsec policy is enabled on the VLAN interface.
Direction	Specifies the policy direction.

## show ipsec interface loopback

Displays the IPsec status on a loopback interface.

## Syntax

- **show ipsec interface loopback <1-256>**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipsec interface loopback** command displays the following information:

Output field	Description
LoopBack Interface	Specifies the loopback interface.
Policy Name	Specifies the IPsec policy that associates with the interface.
IPsec State	Specifies whether the IPsec policy is enabled on the interface.
Direction	Specifies the policy direction.

## show ipsec interface mgmtethernet mgmt

Displays the IPsec status on a management interface.

## Syntax

- **show ipsec interface mgmtethernet mgmt**

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## Command Output

The **show ipsec interface mgmtethernet** command displays the following information:

Output field	Description
Interface	Specifies the VLAN interface.
Policy Name	Specifies the IPsec policy that associates with the management port.
IPsec State	Specifies whether the IPsec policy is enabled on the interface.
Direction	Specifies the policy direction.

## show ipsec policy

Display Internet Protocol Security (IPsec) policy information.

## Syntax

- **show ipsec policy all**
- **show ipsec policy interface WORD<1-32>**
- **show ipsec policy name WORD<1-32>**

## Command Parameters

**all**

Displays all of the IPsec policies on the switch.

**interface WORD<1-32>**

Displays a specific IPsec policy based on the policy name on the interface.

**name WORD<1-32>**

Displays the IPsec policy based on the name of the policy.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipsec policy all** and **show ipsec policy name** commands display the following information:

Output field	Description
PolicyName	Specifies the IPsec policy name.
LocalAddress	Specifies the local address. The default is 0::0.
RemoteAddress	Specifies the remote address. The default is 0::0.
Protocol	Specifies the protocol.
src-port	Specifies the source port.
dest-port	Specifies the destination port.
Action	Specifies the action as either: permit or drop.
Admin	Specifies whether the policy is enabled.

The **show ipsec policy interface** command displays the following information:

Output field	Description
POLICY NAME	Specifies the IPsec policy name.
InterfaceIndex	Specifies the interface.
Policy State	Specifies whether the policy is enabled.

## show ipsec sa

Display Internet Protocol Security (IPsec) security association information.

## Syntax

- **show ipsec sa all**
- **show ipsec sa name WORD<1-32>**

## Command Parameters

### all

Displays all of the IPsec security association information.

### name WORD<1-32>

Displays information about a specific IPsec security association.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipsec sa** command displays the following information:

Output field	Description
sa-name	Specifies all of the IPsec security association names.
key-Mode	Specifies the key mode as manual or automatic. The default is automatic.
Encap protocol	Specifies the encapsulation protocol.
SPI Value	Specifies the SPI value, which is a tag added to the IP header. For IPsec to function, each peer must have the same SPI value configured on both peers for a particular policy.
Encrypt Algorithm	Specifies the encrypt algorithm as one of the following: <ul style="list-style-type: none"> <li>• 3DES-CBC</li> <li>• AES-CBC</li> <li>• AES-CTR</li> <li>• NULL—Only used to debug.</li> </ul>
Encrypt-key	Specifies the encrypt-key parameter for the authentication key in either: <ul style="list-style-type: none"> <li>• hex— Specifies hexadecimal.</li> <li>• ascii—Specifies ASCII, the American Standard Code for Information Interchange character encoding scheme.</li> </ul>
Encrypt-key-Len	Specifies the key length value in a string from 1 to 256 characters. The default KeyLength is 128.
Mode	Specifies the mode value as one of the following: <ul style="list-style-type: none"> <li>• tunnel—Tunnel mode encapsulates the entire IP packet and provides a secure tunnel.</li> <li>• transport—Transport mode encapsulates the IP payload and provides a secure connection between two endpoints.</li> </ul> <p>The default is transport mode.</p>

Output field	Description
Lifetime-Sec	Specifies the lifetime value in seconds. The default is 28800.
Lifetime-Byte	Specifies the lifetime value in bytes. The default is 4294966272.

## show ipsec sa-policy

Display Internet Protocol Security (IPsec) security associations linked to a particular IPsec policy.

### Syntax

- **show ipsec sa-policy**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show ipsec sa-policy** command displays the following information:

Output field	Description
Policy Name	Specifies the IPsec policy name.
Security Association	Specifies the security association name.

## show ipsec statistics gigabitethernet

Display statistics for Internet Protocol Security (IPsec) for an Ethernet interface.

### Syntax

- **show ipsec statistics gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipsec statistics gigabitethernet** command displays the following information:

Output field	Description
Ifindex	Specifies the interface.
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the encapsulating security payload (ESP) replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.

## show ipsec statistics mgmtethernet

Displays the IPsec status on a management interface.

## Syntax

- **show ipsec statistics mgmtethernet mgmt2**

## Command Parameters

<mgmt|mgmt2>

Specifies the management interface (primary or standby) on which to view the IPsec status. This command applies to hardware with a dedicated, physical management interface.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command is only supported on VSP 8600 Series. This command is deprecated for all hardware platforms that support VOSS Release 8.2 and later.

## Command Output

The **show ipsec statistics mgmtethernet** command displays the following information:

Output field	Description
Ifindex	Specifies the interface.
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the AH replay check fails.
InESPReplays	Specifies the total number of ingress packets IPsec discards since boot time because the encapsulating security payload (ESP) replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.

## show ipsec statistics system

Display statistics for Internet Protocol Security (IPsec) for the system.

## Syntax

- **show ipsec statistics system**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipsec statistics system** command displays the following information:

Output field	Description
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the encapsulating security payload (ESP) replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.
InAHSuccesses	Specifies the number of ingress packets IPsec carries because the AH authentication succeeds.
InESPSuccesses	Specifies the number of ingress packets IPsec carries since boot time because the ESP authentication succeeds.
OutAHSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutESPSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutKBytes	Specifies the total number of kilobytes on egress.
OutBytes	Specifies the total number of bytes on egress.

Output field	Description
InKBytes	Specifies the total number of bytes on ingress.
InBytes	Specifies the total number of bytes on ingress.
TotalPacketsProcessed	Specifies the total number of packets processed.
TotalPacketsByPassed	Specifies the total number of packets bypassed.
OutAHFailures	Specifies the number of egress packets IPsec discards since boot time because the AH authentication check fails.
OutESPFailures	Specifies the number of egress packets IPsec discards since boot time because the ESP authentication check fails.
InMD5Hmac	Specifies the number of inbound HMAC MD5 occurrences since boot time.
InSHA1Hmac	Specifies the number of inbound HMAC SHA1 occurrences since boot time.
InAESXCBCs	Specifies the number of inbound AES XCBC MAC occurrences since boot time.
InAnyNullAuth	Specifies the number of inbound null authentication occurrences since boot time.
In3DESCBCs	Specifies the number of inbound 3DES CBC occurrences since boot time.
InAESCBCs	Specifies the number of inbound AES CBC occurrences since boot time.
InAESCTRs	Specifies the number of inbound AES CTR occurrences since boot time.
InAnyNullEncrypt	Specifies the number of inbound null occurrences since boot time. Used for debugging purposes.
OutMD5Hmac	Specifies the number of outbound HMAC MD5 occurrences since boot time.
OutSHA1Hmac	Specifies the number of outbound HMAC SHA1 occurrences since boot time.
OutAESXCBCs	Specifies the number of outbound AES XCBC MAC occurrences since boot time.
OutInAnyNullAuth	Specifies the number of outbound null authentication occurrences since boot time.
Out3DESCBCs	Specifies the number of outbound 3DES CBC occurrences since boot time.
OutAESCBCs	Specifies the number of outbound AES CBC occurrences since boot time.
OutAESCTRs	Specifies the number of outbound AES CTR occurrences since boot time.
OutInAnyNullEncrypt	Specifies the number of outbound null occurrences since boot time. Used for debugging purposes.

## show ipsec statistics vlan

Display statistics for Internet Protocol Security (IPsec) for an VLAN interface.

### Syntax

- **show ipsec statistics vlan <1-4059>**

## Command Parameters

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipsec statistics vlan** command displays the following information:

Output field	Description
Ifindex	Specifies the interface.
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the encapsulating security payload (ESP) replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.

## show ipv6 address

View IPv6 address entries.

## Syntax

- **show ipv6 address interface**
- **show ipv6 address interface gigabitethernet** [{slot/port[/sub-port] [-slot/port[/sub-port]][,...]]
- **show ipv6 address interface ip** WORD<0-46>
- **show ipv6 address interface ip** WORD<0-46> vrf WORD<1-16>
- **show ipv6 address interface ip** WORD<0-46> vrfids WORD<0-512>
- **show ipv6 address interface tunnel** <1-2000>
- **show ipv6 address interface vlan** [ <1-4059>]
- **show ipv6 address interface vrf** WORD<1-16>
- **show ipv6 address interface vrfids** WORD<0-512>

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]][,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

tunnel <1-2000>

Displays the address entries specific to a tunnel ID.

vrf WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

vrfids WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

WORD<0-46>

Specifies an IPv6 address.

## Default

None

## Command Mode

User EXEC

## show ipv6 bfd

Display global Bidirectional Forwarding Detection (BFD) configuration information for IPv6 interfaces.

### Syntax

- **show ipv6 bfd**
- **show ipv6 bfd vrf**
- **show ipv6 bfd vrfids**

### Command Parameters

**vrf**

Specifies a VRF instance by VRF name.

**vrfids**

Specifies a VRF or range of VRFs by ID.

### Command Mode

User EXEC

### Usage Guidelines

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show ipv6 bfd** command displays the following information:

Output field	Description
BFD Version	Specifies the current BFD version.
Admin Status	Specifies whether BFD is enabled globally.
Trap Enable	Specifies whether traps are enabled.
Total session number	Specifies the total number of BFD sessions.
UP	Specifies whether a BFD session is in UP state.
DOWN	Specifies whether a BFD session is in DOWN state.
AdminDown	Specifies whether a BFD session is in AdminDown state.
Init	Specifies whether a BFD session is in Init state.

## Example

The following example displays global configuration information for BFD on an IPv6 interface.

```
Switch:1>show ipv6 bfd
=====
                        BFD information - GlobalRouter
=====
                        BFD Version : 1
                        Admin Status : TRUE
                        Trap Enable  : FALSE
=====
Total session number : 1

UP: 0, DOWN: 1, AdminDown: 0, Init: 0
=====
```

## show ipv6 bfd interfaces

Display Bidirectional Forwarding Detection (BFD) configuration for a port or VLAN on an IPv6 interface.

### Syntax

- **show ipv6 bfd interfaces gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ipv6 bfd interfaces vlan <1-4059>**

### Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Command Mode

User EXEC

### Usage Guidelines

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see [VOSS Feature Support Matrix](#).



## Command Output

The **show ipv6 bfd interfaces** command displays the following information:

Output field	Description
VLAN	Specifies the VLAN ID. The system displays this field only in output for VLAN interfaces.
PORT	Specifies the port number. The system displays this field only in output for GigabitEthernet interfaces.
STATUS	Specifies whether BFD is enabled on the interface.
MIN_RX	Specifies the receive interval in milliseconds.
INTERVAL	Specifies the transmit interval in milliseconds.
MULTIPLIER	Specifies the multiplier used to calculate the amount of time BFD waits before declaring a receive timeout.

## Example

The following example displays port configuration information for BFD.

```
Switch:1>show ipv6 bfd interfaces gigabitethernet 1/3
```

```
=====
```

```
                                Port Bfd
```

```
=====
```

PORT	STATUS	MIN_RX	INTERVAL	MULTIPLIER	VRF-ID
1/3	enable	200	200	3	0

```
=====
```

## show ipv6 bfd neighbors

Display Bidirectional Forwarding Detection (BFD) session information for IPv6 neighbors.

## Syntax

- **show ipv6 bfd neighbors**
- **show ipv6 bfd neighbors next-hop WORD<0-128>**
- **show ipv6 bfd neighbors vrf**
- **show ipv6 bfd neighbors vrfids**

## Command Parameters

**next-hop WORD<0-128>**

Specifies the next-hop IPv6 address in the format a:b:c:d:e:f:g:h.

**vrf**

Specifies a VRF instance by VRF name.

**vrfids**

Specifies a VRF or range of VRFs by ID.

## Command Mode

User EXEC

## Usage Guidelines

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show ipv6 bfd neighbors** command displays the following information:

Output Field	Description
MY_DISC	Specifies the local discriminator for the BFD session.
YOUR_DISC	Specifies the remote discriminator for the BFD session.
NEXT_HOP	Specifies the next-hop IPv6 address.
STATE	Specifies the BFD session state. Possible values are Down, Up, Init, and AdminDown.
MULTI	Specifies the multiplier used to calculate the amount of time BFD waits before declaring a receive timeout.
MIN_TX	Specifies, in microseconds, the minimum interval that the local system prefers to use when transmitting BFD control packets.
MIN_RX	Specifies, in microseconds, the minimum interval between received BFD control packets.
ACT_TX	Specifies, in microseconds, the actual transmission interval.
DETECT_TIME	Specifies the period of time without receiving BFD packets, after which the session is determined to have failed.
REMOTE_STATE	Specifies the BFD session state of the remote system.
APP	Specifies the application configured on the BFD session.
RUN	Specifies the application running on the BFD session.

## Example

The following example displays BFD session information for an IPv6 neighbor.

```
Switch:1>show ipv6 bfd neighbors
-----
                        BFD Session - GlobalRouter
-----
MY_DISC  YOUR_DISC  NEXT_HOP                STATE  MULTI  MIN_TX  MIN_RX  ACT_TX  DETECT_TIME  REMOTE_STATE  APP  RUN
-----
1         0          2001:DB8:0:0:25AB:0:0:1  Down   3      200    200    1000   0          Down         0    0
-----
1 out of 1 BFD session displayed
-----
APP and RUN Legend:
```

B=BGP IPv6, O=OSPFv3, S=IPv6 Static Route

---

## show ipv6 bfd stats

Display Bidirectional Forwarding Detection (BFD) statistics for IPv6 interfaces.

### Syntax

- **show ipv6 bfd stats**
- **show ipv6 bfd stats vrf WORD<1-16>**
- **show ipv6 bfd stats vrfids WORD<0-512>**

### Command Parameters

**vrf**

Specifies a VRF instance by VRF name.

**vrfids**

Specifies a VRF or range of VRFs by ID.

### Command Mode

User EXEC

### Usage Guidelines

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

Output field	Description
MY_DISC	Specifies the local discriminator for the BFD session.
YOUR_DISC	Specifies the remote discriminator for the BFD session.
NEXT_HOP	Specifies the next-hop IPv4 address.
PACKET_IN	Specifies the total number of BFD messages received for this BFD session.
PACKET_OUT	Specifies the total number of BFD messages sent for this BFD session.

Output field	Description
LAST_UP	The value of sysUpTime on the most recent occasion at which the session came up. If no such up event exists this object contains a zero value.
LAST_DOWN	The value of sysUpTime on the most recent occasion at which the last time communication was lost with the neighbor. If no such down event exist this object contains a zero value.

## Example

The following example displays BFD statistics for IPv6 interfaces.

```
Switch:1>show ipv6 bfd stats
=====
BFD staticstics - GlobalRouter
=====
MY_DISC  YOUR_DISC  NEXT_HOP                PACKET_IN  PACKET_OUT  LAST_UP                LAST_DOWN
-----
1         0             2001:DB8:0:0:0:0:ffff  4661750   4620630     Mon Sep  6 15:31:15 2021  Mon Sep
6 15:28:08 2021
-----
```

## show ipv6 dcache

Display the destination cache to see next-hop addresses for destinations. The destination cache is only populated or updated when IPv6 packets originate locally on the central processor of the switch.

## Syntax

- **show ipv6 dcache gigabitethernet {slot/port[sub-port]}**
- **show ipv6 dcache mgmtethernet mgmt**
- **show ipv6 dcache tunnel <1-2000>**
- **show ipv6 dcache vlan <1-4059>**
- **show ipv6 dcache vrf WORD<1-16>**
- **show ipv6 dcache vrfids WORD<0-512>**

## Command Parameters

**gigabitethernet {slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mgmtethernet mgmt**

Identifies the management port.

**tunnel <1-2000>**

Specifies the tunnel ID.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The *mgmtethernet mgmt* parameter only applies to VSP 8600 Series.

## show ipv6 default-routers

---

Display default routers learned from router advertisement messages.

## Syntax

- **show ipv6 default-routers**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 default-routers** command displays the following information:

Parameter	Description
NET ADDRESS	Shows the IPv6 router address received from a valid router advertisement.
VLAN	Shows the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3999. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
LIFETIME	Shows the value placed in the router lifetime field of router advertisements. This value must be either 0 or between 4 and 9000. A value of zero indicates that the system is not a default router. The default is 1800.
IS ACTIVE	Shows if the default router is active or inactive.

## show ipv6 dhcp-relay

Display information about the IPv6 Dynamic Host Configuration Protocol (DHCP) relay counters.

### Syntax

- **show ipv6 dhcp-relay counters**
- **show ipv6 dhcp-relay counters [vrf WORD<1-16>]**
- **show ipv6 dhcp-relay counters [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 dhcp-relay counters [vrfids WORD<0-512>]**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF name.

**vrfids WORD<0-512>**

Specifies a VRF by ID.

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ipv6 dhcp-relay counters** command displays the following information:

Output field	Description
INTERACE	Shows the VLAN or port associated with the respective relay interface.
REQUESTS	Shows the number of DHCP requests on this interface.
REPLIES	Shows the number of DHCP replies on this interface.

```
Switch:1#show ipv6 dhcp-relay counters

=====
                        DHCPv6 Counters
=====
INTERFACE                REQUESTS    REPLIES
-----
1111:0:0:0:0:0:1111      1          1
```

## show ipv6 dhcp-relay fwd-path

Display information about the IPv6 Dynamic Host Configuration Protocol (DHCP) relay forward paths.

### Syntax

- **show ipv6 dhcp-relay fwd-path**
- **show ipv6 dhcp-relay fwd-path [vrf WORD<1-16>]**
- **show ipv6 dhcp-relay fwd-path [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 dhcp-relay fwd-path [vrfids WORD<0-512>]**

### Command Parameters

**vrf WORD<1-16>**

Specifies the name of the VRF.

**vrfids <0-512>**

Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ipv6 dhcp-relay fwd-path** command displays the following information:

Output field	Description
INTERFACE	Shows the VLAN or port associated with the respective relay interface.
SERVER	Specifies the server address.
ENABLE	Specifies if the IPv6 DHCP-relay forwarding path from the client to the server is enabled on the switch.

```
Switch:1(config-if)#show ipv6 dhcp-relay fwd-path
=====
                        DHCPv6 Fwd-path - GlobalRouter
=====
INTERFACE                SERVER                ENABLE
-----
1111:0:0:0:0:0:1111      1234:0:0:0:0:0:1234      enable
```

## show ipv6 dhcp-relay interface

Display information about the IPv6 Dynamic Host Configuration Protocol (DHCP) relay configuration for specific interface(s).

### Syntax

- **show ipv6 dhcp-relay interface**
- **show ipv6 dhcp-relay interface [gigabitethernet]**
- **show ipv6 dhcp-relay interface [gigabitethernet] {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show ipv6 dhcp-relay interface [vlan]**
- **show ipv6 dhcp-relay interface [vlan] [<1-4059>]**
- **show ipv6 dhcp-relay interface [vrf WORD<1-16>]**
- **show ipv6 dhcp-relay interface [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 dhcp-relay interface [vrfids WORD<0-512>]**

### Command Parameters

**gigabitethernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan** <1-4059>



Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies the name of the VRF.

**vrfids <0-512>**

Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 dhcp-relay interface** command displays the following information:

Output field	Description
IF INDEX	Interface If index for which the statistics is captured for this interface.
Descr	Specifies a textual string containing information about the interface. The network management system also configures the Descr string. Type Specifies the type.
MAX HOP	Configures the maximum number of hops before a IPv6 DHCP packet is discarded (1 to 16). The default is 4. To configure this option to the default value, use the default operator with this command.
DHCP-RELAY	Specifies the DHCP Relay for Ipv6 configuration table.
REMOTE-ID	Shows the remote ID associated with the respective interface.

## show ipv6 fhs dhcp-guard policy

Displays DHCP-guard policy information for all the configured DHCP-guard policy.

## Syntax

- **show ipv6 fhs dhcp-guard policy**
- **show ipv6 fhs dhcp-guard policy WORD<1-64>**

## Command Parameters

WORD<1-64>

Specifies the policy name.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 fhs dhcp-guard policy** command displays the following information:

Output field	Description
POLICY-NAME	Indicates the DHCPv6 Guard policy name.
SERVER-ACC-LIST	Indicates if the received DHCPv6 server packet source IPv6 addresss matches the configured IPv6 access list.
REPLY-PREF-LIST	Indicates if the advertised prefix in received DHCPv6 server packet matches the configured IPv6 access list.
MIN-RTR-PREF	Indicates the advertised router preference minimum limit.
MAX-RTR-PREF	Indicates the advertised router preference maximum limit.

## show ipv6 fhs ipv6-access-list

Displays all the configured IPv6 access list in the system.

## Syntax

- **show ipv6 fhs ipv6-access-list**
- **show ipv6 fhs ipv6-access-list WORD<1-64>**

## Command Parameters

WORD<1-64>

Specifies the access list name.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 fhs ipv6-access-list** command displays the following information:

Output field	Description
Access list name	Indicates the IPv6 access list name.
ipv6_prefix	Indicates the IPv6 prefix added to the IPv6 access list.
mask_len	Indicates prefix mask length added to the IPv6 access list.
mask_range_from	Indicates the IPv6 range start mask length.
mask_range_to	Indicates the IPv6 range end mask length.
mode	Indicates the access mode.

## show ipv6 fhs mac-access-list

Displays all the configured MAC access list in the system.

## Syntax

- **show ipv6 fhs mac-access-list**
- **show ipv6 fhs mac-access-list WORD<1-64>**

## Command Parameters

WORD<1-64>

Specifies the MAC access list name.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 fhs mac-access-list** command displays the following information:

Output field	Description
ACC-LIST-NAME	Indicates the MAC access list name.
MAC-ADDRESS	Indicates the MAC address.
ACL-MODE	Indicates the ACL mode.

## show ipv6 fhs port-policy

Displays the RA-guard policy name configured and RA-guard statistics.

### Syntax

- **show ipv6 fhs port-policy**
- **show ipv6 fhs port-policy {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show ipv6 fhs port-policy** command displays the following information:

Output field	Description
PORT	Indicates the port number.
DHCPV6G-POLICY	Indicates the DHCPv6 policy name.
RA-POLICY	Indicates the RA Guard policy name.

## show ipv6 fhs ra-guard policy

Displays configured RA-guard policy information.

### Syntax

- **show ipv6 fhs ra-guard policy**
- **show ipv6 fhs ra-guard policy WORD<1-64>**

## Command Parameters

**WORD<1-64>**

Specifies the policy name.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 fhs ra-guard policy** command displays the following information:

Output field	Description
POL-NAME	Indicates the RA Guard policy name.
DEVICE-ROLE	Indicates if the device role is router or host.
IPv6-ACC-LIST	Indicates the IPv6 access list against which the incoming RA packet's source IPv6 address has to be validated.
MAC-ACC-LIST	Indicates the MAC access list against which the incoming RA packet's source MAC address has to be validated.
PREFIX-LIST	Specifies the IPv6 prefix list against which advertised prefix information in incoming RA packets source need to be validated.
MIN HOP-LIMIT	Indicates the advertised hop count minimum limit.
MAX HOP-LIMIT	Indicates the advertised hop count maximum limit.
MANAGED CONF-FLAG	Indicates the managed address configuration flag status in the advertised RA packet.
RTR-PREF	Indicates the advertised default router preference value.

## show ipv6 fhs snooping binding

Displays entries in the SBT.

## Syntax

- **show ipv6 fhs snooping binding**
- **show ipv6 fhs snooping binding type <dynamic|static>**
- **show ipv6 fhs snooping binding vlan <1-4059>**
- **show ipv6 fhs snooping binding vlan <1-4059> ipv6-address WORD<0-46>**

## Command Parameters

**ipv6-address** WORD<0-46>

Displays a specific binding entry based on its IPv6 address.

**type** <dynamic|static>

Displays binding entries by type.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show ipv6 fhs status

---

Displays the IPv6 First Hop Security (FHS) status information.

## Syntax

- **show ipv6 fhs status**
- **show ipv6 fhs status vlan**
- **show ipv6 fhs status vlan <1-4059>**

## Command Parameters

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show ipv6 forwarding

---

Show IPv6 forwarding information.

### Syntax

- **show ipv6 forwarding**
- **show ipv6 forwarding vrf WORD<1-16>**
- **show ipv6 forwarding vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

### Default

The default is disabled.

## Command Mode

User EXEC

## show ipv6 global

---

Show global IPv6 configuration information.

### Syntax

- **show ipv6 global**
- **show ipv6 global vrf WORD<1-16>**
- **show ipv6 global vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

# show ipv6 interface

---

Show IPv6 information for all or specific interfaces.

## Syntax

- `show ipv6 interface gigabitEthernet [{slot/port[/sub-port]}[-slot/port[/sub-port]][,...]]`
- `show ipv6 interface icmpstatistics`
- `show ipv6 interface icmpstatistics gigabitEthernet [{slot/port[/sub-port]}[-slot/port[/sub-port]][,...]]`
- `show ipv6 interface icmpstatistics loopback <1-256>`
- `show ipv6 interface icmpstatistics mgmtEthernet`
- `show ipv6 interface icmpstatistics mgmtEthernet mgmt`
- `show ipv6 interface icmpstatistics tunnel <1-2000>`
- `show ipv6 interface icmpstatistics vlan <1-4059>`
- `show ipv6 interface icmpstatistics vrf WORD<1-16>`
- `show ipv6 interface icmpstatistics vrfids WORD<0-512>`
- `show ipv6 interface loopback <1-256>`
- `show ipv6 interface mgmtEthernet`
- `show ipv6 interface mgmtEthernet mgmt`
- `show ipv6 interface statistics`
- `show ipv6 interface statistics gigabitEthernet [{slot/port[/sub-port]}[-slot/port[/sub-port]][,...]]`
- `show ipv6 interface statistics loopback <1-256>`
- `show ipv6 interface statistics mgmtEthernet`
- `show ipv6 interface statistics mgmtEthernet mgmt`
- `show ipv6 interface statistics tunnel <1-2000>`
- `show ipv6 interface statistics vlan <1-4059>`
- `show ipv6 interface statistics vrf WORD<1-16>`
- `show ipv6 interface statistics vrfids WORD<0-512>`
- `show ipv6 interface tunnel <1-2000>`
- `show ipv6 interface tunnel vrf WORD<1-16>`
- `show ipv6 interface tunnel vrfids WORD<0-512>`



- **show ipv6 interface vlan** [<1-4059>]
- **show ipv6 interface vrf** WORD<1-16>
- **show ipv6 interface vrfids** WORD<0-512>

## Command Parameters

**gigabitEthernet** {slot/port[/sub-port][/-slot/port[/sub-port]][,...]}

Displays IPv6 interface information for gigabitEthernet. {slot/port[/sub-port][/-slot/port[/sub-port]][,...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**icmpstatistics** [gigabitEthernet | mgmtEthernet | tunnel | vlan]

Shows IPv6 ICMP statistics for the interface as follows: gigabitEthernet-displays interface gigabitEthernet configurations, mgmtEthernet-displays interface mgmtEthernet configurations, tunnel-displays interface tunnel configurations, vlan -displays vlan interface configurations.

**loopback** <1-256>

Displays the interface loopback configurations.

**loopback** <1-256>

Identifies a loopback interface.

**mgmtEthernet** mgmt

Displays IPv6 interface information for the management port.

**statistics** [gigabitEthernet | mgmtEthernet | tunnel | vlan]

Shows IPv6 interface statistics as follows: gigabitEthernet- displays interface gigabitEthernet configurations, mgmtEthernet-displays interface mgmtEthernet configurations, tunnel- displays interface tunnel configurations, vlan -displays vlan interface configurations.

**tunnel** <1-2000>

Displays IPv6 interface information for a tunnel. The tunnel ID is expressed as a value from 1 to 2000.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf** WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

**vrfids** WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The *mgmtethernet* and *mgmtethernet mgmt* parameters only applies to VSP 8600 Series.

## show ipv6 interface loopback

---

Display the IPv6 loopback interface details.

## Syntax

- **show ipv6 interface loopback <1-256>**

## Command Parameters

<1-256>

Specifies the interface ID value.

## Default

None

## Command Mode

User EXEC

## show ipv6 ipvpn

---

Display the configuration for IPv6 VPN enabled VRFs.

## Syntax

- **show ipv6 ipvpn**
- **show ipv6 ipvpn vrf WORD<1-16>**
- **show ipv6 ipvpn vrf WORD<1-16> vrfids WORD<0-512>**
- **show ipv6 ipvpn vrfids WORD<0-512>**

## Command Parameters

vrf WORD<1-16>

Specifies a VRF.

**vrfids WORD<0-512>**

Specifies the VRF ID.

## Default

None

## Command Mode

User EXEC

## Example

The following example displays the command output.

```
Switch:1#show ipv6 ipvpn
=====
                                IPv6  IPVPN
-----
VRF Name          VRF ID   IPv6 IPVPN   IPv4 IPVPN   I-SID   I-SID Name
-----
vrfred             2        enabled  disabled  5555   ISID-5555
-----
1 out of 1 Total IPv6 L3 VSN, 1 active IPv6 and 0 active IPv4 displayed.
```

## show ipv6 mld cache

Displays the learned multicast groups in the cache

## Syntax

- **show ipv6 mld cache**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mld cache** command displays the following information:

Output field	Description
GRPADDR	Indicates the IPv6 address of the multicast address of interest.
LASTREPORTER	Indicates the IPv6 address of the last reporter.
INTERFACE	Indicates the ingress interface for MLDv2.
EXPIRATION	Displays the minimum amount of time remaining before this entry ages out. A value of 0 indicates that the entry will age out immediately if the router leaves the group.

## Example

The following example displays the learned multicast groups in the cache.

```
Switch:1#show ipv6 mld cache
=====
                        MLD Cache Information
=====
GRPADDRESS/LASTREPORTER          INTERFACE  EXPIRATION
-----
ff03:0:0:0:0:0:0:0/              Vlan10    0 day(s), 00h:04m:12s
fe80:0:0:0:200:9aff:fe68:3dd5

1 out of 1 entries displayed
```

## show ipv6 mld group

Displays MLD group information

## Syntax

- **show ipv6 mld group**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mld group** command displays the following information:

Output field	Description
GRPADDR	Specifies the multicast group address that others want to join to. A group address can be the same for many incoming ports.
MEMBER	Specifies the IP address of a source that has sent group report wishing to join this group.
INPORT	Identifies a physical interface or a logical interface which has received group reports from various sources.
EXPIRATION	Specifies the time left before group report expires on this port. This is updated upon receiving a group report.

## Example

The following example displays the MLD group information.

```
Switch:1#show ipv6 mld group
=====
                        Mld Group - GlobalRouter
=====
GRPADDR/MEMBER                               INPORT           EXPIRATION
-----
ff1e:0000:0000:0000:0000:0002:4444/          V666-6/41        0
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2c

1 out of 1 group Receivers displayed

Total number of unique groups 1 text
```

## show ipv6 mld group count

Displays the number of MLD entries

## Syntax

- **show ipv6 mld group count**

## Default

None

## Command Mode

User EXEC

## show ipv6 mld group group

Displays the MLD group IPv6 address

## Syntax

- **show ipv6 mld group group WORD<0-255>**

## Command Parameters

**{slot/port [-slot/port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**detail**

Displays mldv2 specific data.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**WORD<0-255>**

Specifies the IPv6 address.

## Default

None

## Command Mode

User EXEC

## show ipv6 mld group group WORD<0-255> detail

---

Displays MLDv2 specific data

## Syntax

- **show ipv6 mld group group WORD<0-255> detail port {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} Ports list {slot/port [-slot/port]}**
- **show ipv6 mld group group WORD<0-255> detail vlan <1-4059>**

## Command Parameters

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags,

the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Example

The following example displays detailed MLD group information.

```
Switch:1#show ipv6 mld group group ff1e:0000:0000:0000:0000:0000:0002:4444 detail

=====
                          Mld Group Detail - GlobalRouter
=====

Interface:                  Vlan666-6/41
MLDv2 Group:                ff1e:0000:0000:0000:0000:0000:0002:4444
Interface Group Mode:      EXCLUDE
Interface Compatibility Mode: MLD_V2
Interface Group Timer:     258
Vl Host Timer:             Not Running
Interface Group Include Source List:
    Source Address          Expires
    2001:0db8:3c4d:0015:0000:0000:1a2f:1aaa    258
Interface Group Exclude Source List :
    Source Address          Expires
    2001:0db8:3c4d:0015:0000:0000:1a2f:1bbb    N/A
```

## show ipv6 mld group member-subnet

Displays the MLD IPv6 address and network mask

## Syntax

- **show ipv6 mld group member-subnet WORD<0-255>**

## Command Parameters

**WORD<0-255>**

Specifies the IPv6 address or the network mask.

## Default

None

## Command Mode

User EXEC

## show ipv6 mld interface

Displays the IPv6 MLD interface information

## Syntax

- **show ipv6 mld interface**
- **show ipv6 mld interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show ipv6 mld interface vlan <1-4059>**

## Command Parameters

**gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Displays the interface gigabitEthernet MLD interface information. {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mld interface** command displays the following information:

Output field	Description
IF	Specifies the internetwork layer interface value of the interface for which MLD is enabled.
STATUS	Indicates if MLD is activated on the interface.



Output field	Description
VERSION	Indicates the version.
QUERIER	Indicates the address of the MLD Querier on the IPv6 subnet to which this interface attaches.
JOINS	Indicates the number of times a group membership has been added on this interface.
VLAN ID	Indicates the VLAN ID of the physical interface.
PORT NUM	Indicates the port number of the physical interface.
QUERY INTVL	Indicates the query interval, the frequency at which IPv6 MLD snooping host-query packets are transmitted on this interface.
QUERY MAX RESP	Indicates the maximum query response time advertised in IPv6 MLD snooping queries on this interface.
ROBUST	Indicates the robustness value.
LAST LIST QUERY	Indicates the last listener query interval. The last listener query interval is the maximum response delay inserted into group-specific queries sent in response to leave group messages, and it is also the amount of time between group-specific query messages.
SNOOP ENABLE	Indicates if snooping is enabled.
SSM SNOOP ENABLE	Indicates if ssm-snooping is enabled.
DYNAMIC DOWNGRADE ENABLE	Enables dynamic downgrade of the MLD version when older version query message is received.

## Examples

The following example displays MLD interface information.

```
Switch:1#show ipv6 mld interface
=====
                        Mld Interface - GlobalRouter
=====
IF      STATUS VERS  OPER VERS  QUERIER                               Wrong Query JOINS MODE
-----
P6/3   inact  2    2        2001:0db8:3c4d:0015:0000:0000:1a2f:1aaa  0              0    pim
V666   inact  2    2        2001:0db8:3c4d:0015:0000:0000:1a2f:1bbb  0              0    pim

Switch:1#show ipv6 mld interface vlan 10
=====
                        Vlan IPv6 Mld
=====
VLAN QUERY QUERY ROBUST VERSION LAST  SNOOP SSM    DYNAMIC
ID  INTVL MAX  RESP          LIST  ENABLE SNOOP  DOWNGRADE
-----
10  125  10   2    1    1    false false  enabled

Switch(config)#show ipv6 mld interface gigabitethernet 1/11
=====
                        Port IPv6 MLD
=====
PORT QUERY QUERY ROBUST VERSION LAST  DYNAMIC
NUM  INTVL MAX  RESP          LIST  DOWNGRADE
```

```
-----
      RESP                QUERY
-----
1/11 125  10   2    1    1    enabled
-----
1 out of 1 entries displayed
```

---

## show ipv6 mld sender

Displays the MLD sender list

### Syntax

- **show ipv6 mld sender**
- **show ipv6 mld sender count**
- **show ipv6 mld sender group WORD<0-255>**
- **show ipv6 mld sender sender-subnet WORD<0-255>**

### Command Parameters

#### count

Displays number of MLD entries.

#### group WORD<0-255>

Displays the MLD IPv6 group address.

#### sender-subnet WORD<0-255>

Displays the MLD IPv6 address and network mask.

### Default

None

### Command Mode

User EXEC

---

## show ipv6 mld snooping

Displays MLD snooping information

### Syntax

- **show ipv6 mld snooping**

### Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mld snoop** command displays the following information:

Output field	Description
IFINDEX	Identifies the index of the physical interface.
SNOOP ENABLE	Identifies whether snoop is enabled (true) or disabled (false).
SSM SNOOP ENABLE	Identifies whether SSM snoop is enabled (true) or disabled (false).
ACTIVE MROUTER PORTS	Displays all dynamic (querier port) and static mrouter ports that are active on the interface.
MROUTER EXPIRATION TIME	Specifies the time remaining before the multicast router is aged out on this interface. If the switch does not receive queries before this time expires, it flushes out all group memberships known to the VLAN. The Query Max Response Interval (obtained from the queries received) is used as the timer resolution.

## Example

The following example displays the MLD snooping configuration status.

```
Switch:1#show ipv6 mld snoop
=====
                          Mld Snooping - GlobalRouter
=====
IFINDEX SNOOP   SSM   ACTIVE   MROUTER
          ENABLE SNOOP MROUTER  EXPIRATION
          ENABLE ENABLE PORTS   TIME
-----
V666   False   False  NONE    0
1 out of 1 entries displayed
```

## show ipv6 mld snoop-trace

Displays MLD snooping tracing information

## Syntax

- **show ipv6 mld snoop-trace**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mld snoop-trace** command displays the following information:

Output field	Description
GROUP ADDRESS	Specifies the IP multicast address of the group traversing the router
SOURCE ADDRESS	Specifies the IP source address of the multicast group address.
IN VLAN	Specifies the ingress VLAN ID for the multicast source.
IN PORT	Specifies the ingress port for the multicast group.
OUT VLAN	Specifies the egress VLAN ID for the multicast group.
OUT PORT	Specifies the egress port of the multicast group.
TYPE	Specifies the port type on which the snoop entry is learnt.

## Example

The following example displays MLD snooping tracing information.

```
Switch:1#show ipv6 mld snoop-trace
=====
                        Mld Snoop Trace - GlobalRouter
=====
GROUP/
SOURCE          IN    IN  OUT  OUT  TYPE
ADDRESS         VLAN  PORT VLAN  PORT
-----
ff10:0:0:0:0:0:1/  10   2/15 10   3/16  ACCESS
5051:0:0:0:0:1:84:51
```

## show ipv6 mld sys

Displays MLD system parameters

### Syntax

- **show ipv6 mld sys**

### Default

None

### Command Mode

User EXEC

## show ipv6 mld-host-cache

Displays the learned multicast group addresses in the host cache.

## Syntax

- **show ipv6 mld-host-cache**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mld-host-cache** command displays the following information:

Output field	Description
GRPADDRESS	Shows the IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP router.
SELF	Indicates whether or not the group is locally registered into MLD Host Cache. <ul style="list-style-type: none"> <li>• enabled — group is locally registered into MLD Host Cache</li> <li>• disabled — group is not locally registered into MLD Host Cache</li> </ul>
PORT/VID	Shows the port or VLAN that learns the multicast group.

## show ipv6 mroute interface

Displays the IPv6 mroute interface information

## Syntax

- **show ipv6 mroute interface**
- **show ipv6 mroute interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mroute interface** command displays the following information:

Output field	Description
INTERFACE	Displays the slot and port number or VLAN ID for this entry.
TTL	Displays the datagram time-to-live (TTL) threshold for the interface. IPv6 multicast datagrams with a TTL less than this threshold are not forwarded out of the interface. The default value of 0 means that all multicast packets are forwarded out of the interface.
PROTOCOL	Displays the protocol as one of the following: <ul style="list-style-type: none"> <li>other(1): none of the following</li> <li>local(2): manually configured</li> <li>netmgmt(3): configured by a network management protocol</li> <li>pimSparseMode(8): PIM-SMv2</li> <li>igmpOnly(10)</li> <li>pimSsmMode(11)</li> <li>spb</li> </ul>

## Example

The following example displays the IPv6 mroute interface information.

```
Switch:1>show ipv6 mroute interface

=====
                        Mroute Interface - GlobalRouter
=====
INTERFACE    TTL        PROTOCOL
-----
VLAN 2       1          pimsm
VLAN 7       1          pimsm
VLAN 10      1          pimsm
VLAN 20      1          pimsm

4 out of 4 total mroute entries displayed
```

## show ipv6 mroute next-hop

Displays the IPv6 mroute next-hop information

## Syntax

- **show ipv6 mroute next-hop**
- **show ipv6 mroute next-hop vlan <1-4059>**

## Command Parameters

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mroute next-hop** command displays the following information:

Output field	Description
Group	Displays the IPv6 multicast group for this entry that specifies a next hop on an outgoing interface.
Source	Displays the network address that, when combined with the corresponding next hop SourceMask value, identifies the source for this entry that specifies a next hop on an outgoing interface.
Source Mask	Displays the network mask that, when combined with the corresponding next hop Source value, identifies the source for this entry that specifies a next hop on an outgoing interface.
State	Displays whether the outgoing interface and next hop represented by this entry is currently being used to forward IPv6 datagrams as one of the following: <ul style="list-style-type: none"> <li>forwarding: Indicates that it is currently being used</li> <li>pruned: Indicates that it is not being used</li> </ul>
Expire Time	Displays the minimum amount of time that remains before this entry ages out. The value 0 indicates that the entry is not subject to aging.

Output field	Description
Protocol	Displays the protocol as one of the following: <ul style="list-style-type: none"> <li>• other(1): none of the following</li> <li>• local(2): manually configured</li> <li>• netmgmt(3): configured by a network management protocol</li> <li>• pimSparseMode(8): PIM-SMv2</li> <li>• igmpOnly(10)</li> <li>• pimSsmMode(11)</li> <li>• spb</li> </ul>
Closest Member Hops	Displays the minimum number of hops between this router and any member of this IPv6 multicast group reached via this next hop on this outgoing interface. Any IPv6 multicast datagrams for the group which have a TTL less than this number of hops is not forwarded to this next hop.

## Example

The following example displays the IPv6 mroute next-hop information.

```
Switch:1>show ipv6 mroute next-hop vlan 2
=====
Mroute Next-Hop - GlobalRouter
=====
Vlan:          VLAN 2
Port:          -
Group:         ff30:0:0:0:0:0:0:1
Source:        5010:0:0:0:0:1:82:10
Source Mask:   64
State:         pruned
Expire Time:   202
Protocol:      pimsm
Closest Member Hops: 0
-----
Vlan:          VLAN 2
Port:          -
Group:         ff30:0:0:0:0:0:0:1
Source:        5010:0:0:0:0:1:82:11
Source Mask:   64
State:         pruned
Expire Time:   175
Protocol:      pimsm
Closest Member Hops: 0
-----
2 out of 4 total mroute entries displayed
-----
```

## show ipv6 mroute route

Displays the IPv6 mroute route information

### Syntax

- **show ipv6 mroute route**



## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 mroute route** command displays the following information:

Output field	Description
GROUP	Displays the IPv6 multicast group for this entry that specifies a next hop on an outgoing interface.
SRCMASK	Displays the network mask that, when combined with the corresponding next hop Source value, identifies the source for this entry that specifies a next hop on an outgoing interface.
UPSTREAM_NBR	Shows the address of the upstream neighbor from which the IPv6 datagrams from these sources are received.
SOURCE	Displays the network address that, when combined with the corresponding next hop SourceMask value, identifies the source for this entry that specifies a next hop on an outgoing interface.
IF	Displays the slot and port number or VLAN ID for this entry.
EXPIR	Displays the minimum amount of time that remains before this entry ages out. The value 0 indicates that the entry is not subject to aging.
PROT	Displays the protocol as one of the following: <ul style="list-style-type: none"> <li>other(1): none of the following</li> <li>local(2): manually configured</li> <li>netmgmt(3): configured by a network management protocol</li> <li>pimSparseMode(8): PIM-SMv2</li> <li>igmpOnly(10)</li> <li>pimSsmMode(11)</li> <li>spb</li> </ul>

## Example

The following example displays the IPv6 mroute route information.

```
Switch:1>show ipv6 mroute route

=====
                        Mroute Route - GlobalRouter
=====
GROUP                               SOURCE
SRCMASK
      UPSTREAM_NBR                    IF      EXPIR    PROT
-----
ff30:0:0:0:0:0:1                    5010:0:0:0:0:1:82:10      64
      0:0:0:0:0:0:0:0                VLAN 10    202      pimsm
```

```

ff30:0:0:0:0:0:1          5010:0:0:0:0:1:82:11      64
      0:0:0:0:0:0:0          VLAN 10      175      pimsm
2 out of 2 total mroute entries displayed

```

## show ipv6 mroute stats

Display IPv6 multicast route statistics.

### Syntax

- **show ipv6 mroute stats**
- **show ipv6 mroute stats [WORD<7-400> ]**

### Command Parameters

WORD<7-400>

Displays the IPv6 multicast route statistics. You can specify up to 10 group addresses in a single command by separating addresses with a comma ( , ).

### Default

None

### Command Mode

User EXEC

### Command Output

The **show ipv6 mroute stats** command displays the following information:

Output field	Description
GroupAddress	Specifies the multicast group IP address for which to show statistics.
SourceCounter	Specifies the number of sources associated with the multicast route record.
IngressPackets	Specifies the number of packets received for the associated IP address.
IngressBytes	Specifies the number of bytes received for the associated IP address.
AverageSize	Specifies the average packet length for the associated group IP address. This information indicates only the ingress packet length and is calculated using the formula: ingress packet/ingress byte.

---

## show ipv6 nd interface

---

View neighbor discovery interface configuration.

### Syntax

- **show ipv6 nd interface gigabitEthernet** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]]
- **show ipv6 nd interface mgmtEthernet mgmt**
- **show ipv6 nd interface vlan** [<1-4059>]
- **show ipv6 nd interface vrf** WORD<1-16>
- **show ipv6 nd interface vrfids** WORD<0-512>

### Command Parameters

**gigabitEthernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mgmtEthernet mgmt**

Displays the neighbor discovery management interface configuration.

**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf** WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

**vrfids** WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

The *mgmtethernet mgmt* parameter only applies to VSP 8600 Series.

---

## show ipv6 nd-prefix

---

View all configured neighbor discovery prefixes.

### Syntax

- `show ipv6 nd-prefix [detail]`
- `show ipv6 nd-prefix detail vrf WORD<1-16>`
- `show ipv6 nd-prefix detail vrfids WORD<0-512>`
- `show ipv6 nd-prefix interface gigabitEthernet [{slot/port[/sub-port]}[-slot/port[/sub-port]][, ...]]`
- `show ipv6 nd-prefix interface vlan [<1-4059>]`
- `show ipv6 nd-prefix vrf WORD<1-16>`
- `show ipv6 nd-prefix vrfids WORD<0-512>`

### Command Parameters

#### detail

Shows detailed information.

#### gigabitEthernet {slot/port[/sub-port]}[-slot/port[/sub-port]][,...]

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

#### vlan <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

#### vrf WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

#### vrfids WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

### Default

None

### Command Mode

User EXEC

---

## show ipv6 neighbor

---

View entries in the neighbor cache.

### Syntax

- **show ipv6 neighbor**
- **show ipv6 neighbor interface gigbitethernet {slot/port[sub-port]}**
- **show ipv6 neighbor interface mgmtEthernet**
- **show ipv6 neighbor interface mgmtEthernet mgmt**
- **show ipv6 neighbor interface mlt <1-512>**
- **show ipv6 neighbor interface mlt <1-512> vrf WORD<1-16>**
- **show ipv6 neighbor interface mlt <1-512> vrfids WORD<0-512>**
- **show ipv6 neighbor interface vlan <1-4059>**
- **show ipv6 neighbor type <1-4>**
- **show ipv6 neighbor type <1-4> vrf WORD<1-16>**
- **show ipv6 neighbor type <1-4> vrfids WORD<0-512>**
- **show ipv6 neighbor vrf WORD<1-16>**
- **show ipv6 neighbor vrfids WORD<0-512>**
- **show ipv6 neighbor WORD<0-46>**
- **show ipv6 neighbor WORD<0-46> vrf WORD<1-16>**
- **show ipv6 neighbor WORD<0-46> vrfids WORD<0-512>**

### Command Parameters

**{slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**<1-512>**

Specifies the MLT ID.

**mgmtEthernet [mgmt]**

Displays neighbor entries for a management port.

**type <1-4>**

Specifies the type of mapping: 1: other, 2: dynamic, 3: static, or 4: local.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf WORD<1-16>**

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

**WORD<0-46>**

Specifies the neighbor address.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The *mgmtethernet mgmt* parameter only applies to VSP 8600 Series.

## show ipv6 ospf

---

Show the IPv6 OSPFv3 global configuration.

## Syntax

- **show ipv6 ospf**

## Default

None

## Command Mode

User EXEC

## show ipv6 ospf area

---

Show the IPv6 OSPFv3 area configuration.

## Syntax

- **show ipv6 ospf area [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf area vrf WORD<1-16>**
- **show ipv6 ospf area vrfids WORD<0-512>**

## Command Parameters

**vrf** <WORD 1-16>

Specifies the VRF name.

**vrfids** <WORD 0-512>

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ipv6 ospf area-range

---

Show the IPv6 OSPFv3 range configuration.

## Syntax

- **show ipv6 ospf area-range [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf area-range vrf WORD<1-16>**
- **show ipv6 ospf area-range vrfids WORD<0-512>**

## Command Parameters

**vrf** <WORD 1-16>

Specifies the VRF name.

**vrfids** <WORD 0-512>

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ipv6 ospf ase

---

Show the IPv6 OSPFv3 as-external LSAs.

## Syntax

- **show ipv6 ospf ase** [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]
- **show ipv6 ospf ase vrf** WORD<1-16>
- **show ipv6 ospf ase vrfids** WORD<0-512>

## Command Parameters

**metric-type <1-2>**

Specifies the external type.

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

---

## show ipv6 ospf ase metric-type

Display Ipv6 as-external LSA's.

## Syntax

- **show ipv6 ospf ase metric-type** [**vrf WORD<1-16>**] [**vrfids WORD<0-512>**]
- **show ipv6 ospf ase metric-type vrf** WORD<1-16>
- **show ipv6 ospf ase metric-type vrfids** WORD<0-512>

## Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None



## Command Mode

User EXEC

## show ipv6 ospf interface

---

Show the IPv6 OSPFv3 interface configuration.

### Syntax

- **show ipv6 ospf interface [gigabitEthernet {slot/port[sub-port]}] [vlan<1-4059>]**
- **show ipv6 ospf interface [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf interface vrf WORD<1-16>**
- **show ipv6 ospf interface vrfids WORD<0-512>**

### Command Parameters

{slot/port[sub-port]}

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

### Default

None

## Command Mode

User EXEC

## show ipv6 ospf int-timers

---

Show the IPv6 OSPFv3 interface timers.

## Syntax

- **show ipv6 ospf int-timers [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf int-timers vrf WORD<1-16>**
- **show ipv6 ospf int-timers vrfids WORD<0-512>**

## Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ipv6 ospf lsdb

---

Show the IPv6 OSPFv3 Link-state database configuration.

## Syntax

- **show ipv6 ospf lsdb**
- **show ipv6 ospf lsdb [area <A.B.C.D>] [lsa-type <1-11>] [lsid <0-4294967295>] [scope <1-3>] [adv-rtr <A.B.C.D>] [vrf WORD<1-16>] [vrfids WORD<0-512>] [detail]**
- **show ipv6 ospf lsdb [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf lsdb adv-rtr {A.B.C.D}**
- **show ipv6 ospf lsdb adv-rtr {A.B.C.D} [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf lsdb area {A.B.C.D}**
- **show ipv6 ospf lsdb detail**
- **show ipv6 ospf lsdb detail [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf lsdb interface gigabitEthernet {slot/port[sub-port]}**
- **show ipv6 ospf lsdb interface vlan <1-4059>**
- **show ipv6 ospf lsdb lsa-type <1-11>**
- **show ipv6 ospf lsdb lsid <0-4294967295>**
- **show ipv6 ospf lsdb scope <1-3>**
- **show ipv6 ospf lsdb tunnel <1-2000>**

- **show ipv6 ospf lsdb vrf WORD<1-16>**
- **show ipv6 ospf lsdb vrfids WORD<0-512>**

## Command Parameters

**adv-rtr {A.B.C.D}**

Specifies the advertise router configurations.

**area {A.B.C.D}**

Specifies the ipv6 lsdb area configurations.

**gigabitEthernet {slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**interface**

Specifies the ipv6 ospf lsdb interface configurations.

**lsa-type <1-11>**

Specifies the ipv6 ospf lsdb lsa-type.

**lsid <0-4294967295>**

Specifies the ospf lsdb configuration for specific lsid.

**scope <1-3>**

Specifies the ipv6 ospf lsdb scope.

**tunnel <1-2000>**

Specifies the ipv6 ospf lsdb tunnel parameters.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

---

## show ipv6 ospf nbma-nbr interface

---

Show the IPv6 OSPFv3 NBMA neighbor configuration.

### Syntax

- **show ipv6 ospf nbma-nbr interface gigabitEthernet {slot/port[sub-port]} [WORD<1-46>]**
- **show ipv6 ospf nbma-nbr interface vlan <1-4059> [WORD<1-46>]**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**gigabitEthernet {slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**WORD<1-46>**

Specifies an IPv6 address.

### Default

None

### Command Mode

User EXEC

---

## show ipv6 ospf neighbor

---

Show the IPv6 OSPFv3 neighbor configuration.

### Syntax

- **show ipv6 ospf neighbor [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf neighbor vrf WORD<1-16>**
- **show ipv6 ospf neighbor vrfids WORD<0-512>**

### Command Parameters

vrf <WORD 1-16>

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ipv6 ospf redistribute

---

Show the IPv6 OSPFv3 redistribution configuration.

## Syntax

- **show ipv6 ospf redistribute [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf redistribute vrf WORD<1-16>**
- **show ipv6 ospf redistribute vrfids WORD<0-512>**

## Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

## show ipv6 ospf statistics

---

Show the IPv6 OSPFv3 statistics.

## Syntax

- **show ipv6 ospf statistics [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 ospf statistics vrf WORD<1-16>**

- **show ipv6 ospf statistics vrfids WORD<0-512>**

## Command Parameters

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 ospf statistics** command displays the following information:

Output field	Description
NumTxPkt	Shows the count of sent packets.
NumRxPkt	Shows the count of received packets.
NumTxDropPkt	Shows the count of sent, dropped packets.
NumRxDropPkt	Shows the count of received, dropped packets.
NumRxBadPkt	Shows the count of received, bad packets.
NumSpfRun	Shows the count of intra-area route table updates with calculations using this area link-state database.
LastSpfRun	Shows the count of the most recent SPF run.
LsdbTblSize	Shows the size of the link-state database table.
NumBadLsReq	Shows the count of bad link requests.
NumSeqMismatch	Shows the count of sequence mismatched packets.

## show ipv6 pim

Displays PIM IPv6 configurations.

## Syntax

- **show ipv6 pim**

## Default

None

## Command Mode

User EXEC

## Example

```
Switch:1#show ipv6 pim
```

```
=====
                        Pim General Group - GlobalRouter
=====
PimStat          : enabled
Mode             : sparse
StaticRP         : disabled
SptInfiniteThreshold : enabled
FwdCacheTimeout  : 210
DiscDataTimeout  : 60
RegSupprTimeout  : 60
UniRouteChangeTimeout : 5
JoinPruneInt     : 60
```

## show ipv6 pim active-rp

Displays information about the active rendezvous point (RP) for all groups or a specific group.

## Syntax

- **show ipv6 pim active-rp**
- **show ipv6 pim active-rp group**

## Command Parameters

**group**

Specifies the IPv6 group address.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 pim active-rp** command displays the following information:

Output field	Description
GRPADDR	Shows the IPv6 address of the multicast group.
RP-ADDR	Shows the IPv6 address of the RP router. This address can be one of the local PIM-SM enabled interfaces or a global IPv6 address of the chosen RP based on hash function.
RP-PRIORITY	Shows the priority of the RP.

## Example

The following example displays information about the active rendezvous point (RP) for all groups. If you do not specify an IPv6 address, you receive information about the active RP for all running multicast groups on the switch.

```
Switch:1>show ipv6 pim active-rp
=====
                        Pim Grp->RP Active RP Table - GlobalRouter
=====
GRPADDR/
RP-ADDR                               RP-PRIORITY
-----
ff30:0:0:0:0:0:0:1
5040:0:0:0:0:1:84:1
```

## show ipv6 pim interface

Displays information about the IPv6 PIM-SM interface configuration on the switch.

## Syntax

- **show ipv6 pim interface**
- **show ipv6 pim interface gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show ipv6 pim interface vlan <1-4059>**

## Command Parameters

**gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the



*vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 pim interface** command displays the following information:

Output field	Description
IF	Indicates the slot and port number or VLAN ID of the interface where PIM is enabled.
MODE	Indicates the configured mode of this interface. The valid modes are SSM and Sparse.
HLINT	Specifies how long to wait (in seconds) before the PIM router sends out the next hello message to neighboring switches. The default hello interval is 30 seconds.
JPINT	Specifies how long to wait (in seconds) before the PIM router sends out the next join or prune message to its upstream neighbors. The default join and prune interval is 60 seconds.
OPSTAT	Indicates the status of PIM on this interface: up or down.
INTF TYPE	Indicates the PIM interface type. The PIM interface type is active.
VLAN-ID or PORT-NUM	Indicates the slot and port number or VLAN ID of the interface where PIM is enabled.
PIM ENABLE	Indicates the administrative status of PIM.
MODE	Indicates the configured mode of this interface. The valid modes are SSM and Sparse.
HELLOINT	Specifies how long to wait (in seconds) before the PIM router sends out the next hello message to neighboring switches. The default hello interval is 30 seconds.
JPINT	Specifies how long to wait (in seconds) before the PIM router sends out the next join or prune message to its upstream neighbors. The default join and prune interval is 60 seconds.
INTF TYPE	Indicates the PIM interface type. The PIM interface type is active.

## Example

The command displays information about the IPv6 PIM-SM interface configuration on the switch.

```
Switch:1>show ipv6 pim interface
=====
                        Pim Interface - GlobalRouter
=====
IF                MODE        HLINT    JPINT    OPSTAT    INTF TYPE
-----
Vlan2             sparse    30       60       up        active
  ADDR/MASK : fe80:0:0:0:12cd:aeff:fe6a:1902/64
  DR        : fe80:0:0:0:12cd:aeff:fe6a:1902

Vlan7             sparse    30       60       up        active
  ADDR/MASK : fe80:0:0:0:12cd:aeff:fe6a:1903/64
  DR        : fe80:0:0:0:b647:5eff:fe3a:8582

Vlan10            sparse    30       60       up        active
  ADDR/MASK : fe80:0:0:0:12cd:aeff:fe6a:1900/64
  DR        : fe80:0:0:0:12cd:aeff:fe6a:1900

Vlan20            sparse    30       60       up        active
  ADDR/MASK : fe80:0:0:0:12cd:aeff:fe6a:1901/64
  DR        : fe80:0:0:0:12cd:aeff:fe6a:1901

Total PIM Interface Entries:  4/0
=====
```

## show ipv6 pim mode

Displays the IPv6 PIM mode.

### Syntax

- **show ipv6 pim mode**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show ipv6 pim mode** command displays the following information:

Output field	Description
Mode	Indicates the PIM mode as SM or SSM.

## Example

The following example displays the IPv6 PIM mode (SM or SSM).

```
Switch:1>show ipv6 pim mode

=====
                          Pim Global Mode - GlobalRouter
=====
Mode      : sparse
```

## show ipv6 pim mroute

Displays the IPv6 mroute information

### Syntax

- **show ipv6 pim mroute**
- **show ipv6 pim mroute source WORD<0-255>**

### Command Parameters

**group WORD<0-255>**

Specifies mroute information for the group.

**source WORD<0-255>**

Specifies mroute information for the source.

**terse**

Displays brief configuration settings for mroute.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show ipv6 pim mroute** command displays the following information:

Output field	Description
Src	Displays the IPv6 address of the source that sends the multicast stream. A nonzero value indicates that a source sends multicast traffic. 0:0:0:0:0:0:0:0 indicates that this entry is created in response to a receiver that wants to receive this traffic.
Grp	Displays the IPv6 multicast group address.
RP	Displays the IPv6 address of the RP router.

Output field	Description
Upstream	Displays the IPv6 address of the nexthop router towards the source of the multicast traffic or RP.
Flags	Displays the flags configured based on the condition of the receivers, the RP, and the senders. Use the legend at the bottom of the output to explain the flag values.
Incoming Port	Lists the port through which a multicast packet can ingress. If the port is a member of a Multi-Link Trunk (MLT), the packets can ingress on any port of the MLT.
Outgoing Ports	Lists all ports through which traffic that enters on incoming ports exit.
Joined Ports	Lists all ports that received PIM join messages.
Pruned Ports	Lists all ports that received PIM prune messages.
Leaf Ports	Lists multicast receivers that directly connect to the router.
Asserted Ports	Lists all ports that received assert messages. The router uses assert messages to help determine the best path to the source.
Prune Pending Ports	Lists all ports currently in the prune-pending state.
Assert Winner Ifs	Lists interfaces elected the assert winner. The winner continues to forward multicast traffic to the LAN.
Assert Loser Ifs	Lists interfaces not elected as the assert winner. The loser interface is pruned.
Timers	Displays the up time and expiration time for the entry in the routing table.
AssertVifTimer	Displays the time after which the assert winner state refreshes.

## Example

The following commands displays information from the route table.

```
Switch:1>show ipv6 pim mroute
=====
                        Pim Multicast Route - GlobalRouter
=====

Src: 5010:0:0:0:0:1:82:10
Grp: ff30:0:0:0:0:0:0:1
RP: 5040:0:0:0:0:1:84:1
Upstream: NULL
Flags: SPT CACHE SG
Incoming Port: Vlan10-1/9,
Outgoing Ports: Vlan7-1/41/3-1/41/4,
Joined Ports: Vlan7-1/41/3 (MLT- 7),
Pruned Ports: Vlan2-1/41/1 (MLT- 2),
Leaf Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS  Assert
    203    0   39     0
```

```

VLAN-Id:      2      7      10     20
Join-P:       0     160     0      0
Assert:       0      0      0      0
-----
Src: 5010:0:0:0:0:1:82:11
Grp: ff30:0:0:0:0:0:0:1
RP: 5040:0:0:0:0:1:84:1
Upstream: NULL
Flags: SPT CACHE SG
Incoming Port: Vlan10-1/9,
Outgoing Ports: Vlan7-1/41/3-1/41/4,
Joined Ports: Vlan7-1/41/3 (MLT- 7),
Pruned Ports: Vlan2-1/41/1 (MLT- 2),
Leaf Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:
  Entry   JP   RS  Assert
    176    0   34     0
VLAN-Id:      2      7      10     20
Join-P:       0     173     0      0
Assert:       0      0      0      0
-----

Total Num of Entries Displayed 2/2
Flags Legend:
SPT = Shortest path tree, WC=(*,Grp) entry, RP=Rendezvous Point tree, CACHE=Kernel Cache,
ASSERTED=Asserted, SG=(Src,Grp) entry, PMBR=(*,*,RP) entry, FWD_TO_RP=Forwarding to RP,
FWD_TO_DR=Forwarding to DR, SG_NODATA=SG Due to Join, CP_TO_CPU=Copy to CPU, STATIC_MROUTE=Static
Mroute, MRTF_SMLT_PEER_SG=Peer SG On Non-DR For SMLT
-----

```

## show ipv6 pim neighbor

Displays information about the neighboring routers configured with IPv6 PIM-SM

### Syntax

- **show ipv6 pim neighbor**
- **show ipv6 pim neighbor WORD<0-255>**

### Command Parameters

**WORD<0-255>**

Specifies the IPv6 address.

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ipv6 pim neighbor** command displays the following information:

Output field	Description
INTERFACE	Indicates the interface number.
ADDRESS	Indicates the IPv6 address of the PIM neighbor.
UPTIME	Indicates the elapsed time since this PIM neighbor last became a neighbor of the local router.
EXPIRE	Indicates the time that remains before this PIM neighbor times out.

## Example

The following example displays information about the neighboring routers configured with IPv6 PIM-SM.

```
Switch:1>show ipv6 pim neighbor
=====
                          Pim Neighbor - GlobalRouter
=====
INTERFACE ADDRESS                               UPTIME                               EXPIRE
-----
Vlan2      fe80:0:0:0:12cd:aeff:fe69:f900  0 day(s), 00:08:33  0 day(s), 00:01:43
Vlan7      fe80:0:0:0:b647:5eff:fe3a:8582  0 day(s), 00:08:30  0 day(s), 00:01:18

Total PIM Neighbors Displayed:  2/2
=====
```

## show ipv6 pim rp-hash

display information about the RPs selected for a multicast group

### Syntax

- **show ipv6 pim rp-hash**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show ipv6 pim rp-hash** command displays the following information:

Output field	Description
GRPADDRESS	Shows the IPv6 address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP router.
GRPMASK	Shows the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP router.
RP-ADDR	Shows the IPv6 address of the static RP.
HOLDTIME	Shows the hold time of the static RP. The value is 0.
EXPTIME	Shows the minimum time remaining before the static RP is down. The value is 0.

## Example

The following example displays information about the RPs selected for a multicast group.

```
Switch:1>show ipv6 pim rp-hash
=====
                          Pim RPSet - GlobalRouter
=====
GRPADDR/GRPMASK                HOLDTIME      EXPTIME
RP-ADDR
-----
ff10:0:0:0:0:0:0:0/64           0             0
5040:0:0:0:0:1:84:1
ff30:0:0:0:0:0:0:0/64           0             0
5040:0:0:0:0:1:84:1
ff30:1:0:0:0:0:0:0/32           0             0
5174:0:0:0:0:1:84:1

Total RP Set Entries Displayed:  3/3
=====
```

## show ipv6 pim static-rp

Displays the IPv6 static RP table

## Syntax

- **show ipv6 pim static-rp**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 pim static-rp** command displays the following information:

Output field	Description
GRPADDR	Indicates the IPv6 address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a static RP.
GRPMASK	Indicates the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a static RP.
RPADDR	Indicates the IPv6 address of the static RP. This address can be one of the local IPv6 PIM-SM enabled interfaces or any reachable IPv6 global address as configured using the <b>static-rp</b> CLI commands.
STATUS	Indicates the status of IPv6 static RP.

## Example

The following example displays the IPv6 static RP table.

```
Switch:1>show ipv6 pim static-rp
=====
                          Pim Static RP Table - GlobalRouter
=====
GRPADDR/GRPMASK                STATUS
RPADDR
-----
ff10:0:0:0:0:0:0:0/64
5040:0:0:0:0:1:84:1              valid
ff30:0:0:0:0:0:0:0/64
5040:0:0:0:0:1:84:1              valid
ff30:1:0:0:0:0:0:0/32
5174:0:0:0:0:1:84:1              valid

Total PIM Static RPs Displayed: 3/3
```

## show ipv6 prefix-list

Show IPv6 prefix-list information.

## Syntax

- **show ipv6 prefix-list [vrf WORD<1-16>] [vrfids WORD<0-512>]**
- **show ipv6 prefix-list prefix WORD<1-256>**
- **show ipv6 prefix-list vrf WORD<1-16>**



- **show ipv6 prefix-list vrfids WORD<0-512>**
- **show ipv6 prefix-list WORD<1-64>**

## Command Parameters

**prefix WORD<1-256>**

Specifies the prefix.

**vrf <WORD 1-16>**

Specifies the VRF name.

**vrfids <WORD 0-512>**

Specifies VRF IDs.

**WORD<1-64>**

Specifies the prefix-list name.

## Default

None

## Command Mode

User EXEC

## show ipv6 rip

---

Displays RIPng parameters per interface.

## Syntax

- **show ipv6 rip**

## Default

None

## Command Mode

User EXEC

## show ipv6 rip interface

---

Displays RIPng redistribution configuration.

## Syntax

- **show ipv6 rip interface**

- **show ipv6 rip interface gigabitEthernet {slot/port[sub-port]}**
- **show ipv6 rip interface vlan <1-4059>**

## Command Parameters

### **gigabitEthernet {slot/port[sub-port]}**

Displays interface gigabitEthernet RIPng configurations. {slot/port[sub-port]} identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### **vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show ipv6 rip statistics

---

Displays RIPng statistics.

## Syntax

- **show ipv6 rip statistics**

## Default

None

## Command Mode

User EXEC

## show ipv6 route

---

Display the b-mac address as next hop rather than host name.

## Syntax

- `show ipv6 route [vrf WORD<1-16> | vrfids WORD<0-512>]`
- `show ipv6 route count-summary vrf WORD<1-16>`
- `show ipv6 route count-summary vrfids WORD<0-512>`
- `show ipv6 route dest WORD<0-46>`
- `show ipv6 route dest WORD<0-46> vrf WORD<1-16>`
- `show ipv6 route dest WORD<0-46> vrfids WORD<0-512>`
- `show ipv6 route gigabitethernet {slot/port[sub-port]}`
- `show ipv6 route next-hop WORD<0-46>`
- `show ipv6 route next-hop WORD<0-46> vrf WORD<1-16>`
- `show ipv6 route next-hop WORD<0-46> vrfids WORD<0-512>`
- `show ipv6 route protocol bgp`
- `show ipv6 route protocol bgp vrf WORD<1-16>`
- `show ipv6 route protocol bgp vrfids WORD<0-512>`
- `show ipv6 route protocol isis`
- `show ipv6 route protocol isis vrf WORD<1-16>`
- `show ipv6 route protocol isis vrfids WORD<0-512>`
- `show ipv6 route protocol local`
- `show ipv6 route protocol local vrf WORD<1-16>`
- `show ipv6 route protocol local vrfids WORD<0-512>`
- `show ipv6 route protocol ospf`
- `show ipv6 route protocol ospf vrf WORD<1-16>`
- `show ipv6 route protocol ospf vrfids WORD<0-512>`
- `show ipv6 route protocol rip`
- `show ipv6 route protocol rip vrf WORD<1-16>`
- `show ipv6 route protocol rip vrfids WORD<0-512>`
- `show ipv6 route protocol static`
- `show ipv6 route protocol static vrf WORD<1-16>`
- `show ipv6 route protocol static vrfids WORD<0-512>`
- `show ipv6 route spbm-nh-as-mac`
- `show ipv6 route static`
- `show ipv6 route static vrf WORD<1-16>`
- `show ipv6 route static vrfids WORD<0-512>`
- `show ipv6 route tunnel <1-2000>`
- `show ipv6 route vlan <1-4059>`
- `show ipv6 route vrf WORD<1-16>`
- `show ipv6 route vrfids WORD<0-512>`

## Default

None

## Command Mode

User EXEC

# show ipv6 route alternative

---

Display IPv6 alternative routes.

## Syntax

- `show ipv6 route alternative protocol bgp`
- `show ipv6 route alternative protocol bgp vrf WORD<1-16>`
- `show ipv6 route alternative protocol bgp vrfids WORD<0-512>`
- `show ipv6 route alternative protocol isis`
- `show ipv6 route alternative protocol isis vrf WORD<1-16>`
- `show ipv6 route alternative protocol isis vrfids WORD<0-512>`
- `show ipv6 route alternative protocol local`
- `show ipv6 route alternative protocol local vrf WORD<1-16>`
- `show ipv6 route alternative protocol local vrfids WORD<0-512>`
- `show ipv6 route alternative protocol ospf vrf WORD<1-16>`
- `show ipv6 route alternative protocol ospf vrfids WORD<0-512>`
- `show ipv6 route alternative protocol rip`
- `show ipv6 route alternative protocol rip vrf WORD<1-16>`
- `show ipv6 route alternative protocol rip vrfids WORD<0-512>`
- `show ipv6 route alternative protocol static`
- `show ipv6 route alternative protocol static vrf WORD<1-16>`
- `show ipv6 route alternative protocol static vrfids WORD<0-512>`
- `show ipv6 route alternative spbm-nh-as-mac`
- `show ipv6 route alternative vrf WORD<1-16>`
- `show ipv6 route alternative vrfids WORD<0-512>`

## Command Parameters

`protocol {bgp | isis | local | ospf | rip | static}`

Displays routes for a particular protocol

`spbm-nh-as-mac`

Shows spbm route next hop as mac.

`vrf WORD<1-16>`

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

## show ipv6 route preference

---

Display the IPv6 route preference information to confirm that the configuration is correct.

## Syntax

- **show ipv6 route preference**
- **show ipv6 route preference vrf WORD<1-16>**
- **show ipv6 route preference vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

## show ipv6 source-guard

---

Displays IP Source Guard configuration on all ports or for a specified port, for IPv6 addresses.

## Syntax

- **show ipv6 source-guard interface enabled**

## Default

None

## Command Mode

User EXEC

## show ipv6 source-guard binding

---

Displays the IPv6 addresses that are allowed on all IP Source Guard enabled ports or for a specified port.

## Syntax

- **show ipv6 source-guard binding**
- **show ipv6 source-guard binding interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show ipv6 source-guard binding WORD<0-46>**

## Command Parameters

interface gigabitethernet [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}

Displays the IPv6 addresses that are allowed on the specified IP Source Guard port.

WORD<0-46>

Specifies the IPv6 address bindings for the specified IPv6 address.

## Default

None

## Command Mode

User EXEC

## show ipv6 tcp

---

You can display IPv6 TCP information. Check the health of connections, from the switch perspective, as they traverse the network detect intermittent connectivity detect attacks on resources determine which applications are active by checking the port numbers view statistics about TCP connections

## Syntax

- **show ipv6 tcp**
- **show ipv6 tcp connections**
- **show ipv6 tcp connections vrf WORD<1-16>**

- **show ipv6 tcp connections vrfids WORD<0-512>**
- **show ipv6 tcp listener**
- **show ipv6 tcp listener vrf WORD<1-16>**
- **show ipv6 tcp listener vrfids WORD<0-512>**
- **show ipv6 tcp properties**
- **show ipv6 tcp properties vrf WORD<1-16>**
- **show ipv6 tcp properties vrfids WORD<0-512>**
- **show ipv6 tcp statistics**
- **show ipv6 tcp statistics vrf WORD<1-16>**
- **show ipv6 tcp statistics vrfids WORD<0-512>**

## Command Parameters

### connections

Displays IPv6 TCP connection table information that includes: local port remote port local address remote address state.

### listener

Displays IPv6 TCP listener table information that includes: local port and local address.

### properties

Displays IPv6 TCP global properties information that includes: RtoAlgorithm - the timeout value used for retransmitting unacknowledged octets. RtoMin - the minimum time, in milliseconds, permitted by a TCP implementation for the retransmission timeout. RtoMax - the maximum time (in milliseconds) permitted by a TCP implementation for the transmissions timeout. MaxConn - the maximum connections for the device.

### statistics

Displays IPv6 TCP global statistics information that includes: ActiveOpens, PassiveOpens, AttemptFails, EstabResets, CurrEstab, InSegs, OutSegs, RetransSegs, InErrs, OutRsts, HCInSegs, and HCOOutSegs.

### vrf WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

### vrfids WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

---

## show ipv6 trace

---

Show the status of IPv6 trace commands.

### Syntax

- `show ipv6 trace base`
- `show ipv6 trace base vrf WORD<1-16>`
- `show ipv6 trace base vrfids WORD<0-512>`
- `show ipv6 trace forwarding`
- `show ipv6 trace forwarding vrfids WORD<0-512>`
- `show ipv6 trace forwarding vrf WORD<1-16>`
- `show ipv6 trace nd`
- `show ipv6 trace nd vrf WORD<1-16>`
- `show ipv6 trace nd vrfids WORD<0-512>`
- `show ipv6 trace ospf`
- `show ipv6 trace ospf vrf WORD<1-16>`
- `show ipv6 trace ospf vrfids WORD<0-512>`
- `show ipv6 trace rip`
- `show ipv6 trace rtm`
- `show ipv6 trace rtm vrf WORD<1-16>`
- `show ipv6 trace rtm vrfids WORD<0-512>`
- `show ipv6 trace transport`
- `show ipv6 trace transport vrfids WORD<0-512>`
- `show ipv6 trace transport vrf WORD<1-16>`

### Command Parameters

[base|forwarding|nd|ospf|rip|rtm|transport]

Shows the status for the selected type of trace command.

vrf WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

vrfids WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

### Default

None

### Command Mode

User EXEC



---

## show ipv6 tunnel

---

Shows information about configured IPv6 tunnels, for example, operational state or addresses.

### Syntax

- **show ipv6 tunnel <1-2000>**
- **show ipv6 tunnel detail**
- **show ipv6 tunnel local {A.B.C.D}**
- **show ipv6 tunnel remote {A.B.C.D}**

### Command Parameters

**<1-2000>**

Shows configuration information for a specific tunnel ID.

**detail**

Shows detailed configuration information, for example, the operational status and origin.

**local {A.B.C.D}**

Shows configuration information for a specific local endpoint address.

**remote {A.B.C.D}**

Shows configuration information for a specific remote endpoint address.

### Default

None

### Command Mode

User EXEC

---

## show ipv6 udp

---

Show IPv6 User Datagram Protocol (UDP) information.

### Syntax

- **show ipv6 udp [vrf WORD<1-16> | vrfids WORD<0-512>]**
- **show ipv6 udp endpoints [vrf WORD<1-16> | vrfids WORD<0-512>]**
- **show ipv6 udp endpoints vrf WORD<1-16>**
- **show ipv6 udp endpoints vrfids WORD<0-512>**
- **show ipv6 udp vrf WORD<1-16>**
- **show ipv6 udp vrfids WORD<0-512>**

## Command Parameters

### endpoints

Shows IPv6 UDP information for the endpoints.

### vrf WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

### vrfids WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

## show ipv6 vrrp

---

Shows the global status of Virtual Router Redundancy Protocol (VRRP) for IPv6.

## Syntax

- **show ipv6 vrrp**
- **show ipv6 vrrp vrf WORD<1-16>**
- **show ipv6 vrrp vrfids WORD<0-512>**

## Command Parameters

### vrf WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

### vrfids WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

## show ipv6 vrrp address

---

Display address information for a specific link-local address or virtual router ID.

## Syntax

- **show ipv6 vrrp address**
- **show ipv6 vrrp address link-local WORD<0-127>**
- **show ipv6 vrrp address link-local WORD<0-127> vrfids WORD<0-512>**
- **show ipv6 vrrp address link-local WORD<0-127> vrf WORD<1-16>**
- **show ipv6 vrrp address vrf WORD<1-16>**
- **show ipv6 vrrp address vrfids WORD<0-512>**
- **show ipv6 vrrp address vrid <1-255>**
- **show ipv6 vrrp address vrid <1-255> vrf WORD<1-16>**
- **show ipv6 vrrp address vrid <1-255> vrfids WORD<0-512>**

## Command Parameters

**link-local WORD<0-127>**

Displays information by link-local IPv6 address.

**vrf WORD<1-16>**

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

**vrid <1-255>**

Displays information by virtual router ID.

## Default

None

## Command Mode

User EXEC

## show ipv6 vrrp interface

---

Shows the extended Virtual Router Redundancy Protocol (VRRP) configuration for all interfaces or for a specific interface.

## Syntax

- **show ipv6 vrrp interface [verbose]**
- **show ipv6 vrrp interface gigabitethernet [{slot/port[/sub-port]} [-slot/port[/sub-port]] [, ...]] [verbose]**
- **show ipv6 vrrp interface gigabitethernet vrf WORD<1-16>**
- **show ipv6 vrrp interface gigabitethernet vrfids WORD<0-512>**

- **show ipv6 vrrp interface vlan [<1-4059>] [verbose]**
- **show ipv6 vrrp interface vlan vrf WORD<1-16>**
- **show ipv6 vrrp interface vlan vrfids WORD<0-512>**
- **show ipv6 vrrp interface vrf WORD<1-16>**
- **show ipv6 vrrp interface vrfids WORD<0-512>**
- **show ipv6 vrrp interface vrid <1-255> [verbose]**
- **show ipv6 vrrp interface vrid <1-255> vrf WORD<1-16>**
- **show ipv6 vrrp interface vrid <1-255> vrfids WORD<0-512>**

## Command Parameters

{slot/port[/sub-port][/-slot/port[/sub-port]][,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<1-255>

Displays information by virtual router ID.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

verbose

Displays extended information.

vrf WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

vrfids WORD<0-512>

Specifies a VRF by ID. The VRF parameter is optional.

## Default

None

## Command Mode

User EXEC

## show ipv6 vrrp interface gigabitethernet statistics

Shows the IPv6 gigabitEthernet interface statistics.

## Syntax

- **show ipv6 vrrp interface gigabitethernet statistics** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]] [verbose]

## Command Parameters

**statistics** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Displays the IPv6 statistics for a port. {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**verbose**

Displays extended information.

## Default

None

## Command Mode

User EXEC

## show ipv6 vrrp statistics

---

Views VRRP for IPv6 statistics to manage network performance.

## Syntax

- **show ipv6 vrrp statistics**
- **show ipv6 vrrp statistics link-local** WORD<0-127>
- **show ipv6 vrrp statistics link-local** WORD<0-127> **vrf** WORD<1-16>
- **show ipv6 vrrp statistics link-local** WORD<0-127> **vrfids** WORD<0-512>
- **show ipv6 vrrp statistics vrf** WORD<1-16>
- **show ipv6 vrrp statistics vrfids** WORD<0-512>
- **show ipv6 vrrp statistics vrid** <1-255>
- **show ipv6 vrrp statistics vrid** <1-255> **vrf** WORD<1-16>
- **show ipv6 vrrp statistics vrid** <1-255> **vrfids** WORD<0-512>

## Command Parameters

<1-255>

Displays information by virtual router ID.

vrf WORD<1-16>

Specifies a VRF name. The VRF parameter is optional.

**vrfids WORD<0-512>**

Specifies a VRF by ID. The VRF parameter is optional.

**WORD<0-127>**

Displays information by link-local IPv6 address.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ipv6 vrrp statistics** command displays the following information:

Output field	Description
CHK_SUM_ERR	Shows the number of VRRP packets received with an invalid VRRP checksum value.
VERSION_ERR	Shows the number of VRRP packets received with an unknown or unsupported version number.
VRID_ERR	Shows the number of VRRP packets received with an invalid Vrid for this virtual router.
BECOME_MASTER	Shows the total number of times that the state of this virtual router has transitioned to master. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
ADVERTISE_RCV	Shows the total number of VRRP advertisements received by this virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
ADVERTISE_INT_ERR	Shows the total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
TTL_ERR	Shows the total number of VRRP packets received by the virtual router with IPv4 TTL (for VRRP over IPv4) or IPv6 Hop Limit (for VRRP over IPv6) not equal to 255. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
PRIO_0_RCV	Shows the total number of VRRP packets received by the virtual router with a priority of 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.

Output field	Description
PRI0_0_SENT	Shows the total number of VRRP packets sent by the virtual router with a priority of 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
INVALID_TYPE_ERR	Shows the number of VRRP packets received by the virtual router with an invalid value in the 'type' field. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
ADDRESS_LIST_ERR	Shows the total number of packets received for which the address list does not match the locally configured list for the virtual router. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
UNKNOWN_AUTHTYPE	Shows the total number of packets received with an unknown authentication type.
PACKLEN_ERR	Shows the total number of packets received with a packet length less than the length of the VRRP header. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by the value of DiscontinuityTime.

## show isis

Display the global Intermediate-System-to-Intermediate-System (IS-IS) configuration.

### Syntax

- **show isis**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show isis** command displays the following information:

Output field	Description
AdminState	Indicates the administrative state of the router.
RouterType	Indicates the router Level: I1, I2, or I1/2.
System ID	Indicates the system ID.
Max LSP Gen Interval	Indicates the maximum time between LSP updates in seconds.
Metric	Indicates if the metric is narrow or wide.

Output field	Description
Overload-on-startup	Indicates the IS-IS overload-on-startup value in seconds. The overload-onstartup value is used as a timer to control when to send out Link State Packets (LSPs) with the overload bit cleared after IS-IS startup. The default value is 20 seconds.
Overload	Indicates if there is an overload condition.
Csnp Interval	Indicates the interval between CSNP updates in seconds.
PSNP Interval	Indicates the interval between PSNP updates in seconds.
Rxmt LSP Interval	Indicates the received LSP time interval.
spf-delay	Indicates an SPF delay in milliseconds. The default value is 100 milliseconds.
Router Name	Indicates the IS-IS name of the router.
ip source-address	Indicates the IP source address used for SPBM IP shortcuts.
ipv6 source-address	Indicates the IPv6 source address used for SPBM IP shortcuts.
ip tunnel source-address	Indicates the IP tunnel source address used for SPBM Fabric Extend.
Tunnel vrf	Indicates the name of the vrf that contains the tunnel endpoints.
ONA Port	Indicates the port to which the ONA device is attached.  <b>Note:</b> The ONA port parameter only applies to the VSP 4450 Series.
ip tunnel mtu	Indicates the maximum size of a packet that can be transmitted through the IP tunnel.
Num of Interfaces	Indicates the number of interfaces on the router.
Num of Area Addresses	Indicates the number of area addresses on the router.
Num of Summary Address	Indicates the summary of the addresses on router.
inband-mgmt-ip	Indicates the DvR management IP address for this node, in the DvR domain.  <b>Note:</b> Exception: not supported on VSP 8600 Series or XA1400 Series.
backbone	Indicates whether this node is part of the DvR backbone.
Dynamically Learned Area	For Fabric Area Network (FAN) members, specifies the IS-IS area that is dynamically learned from the neighbor's Hello PDU if the node does not have the IS-IS manual area configured.
FAN Member	Indicates whether the node is a member of the FAN.



Output field	Description
Hello Padding <b>Note:</b> Exception: does not apply to VSP 8600 Series.	Indicates IS-IS hello packets are padded to detect mismatched MTUs on adjacencies.
Multi-area OperState <b>Note:</b> Exception: only supported on VSP 7400 Series.	Indicates the Multi-area SPB operational state as: <ul style="list-style-type: none"> <li>• Disabled—Multi-area SPB is disabled on the switch.</li> <li>• Init—the switch is initializing to function as a boundary node.</li> <li>• Designated—the switch is operating as a designated boundary node.</li> <li>• Non-designated—the switch is operating as a non-designated boundary node.</li> </ul>

## Example

```
Switch:1>show isis
=====
                        ISIS General Info
=====
                        AdminState : enabled
                        RouterType  : Level 1
                        System ID   : 0014.c7e1.33df
Max LSP Gen Interval : 900
                        Metric     : wide
Overload-on-startup  : 20
                        Overload   : false
Csnp Interval       : 10
PSNP Interval       : 2
Rxmt LSP Interval   : 5
                        spf-delay  : 100
Router Name         : Switch1
ip source-address   : 41.41.41.100
ipv6 source-address : 41:0:0:0:0:0:0:100
ip tunnel source-address : 11.11.12.11
                        Tunnel vrf : spboip
ip tunnel mtu       : 1950
Num of Interfaces   : 2
Num of Area Addresses : 1
inband-mgmt-ip     :
                        backbone   : disabled
Dynamically Learned Area : 00.0000.0000
                        FAN Member : No
Hello Padding       : enabled
Multi-Area OperState : disabled
Multi-Area Flags    :
```

## show isis adjacencies

Display Intermediate-System-to-Intermediate-System (IS-IS) adjacencies.

## Syntax

- **show isis adjacencies [home|remote]**

## Command Parameters

### home

Displays the IS-IS adjacencies that the system configures in the home area.

### remote

Displays the IS-IS adjacencies that the system configures in the remote area.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis adjacencies** command displays the following information:

Parameter	Description
INTERFACE	Indicates the interface port, MLT, or logical interface on which IS-IS exists.
L	Indicates the level of the adjacent router.
STATE	Indicates the state of IS-IS on the interface (enabled [UP] or disabled [DOWN]). The state is non-configurable.
UPTIME	Indicates the length of time the adjacency has been up in ddd hh:mm:ss format.
PRI	Indicates the priority of the neighboring Intermediate System for becoming the Designated Intermediate System (DIS).
HOLDTIME	Indicates the calculated hold time for the Hello (hello multiplier x hello interval); if the route is determined to be a designated router, then the product is divided by 3.
SYSID	Indicates the adjacent system ID of the router.
HOST-NAME	Indicates the hostname listed in the LSP. If the host name is not configured, then the system name is displayed.
STATUS	Indicates if the adjacency is active.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1# show isis adjacencies
=====
                        ISIS Adjacencies
=====
INTERFACE L STATE  UPTIME   PRI  HOLDTIME  SYSID          HOST-NAME    STATUS  AREA  AREA-NAME
-----
```

```

Port1/11 1 UP 05:02:18 127 22 beb0.0000.7204 Switch-Lab1 ACTIVE HOME area-9.00.02
Port1/12 1 UP 05:00:18 127 25 beb0.0000.7204 Switch-Lab2 BACKUP HOME area-9.00.02
Port1/16 1 UP 05:00:25 127 24 beb0.0000.7204 Switch-Lab3 BACKUP HOME area-9.00.02
-----
Home: 3 out of 3 interfaces have formed an adjacency
Remote: 0 out of 0 interfaces have formed an adjacency
-----

```

## show isis area

Displays the Intermediate-System-to-Intermediate-System (IS-IS) area information.

### Syntax

- **show isis area**

### Default

The default is none.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Example

Displaying the IS-IS area information on the switch:

```

Switch:1>show isis area
=====
ISIS Area Address
=====
ADDRESS                                ORIGIN  AREA-ROLE  AREA-NAME
-----
10.10.10.11                             config  HOME       v49_1
10.10.10.21                             config  REMOTE     v49_2
-----

```

## show isis area-vnode

Displays the IS-IS SPBM area virtual node information.

## Syntax

- **show isis area-vnode**

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis area-vnode** command displays the following information:

Parameter	Description
REPRESENTED-AREA	Indicates the type of area that the area virtual node represents.
SYSTEM-ID	Indicates the adjacent system ID of the router.
NICK-NAME	Indicates the nickname of the area virtual node.
HOST-NAME	Indicates the hostname listed in the LSP. If the host name is not configured, then the system name is displayed.
AREA	Indicates the type of area as home or remote.

## Example

Displaying the IS-IS SPBM area virtual node information on the switch:

```
Switch:1>show isis area-vnode
=====
                        ISIS SPBM Multi-Area VNode Info
=====
VNODE          VNODE          VNODE          REPRESENTED   REPRESENTED
SYSTEM-ID      NICK-NAME      HOST-NAME      AREA-ADDRESS  AREA         VNODE
USED-IN-AREA
-----
9200.30ff.fff0  9.00.30        area-9.00.30   49.0030      HOME         REMOTE
9200.50ff.fff0  9.00.50        area-9.00.50   49.0050      REMOTE      HOME
```

## show isis dup-detection-temp-disable

Displays the Intermediate-System-to-Intermediate-System (IS-IS) duplicate detection temp disable inf

## Syntax

- **show isis dup-detection-temp-disable remaining-time**

## Command Parameters

### remaining-time

Displays IS-IS duplicate detection temp disable remaining time.

## Default

None

## Command Mode

User EXEC

## **show isis int-auth**

---

Display the Intermediate-System-to-Intermediate-System (IS-IS) interface authentication configuration.

## Syntax

- **show isis int-auth**
- **show isis int-auth [home|remote]**

## Command Parameters

### home

Displays the IS-IS interface authentication information that the system configures in the home area.

### remote

Displays the IS-IS interface authentication information that the system configures in the remote area.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis int-auth** command displays the following information:

Parameter	Description
IFIDX	Shows the interface index for the Ethernet or MLT interface.
AUTH-TYPE	Shows the type of authentication configured for the interface. Types include: <ul style="list-style-type: none"> <li>• none for no authentication.</li> <li>• simple for a simple password.</li> <li>• hmac-md5 for MD5 encryption.</li> <li>• hmac-sha-256 for SHA-256 encryption.</li> </ul>
AUTH-KEYID	Shows the authentication password configured for the interface. If the KeyId is not configured, the value is 0.
AUTH-KEY	Shows the HMAC-MD5 key needed for encryption. This is used only for HMAC-MD5.
ORIGIN	Indicates the origin of the IS-IS circuit configuration on the port, either manually configured through CLI or EDM, or dynamically configured through Auto-sense. <p><b>Note:</b> Exception: not supported on VSP 8600 Series and XA1400 Series.</p>
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1# show isis int-auth home
=====
                        ISIS Interface Auth
=====
IFIDX      AUTH-TYPE  AUTH-KEYID  AUTH-KEY  ORIGIN  AREA  AREA-NAME
-----
Mlt2      none      0           CONFIG   HOME
area-9.00.02
Port1/21  none      0           CONFIG   HOME   area-9.00.02
```

## show isis int-ckt-level

Display the Intermediate-System-to-Intermediate-System (IS-IS) circuit level parameters.

## Syntax

- **show isis int-ckt-level**
- **show isis int-ckt-level [home|remote]**

## Command Parameters

### home

Displays the IS-IS interface circuit level parameters that the system configures in the home area.

### remote

Displays the IS-IS interface circuit level parameters that the system configures in the remote area.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis int-ckt-level** command displays the following information:

Parameter	Description
IFIDX	Shows the interface index for the ethernet or MLT interface.
LEVEL	Shows the level of the IS-IS interface (Level 1 [default] or Level 2).
DIS	Shows the Designated Intermediate System (DIS) of the circuit.
CKT ID	Displays the CKT ID.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1# show isis int-ckt-level home
=====
                    ISIS Circuit level parameters
=====
IFIDX           LEVEL           DIS           CKTID          AREA    AREA-NAME
-----
Mlt2            Level 1                    1           HOME    area-9.00.02
Port1/21       Level 1                    2           HOME    area-9.00.02
```

## show isis int-counters

Display Intermediate-System-to-Intermediate-System (IS-IS) interface counters.

## Syntax

- **show isis int-counters**
- **show isis int-counters [home|remote]**

## Command Parameters

### home

Displays the IS-IS interface counters that the system configures in the home area.

### remote

Displays the IS-IS interface counters that the system configures in the remote area.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis int-counters** command displays the following information:

Parameter	Description
IFIDX	Shows the interface index for the Ethernet or MLT interface.
LEVEL	Shows the level of the IS-IS interface.
AUTH FAILS	Shows the number of times authentication has failed per interface.
ADJ CHANGES	Shows the number of times the adjacencies have changed.
INIT FAILS	Shows the number of times the adjacency has failed to establish.
REJ ADJ	Shows the number of times the adjacency was rejected by another router.
ID LEN	Shows the ID field length mismatches.
MAX AREA	Shows the maximum area address mismatches.
LAN DIS CHANGES	Shows the number of times the DIS has changed.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1# show isis int-counters
```

```
=====
                          ISIS Interface Counters
=====
```



IFIDX	LEVEL	AUTH FAILS	ADJ CHANGES	INIT FAILS	REJ ADJ	ID LEN	MAX AREA	LAN DIS CHANGES	AREA	AREA-NAME
Mlt2	Level 1	0	1	0	0	0	0	0	HOME	area-9.00.02
Port1/21	Level 1	0	1	0	0	0	0	0	HOME	area-9.00.02

## show isis interface

Display Intermediate-System-to-Intermediate-System (IS-IS) interface configuration and status parameters (including adjacencies).

### Syntax

- **show isis interface**
- **show isis interface [l1|l2|l12] [home|remote]**

### Command Parameters

#### home

Displays the IS-IS interface information that the system configures in the home area.

#### [ l1 | l2 | l12 ]

Displays the interface information for the specified level: l1 (Level 1), l2 (Level 2), l12 (Level 1 and 2). The switch is a Level 1 router, which means it has only Level 1 links and can route within only one area. Level 1 routers route only within their assigned area and cannot route outside that area. Level 2 routers route between areas and toward other domains. Level 1/Level 2 routers route within an assigned area and between areas. Level 1/Level 2 routers maintain both a Level 1 Link State Database and a Level 2 Link State Database.

#### remote

Displays the IS-IS interface information that the system configures in the remote area.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show isis interface** command displays the following information:

Parameter	Description
IFIDX	Indicates the interface index for the Ethernet or MLT interface.
TYPE	Indicates the type of interface configured (only pt-pt is supported).

Parameter	Description
LEVEL	Indicates the level of the IS-IS interface (Level 1 [default] or Level 2).
OP-STATE	Shows the physical connection state of the interface.
ADM-STATE	Shows the configured state of the interface.
ADJ	Shows how many adjacencies are learned through the interface.
UP-ADJ	Shows how many adjacencies are active through the interface.
SPBM-L1-METRIC	Indicates the IS-IS interface Level 1 metric.
ORIGIN	Indicates the origin of the IS-IS circuit configuration on the port, either manually configured through CLI or EDM, or dynamically configured through Auto-sense.  <b>Note:</b> Exception: not supported on VSP 8600 Series and XA1400 Series.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1# show isis interface
```

```

=====
                        ISIS Interfaces
=====
IFIDX   TYPE   LEVEL  OP-STATE  ADM-STATE  ADJ  UP-ADJ  SPBM-L1  OP-SPBM-  ORIGIN  AREA  AREA-NAME
        -METRIC  -METRIC
-----
Mlt2    pt-pt  Level 1  UP        UP          1    1       10       10       CONFIG  HOME  area-9.00.02
Port1/21 pt-pt  Level 1  UP        UP          1    1       10       10       CONFIG  HOME  area-9.00.02
=====

```

## show isis int-l1-cntl-pkts

Display Intermediate-System-to-Intermediate-System (IS-IS) Level 1 control packet counters.

### Syntax

- **show isis int-l1-cntl-pkts**
- **show isis int-l1-cntl-pkts [home|remote]**

### Command Parameters

#### home

Displays the IS-IS L1 control packet counters that the system configures in the home area.

#### remote

Displays the IS-IS L1 control packet counters that the system configures in the remote area.

### Default

None

## Command Mode

User EXEC

## Command Output

The **show isis int-l1-cntl-pkts** command displays the following information:

Parameter	Description
IFIDX	Shows the interface index for the Ethernet or MLT interface.
DIRECTION	Shows the packet flow (Transmitted or Received).
HELLO	Shows the amount of interface-level Hello packets.
LSP	Shows the amount of LSP packets.
CSNP	Shows the amount of CSNPs.
PSNP	Shows the amount of PSNPs.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1# show isis int-l1-cntl-pkts
=====
                    ISIS L1 Control Packet counters
=====
IFIDX      DIRECTION      HELLO      LSP      CSNP      PSNP      AREA      AREA-NAME
-----
Mlt2      Transmitted    13346      231      2         229      HOME      area-9.00.02
Mlt2      Received       13329      230      1         230      HOME      area-9.00.02
Port1/21  Transmitted    13340      227      2         226      HOME      area-9.00.02
Port1/21  Received       13335      226      1         227      HOME      area-9.00.02
```

## show isis int-l2-cntl-pkts

Display Intermediate-System-to-Intermediate-System (IS-IS) Level 2 control packet counters.

## Syntax

- **show isis int-l2-cntl-pkts**

## Default

None

## Command Mode

User EXEC

## show isis int-timers

Display Intermediate-System-to-Intermediate-System (IS-IS) interface timers.

### Syntax

- **show isis int-timers**
- **show isis int-timers [home|remote]**

### Command Parameters

#### home

Displays the IS-IS interface timer information that the system configures in the home area.

#### remote

Displays the IS-IS interface timer information that the system configures in the remote area.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show isis int-timers** command displays the following information:

Parameter	Description
IFIDX	Indicates the interface index for the Ethernet or MLT interface.
LEVEL	Indicates the IS-IS interface level.
HELLO INTERVAL	Indicates the interval at which a Hello packet is sent to the IS-IS network.
HELLO MULTIPLIER	Indicates the multiplier that is used in conjunction with the Hello Interval.
HELLO DR	Indicates the interval at which a Hello packet is sent to the IS-IS network if the router is a designated router (DIS).
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

### Example

```
Switch:1# show isis int-timers home
```

```
=====
                        ISIS Interface Timers
=====
```

IFIDX	LEVEL	HELLO INTERVAL	HELLO MULTIPLIER	HELLO DR	AREA	AREA-NAME
Mlt2	Level 1	9	3	3	HOME	area-9.00.02
Port1/21	Level 1	9	3	3	HOME	area-9.00.02

## show isis logical-interface

Display IS-IS logical interfaces.

### Syntax

- **show isis logical-interface [mtu] [name] [shaper]**

### Command Parameters

#### mtu

Displays IS-IS logical interface IDs, names, and the Maximum Transmission Unit (MTU) values.

#### name

Displays IS-IS logical interface name.

#### shaper

Displays IS-IS logical interface IDs, names, and egress shaping rate values in Mbps.



#### Note

Displays only interfaces with egress shaping rate values configured.

### Default

The default is non.

### Command Mode

User EXEC

### Usage Guidelines

The *mtu* parameter only applies to XA1400 Series.

## Command Output

The **show isis logical-interface** command displays the following information:

Output field	Description
BFD STATUS	Specifies the status of BFD on this logical interface. The status can be enabled or disabled.
IFIDX	Specifies an index value for this logical interface.
NAME	Specifies the administratively assigned name of this logical interface, which can be up to 16 characters.
ENCAP TYPE	Specifies whether the encapsulation type for the logical interface is Layer 2 (L2-P2P-VID) or Layer 3 (IP).
L2_INFO PORT/MLT	Specifies the port or MLT that the logical interface is connected to in an Layer 2 network.
L2_INFO VLAN	Specifies the list of VLANs that are associated with this Layer 2 logical interface.
TUNNEL DEST-IP	Specifies the destination IP address for the logical interface.
L3_TUNNEL_NEXT_HOP_INFO PORT/MLT	Specifies the outgoing interface (port or MLT) for VXLAN traffic.
L3_TUNNEL_NEXT_HOP_INFO VLAN	Specifies the outgoing VLAN interface for VXLAN traffic.
L3_TUNNEL_NEXT_HOP_INFO VRF	Specifies the name of the VRF that this Layer 3 logical interface is configured on.

## show isis lsdb

Display the Intermediate-System-to-Intermediate-System (IS-IS) Link State Database (LSDB).

### Syntax

- **show isis lsdb**
- **show isis lsdb [level {l1|l2|l1l2}] [sysid <xxxx.xxx.xxx>] [lspid <xxxx.xxx.xx-xx>] [tlv <1-236> ] [detail] [home|remote]**
- **show isis lsdb local**
- **show isis lsdb tlv <1-236> sub-tlv <1-3>**
- **show isis lsdb ip-unicast**
- **show isis lsdb ip-unicast [i-sid <0-16777215>] [lspid xxx.xxx.xx-xx] [sysid xxx.xxx] [home|remote]**
- **show isis lsdb ipv6-unicast**
- **show isis lsdb ipv6-unicast [i-sid <0-16777215>] [lspid xxx.xxx.xx-xx] [sysid xxx.xxx] [home|remote]**

### Command Parameters

detail

Displays detailed information, which includes the Link State Packet (LSP) ID, the level of the external router, the maximum age of the LSP, the LSP sequence number and the LSP checksum.

**home**

Displays the IS-IS link state database information that the system configures in the home area.

**ip-unicast**

Displays the link state database for the ip-unicast.

**ipv6-unicast**

Displays the link state database for the IPv6 unicast.

**i-sid <0-16777215>**

Specifies the i-sid value to filter by.

**level { I1 | I2 | I12 }**

Displays the link state database for the specified level: I1 (Level 1), I2 (Level 2), or I12 (Level 1 and 2). The switch is a Level 1 router, which means it has only Level 1 links and can route within only one area. Level 1 routers route only within their assigned area and cannot route outside that area. Level 2 routers route between areas and toward other domains. Level 1/Level 2 routers route within an assigned area and between areas. Level 1/Level 2 routers maintain both a Level 1 link state database and a Level 2 Link State database.

**local**

Displays information on the local link state database.

**lspid xxxx.xxxx.xxxx.xx-xx - 8 bytes**

Displays the link state database for the specified Link State Packet (LSP) ID. The LSP ID is assigned to external IS-IS routing devices.

**remote**

Displays the IS-IS link state database information that the system configures in the remote area.

**sub-tlv <1-3>**

Displays the link state database for a specified sub-Type-Length-Value (TLV). Shortest Path Bridging MAC (SPBM) employs Intermediate-System-to-Intermediate-System (IS-IS) as the interior gateway protocol and implements additional TLVs to support additional functionality. TLVs exist inside IS-IS packets and Sub-TLVs exist as additional information in TLVs.

**sysid xxxx.xxxx.xxxx - 6 bytes**

Displays the link state database for the specified system ID.

**sysid xxxx.xxxx.xxxx - 6 bytes**

Displays the link state database for a specified sub-Type-Length-Value (TLV). Shortest Path Bridging MAC (SPBM) employs Intermediate-System-to-Intermediate-System (IS-IS) as the interior gateway protocol and implements additional TLVs to support additional functionality. TLVs exist inside IS-IS packets and Sub-TLVs exist as additional information in TLVs.

**tlv <1-236>**

Displays the link state database for a specified Type-Length-Value (TLV). Shortest Path Bridging MAC (SPBM) employs Intermediate-System-to-Intermediate-System (IS-IS) as the interior gateway protocol and implements additional TLVs to support additional functionality. TLVs exist inside IS-IS packets and give additional information.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis lsdb** command displays the following information:

Parameter	Description
LSP ID	Indicates the LSP ID assigned to external IS-IS routing devices.
LEVEL	Indicates the level of the external router: l1, l2, or l12.
LIFETIME	Indicates the maximum age of the LSP. If the max-lsp-gen-interval is set to 900 (default) then the lifetime value begins to count down from 1200 seconds and updates after 300 seconds if connectivity remains. If the timer counts down to zero, the counter adds on an additional 60 seconds, then the LSP for that router is lost. This happens because of the zero age lifetime, which is detailed in the RFC standards.
SEQNUM	Indicates the LSP sequence number. This number changes each time the LSP is updated.
CHKSUM	Indicates the LSP checksum. This is an error checking mechanism used to verify the validity of the IP packet.
HOST-NAME	Indicates the hostname listed in the LSP. If the host name is not configured, then the system name is displayed.
AREA	Indicates the type of area as home or remote.

## Example

```
Switch:1# show isis lsdb
=====
                        ISIS LSDB
=====
LSP ID                LEVEL  LIFETIME  SEQNUM  CHKSUM  HOST-NAME  AREA
-----
0014.c7e1.33df.00-00  1      545      0xb1   0xed28  NewYork    HOME
0016.ca23.73df.00-00  1      1119     0x9f   0x9c9d  Switch-Lab2 HOME
0018.b0bb.b3df.00-00  1      708      0xb9   0xcb1a  Switch-Lab1 HOME
=====

Level-1 HOME AREA: 3 out of 3 Total Num of LSP Entries
Level-1 REMOTE AREA: 0 out of 3 Total Num of LSP Entries
Level-2 HOME AREA: 0 out of 0 Total Num of LSP Entries
Level-2 REMOTE AREA: 0 out of 3 Total Num of LSP Entries
```

## show isis manual-area

Display Intermediate-System-to-Intermediate-System (IS-IS) areas.



## Syntax

- **show isis manual-area**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis manual-area** command displays the following information:

Output field	Description
AREA ADDRESS	Shows the manual areas defined. There can only be one area. Use the same manual area across the entire SPBM cloud. The manual area can be from 1-13 bytes in length.

## show isis multi-area dvr redistribute

Displays the IS-IS Multi-area SPB Distributed Virtual Routing (DVR) redistribution configuration on the switch.

## Syntax

- **show isis multi-area dvr redistribute**

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area dvr redistribute** command displays the following information:

Parameter	Description
ADMIN STATE	Indicates the administrative state of Multi-area SPB DvR redistribution.

## Example

Displaying the IS-IS Multi-area SPB DvR redistribution configuration on the switch.

```
Switch:1>show isis multi-area dvr redistribute
=====
                        MULTI-AREA DVR REDISTRIBUTE
=====
Admin State
-----
Enabled
-----
```

## show isis multi-area ip redistribute home-to-remote

Displays the IS-IS Multi-area SPB IPv4 home to remote redistribution configuration on the switch.

## Syntax

- **show isis multi-area ip redistribute home-to-remote**
- **show isis multi-area ip redistribute home-to-remote vrf WORD<1-16>**
- **show isis multi-area ip redistribute home-to-remote vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies the Virtual Router Forwarding (VRF) name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs as text from range 0 to 512 characters in length.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area ip redistribute home-to-remote** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB IPv4 home to remote redistribution.

## Example

Displaying the IS-IS Multi-area SPB IPv4 home to remote redistribution on the switch:

```
Switch:1>show isis multi-area ip redistribute home-to-remote
=====
                ISIS Multiarea Redistribute List for ip unicast - GlobalRouter
=====
DIRECTION          ENABLE          RPOLICY
-----
home-to-remote     TRUE
=====
                ISIS Multiarea Redistribute List for routed multicast - GlobalRouter
=====
DIRECTION          ENABLE          RPOLICY
-----
home-to-remote     TRUE
```

## show isis multi-area ip redistribute remote-to-home

Displays the IS-IS Multi-area SPB IPv4 remote to home redistribution configuration on the switch.

## Syntax

- **show isis multi-area ip redistribute remote-to-home**
- **show isis multi-area ip redistribute remote-to-home vrf WORD<1-16>**
- **show isis multi-area ip redistribute remote-to-home vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies the Virtual Router Forwarding (VRF) name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs as text from range 0 to 512 characters in length.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area ip redistribute remote-to-home** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB IPv4 remote to home redistribution.

## Example

Displaying the IS-IS Multi-area SPB IPv4 remote to home redistribution on the switch:

```
Switch:1>show isis multi-area ip redistribute remote-to-home
=====
                ISIS Multiarea Redistribute List for ip unicast - GlobalRouter
=====
DIRECTION          ENABLE          RPOLICY
-----
remote-to-home     TRUE
=====

                ISIS Multiarea Redistribute List for routed multicast - GlobalRouter
=====
DIRECTION          ENABLE          RPOLICY
-----
remote-to-home     TRUE
```

## show isis multi-area ip redistribute routed-multicast

Displays the IS-IS Multi-area SPB IPv4 routed multicast redistribution configuration on the switch.

## Syntax

- `show isis multi-area ip redistribute routed-multicast`
- `show isis multi-area ip redistribute routed-multicast home-to-remote`
- `show isis multi-area ip redistribute routed-multicast home-to-remote vrf WORD<1-16>`
- `show isis multi-area ip redistribute routed-multicast home-to-remote vrfids WORD<0-512>`
- `show isis multi-area ip redistribute routed-multicast remote-to-home`
- `show isis multi-area ip redistribute routed-multicast remote-to-home vrf WORD<1-16>`
- `show isis multi-area ip redistribute routed-multicast remote-to-home vrfids WORD<0-512>`
- `show isis multi-area ip redistribute routed-multicast vrf WORD<1-16>`
- `show isis multi-area ip redistribute routed-multicast vrfids WORD<0-512>`

## Command Parameters

### home-to-remote

Specifies the home to remote redistribution.

### remote-to-home

Specifies the remote to home redistribution.

### vrf WORD<1-16>

Specifies the Virtual Router Forwarding (VRF) name.

### vrfids WORD<0-512>

Specifies a range of VRF IDs as text from range 0 to 512 characters in length.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area ip redistribute routed-multicast** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB routed multicast redistribution.

## Example

Displaying the IS-IS Multi-area SPB IPv4 routed multicast redistribution configuration on the switch:

```
Switch:1>show isis multi-area ip redistribute routed-multicast
=====
          ISIS Multiarea Redistribute List for routed multicast - GlobalRouter
=====
DIRECTION          ENABLE          RPOLICY
-----
home-to-remote     TRUE
remote-to-home     TRUE
```

## show isis multi-area ip redistribute unicast

Displays the IS-IS Multi-area SPB IPv4 unicast redistribution configuration on the switch.

## Syntax

- **show isis multi-area ip redistribute unicast**
- **show isis multi-area ip redistribute unicast home-to-remote**
- **show isis multi-area ip redistribute unicast home-to-remote vrf WORD<1-16>**
- **show isis multi-area ip redistribute unicast home-to-remote vrfids WORD<0-512>**
- **show isis multi-area ip redistribute unicast remote-to-home**
- **show isis multi-area ip redistribute unicast remote-to-home vrf WORD<1-16>**
- **show isis multi-area ip redistribute unicast remote-to-home vrfids WORD<0-512>**
- **show isis multi-area ip redistribute unicast vrf WORD<1-16>**
- **show isis multi-area ip redistribute unicast vrfids WORD<0-512>**

## Command Parameters

home-to-remote

Specifies the home to remote redistribution.

#### remote-to-home

Specifies the remote to home redistribution.

#### vrf WORD<1-16>

Specifies the Virtual Router Forwarding (VRF) name.

#### vrfids WORD<0-512>

Specifies a range of VRF IDs as text from range 0 to 512 characters in length.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area ip redistribute unicast** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB IPv4 unicast redistribution.

## Example

Displaying the IS-IS Multi-area SPB IPv4 unicast redistribution on the switch:

```
Switch:1>show isis multi-area ip redistribute unicast

=====
                ISIS Multiarea Redistribute List for ip unicast - GlobalRouter
=====
DIRECTION          ENABLE    RPOLICY
-----
home-to-remote     TRUE
remote-to-home     TRUE
```

## show isis multi-area ip redistribute vrf

Displays the IS-IS Multi-area SPB IPv4 redistribution configuration for a specific Virtual Router Forwarding (VRF) instance.

### Syntax

- **show isis multi-area ip redistribute vrf WORD<1-16>**

### Command Parameters

**WORD<1-16>**

Specifies the VRF name.

### Default

The default is none.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show isis multi-area ip redistribute vrf WORD<1-16>** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB IPv4 unicast and routed multicast redistribution for a specific VRF.

### Example

Displaying the IS-IS Multi-area SPB IPv4 redistribution configuration for the VRF instance:

```
Switch:1>show isis multi-area ip redistribute vrf VRF1
=====
                ISIS Multiarea Redistribute List for ip unicast - VRF VRF1
=====
DIRECTION          ENABLE          RPOLICY
-----
```



```

home-to-remote      FALSE
=====
                ISIS Multiarea Redistribute List for routed multicast - VRF VRF1
=====
DIRECTION           ENABLE      RPOLICY
-----
home-to-remote      TRUE       Test

```

## show isis multi-area ip redistribute vrfids

Displays the IS-IS Multi-area SPB IPv4 redistribution configuration for a specific Virtual Router Forwarding (VRF) ID.

### Syntax

- **show isis multi-area ip redistribute vrfids WORD<0-512>**

### Command Parameters

**WORD<0-512>**

Specifies the VRF ID.

### Default

The default is none.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show isis multi-area ip redistribute vrfids WORD<0-512>** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB IPv4 unicast and routed multicast redistribution for a specific VRF ID.

## Example

Displaying the IS-IS Multi-area SPB IPv4 redistribution configuration for the VRF ID:

```
Switch:1>show isis multi-area ip redistribute vrfids 512
=====
                ISIS Multiarea Redistribute List for ip unicast - VRF MgmtRouter
=====
DIRECTION          ENABLE      RPOLICY
-----
home-to-remote     TRUE       Test
=====
                ISIS Multiarea Redistribute List for routed multicast - VRF MgmtRouter
=====
DIRECTION          ENABLE      RPOLICY
-----
home-to-remote     TRUE       Test
```

## show isis multi-area ipv6 redistribute home-to-remote

Displays the IS-IS Multi-area SPB IPv6 home to remote redistribution configuration on the switch.

### Syntax

- **show isis multi-area ipv6 redistribute home-to-remote**
- **show isis multi-area ipv6 redistribute home-to-remote vrf WORD<1-16>**
- **show isis multi-area ipv6 redistribute home-to-remote vrfids WORD<0-512>**

### Command Parameters

**vrf WORD<1-16>**

Specifies the Virtual Router Forwarding (VRF) name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs as text from range 0 to 512 characters in length.

### Default

The default is none.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area ipv6 redistribute home-to-remote** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPBIPv6 redistribution.

## Example

Displaying the IS-IS Multi-area SPB IPv6 home to remote redistribution on the switch:

```
Switch:1>show isis multi-area ipv6 redistribute home-to-remote
=====
          ISIS Multiarea Redistribute List for ipv6 unicast - GlobalRouter
=====
DIRECTION          ENABLE          RPOLICY
-----
home-to-remote     TRUE
```

## show isis multi-area ipv6 redistribute remote-to-home

Displays the IS-IS Multi-area SPB IPv6 remote to home redistribution configuration on the switch.

## Syntax

- **show isis multi-area ipv6 redistribute remote-to-home**
- **show isis multi-area ipv6 redistribute remote-to-home vrf WORD<1-16>**
- **show isis multi-area ipv6 redistribute remote-to-home vrfids WORD<0-512>**

## Command Parameters

**vrf WORD<1-16>**

Specifies the Virtual Router Forwarding (VRF) name.

**vrfids WORD<0-512>**

Specifies a range of VRF IDs as text from range 0 to 512 characters in length.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area ipv6 redistribute remote-to-home** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB IPv6 redistribution.

## Example

Displaying the IS-IS Multi-area SPB IPv6 remote to home redistribution on the switch:

```
Switch:1>show isis multi-area ipv6 redistribute remote-to-home
=====
                ISIS Multiarea Redistribute List for ipv6 unicast - GlobalRouter
=====
DIRECTION          ENABLE          RPOLICY
-----
remote-to-home    TRUE
```

## show isis multi-area ipv6 redistribute unicast

Displays the IS-IS Multi-area SPB IPv6 unicast redistribution configuration on the switch.

## Syntax

- **show isis multi-area ipv6 redistribute unicast**
- **show isis multi-area ipv6 redistribute unicast home-to-remote**
- **show isis multi-area ipv6 redistribute unicast home-to-remote vrf WORD<1-16>**
- **show isis multi-area ipv6 redistribute unicast home-to-remote vrfids WORD<0-512>**
- **show isis multi-area ipv6 redistribute unicast remote-to-home**
- **show isis multi-area ipv6 redistribute unicast remote-to-home vrf WORD<1-16>**
- **show isis multi-area ipv6 redistribute unicast remote-to-home vrfids WORD<0-512>**
- **show isis multi-area ipv6 redistribute unicast vrf WORD<1-16>**
- **show isis multi-area ipv6 redistribute unicast vrfids WORD<0-512>**

## Command Parameters

### home-to-remote

Specifies the home to remote redistribution.

### remote-to-home

Specifies the remote to home redistribution.

### vrf WORD<1-16>

Specifies the Virtual Router Forwarding (VRF) name.

### vrfids WORD<0-512>

Specifies a range of VRF IDs as text from range 0 to 512 characters in length.

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area ipv6 redistribute unicast** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPBIPv6 unicast redistribution.

## Example

Displaying the IS-IS Multi-area SPB IPv6 unicast redistribution on the switch:

```
Switch:1>show isis multi-area ipv6 redistribute unicast
=====
          ISIS Multiarea Redistribute List for ipv6 unicast - GlobalRouter
=====
DIRECTION          ENABLE          RPOLICY
-----
home-to-remote     TRUE           Test1
remote-to-home     TRUE           Test2
```

## show isis multi-area ipv6 redistribute vrf

Displays the IS-IS Multi-area SPB IPv6 redistribution configuration for a specific Virtual Router Forwarding (VRF) instance.

### Syntax

- **show isis multi-area ipv6 redistribute vrf WORD<1-16>**

### Command Parameters

**WORD<1-16>**

Specifies the VRF name.

### Default

The default is none.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show isis multi-area ipv6 redistribute vrf WORD<1-16>** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB IPv6 redistribution for a specific VRF.

### Example

Displaying the IS-IS Multi-area SPB IPv6 redistribution configuration for the VRF instance:

```
Switch:1>show isis multi-area ipv6 redistribute vrf VRF1
=====
                ISIS Multiarea Redistribute List for ipv6 unicast - VRF VRF1
=====
DIRECTION          ENABLE          RPOLICY
```

```
-----
remote-to-home      TRUE      Test
```

## show isis multi-area ipv6 redistribute vrfids

Displays the IS-IS Multi-area SPB IPv6 redistribution configuration for a specific Virtual Router Forwarding (VRF) ID.

### Syntax

- **show isis multi-area ipv6 redistribute vrfids WORD<0-512>**

### Command Parameters

**WORD<0-512>**

Specifies the VRF ID.

### Default

The default is none.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show isis multi-area ipv6 redistribute vrfids WORD<0-512>** command displays the following information:

Parameter	Description
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB IPv6 redistribution for a specific VRF ID.

Displaying the IS-IS Multi-area SPB IPv6 redistribution configuration for the VRF ID:

```
Switch:1>show isis multi-area ipv6 redistribute vrfids 512
-----
          ISIS Multiarea Redistribute List for ipv6 unicast - VRF MgmtRouter
-----
DIRECTION      ENABLE      RPOLICY
```

```
-----
home-to-remote      TRUE      Test
```

## show isis multi-area l2 isid-list

Displays the IS-IS Multi-area SPB layer 2 I-SID list information.

### Syntax

- **show isis multi-area l2 isid-list**

### Default

The default is none.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show isis multi-area l2 isid-list** command displays the following information:

Parameter	Description
List Name	Indicates the name of the I-SID list.
I-SID / I-SID RANGE	Indicates the range of I-SID values in the I-SID list.

Displaying IS-IS Multi-area SPB layer 2 I-SID redistribution:

```
Switch:1>show isis multi-area l2 isid-list
=====
                        MULTI AREA L2 ISID LIST
=====
List Name                I-SID / I-SID RANGE
-----
test                    50510 - 501512
All 1 out of 1 Total Num of Isid Lists displayed
```

## show isis multi-area l2 redistribute i-sid

Displays the IS-IS Multi-area SPB layer 2 I-SID redistribution configuration on the switch.



## Syntax

- **show isis multi-area l2 redistribute i-sid**

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area l2 redistribute i-sid** command displays the following information:

Parameter	Description
Permit	Indicates the action mode for the specific range of I-SID values.
Except List Name	Indicates the name of the I-SID list.

Displaying the IS-IS Multi-area SPB layer 2 I-SID redistribution:

```
Switch:1>show isis multi-area l2 redistribute i-sid
=====
                        MULTI AREA L2 ISID REDIST POLICY
=====
Permit                Except List Name
-----
permit-all           testlist
```

## show isis multi-area l2 redistribute snoop-multicast

Displays the IS-IS Multi-area SPB layer 2 multicast snooping redistribution configuration on the switch.

## Syntax

- **show isis multi-area l2 redistribute snoop-multicast**

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show isis multi-area l2 redistribute snoop-multicast** command displays the following information:

Parameter	Description
ISID	Indicates the I-SID value.
ISID LIST	Indicates the name of the I-SID list.
DIRECTION	Indicates the direction of the redistribution policy.
ENABLE	Indicates if the redistribution policy is enabled on the switch.
RPOLICY	Indicates the route policy for IS-IS Multi-area SPB layer 2 multicast snooping redistribution for a specific I-SID or I-SID list.

Displaying the IS-IS Multi-area SPB layer 2 multicast snooping configuration:

```
Switch:1>show isis multi-area l2 redistribute snoop-multicast
=====
MULTI-AREA L2 SNOOP MULTICAST REDISTRIBUTE BY ISID
=====
ISID      DIRECTION      ENABLE      RPOLICY
-----
1100     home-to-remote  TRUE       test
=====
MULTI-AREA L2 SNOOP MULTICAST REDISTRIBUTE BY ISID LIST
=====
ISID LIST  DIRECTION      ENABLE      RPOLICY
-----
List1     home-to-remote  TRUE       test
=====
```

## show isis net

Display Intermediate-System-to-Intermediate-System (IS-IS) net information.

## Syntax

- **show isis net**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis net** command displays the following information:

Output field	Description
NET	Shows the NET address. Output from this command is from the global IS-IS configuration of the manual area and the configuration of the system ID. There is only one manual areas defined and only one system ID. The manual area is from 1-13 bytes in length. The system ID is 6 bytes in length.

## show isis remote

Displays IS-IS remote configuration on the switch.

## Syntax

- **show isis remote**

## Default

The default is none.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

Displaying IS-IS remote area configuration:

```
Switch:1>show isis remote
=====
                        ISIS Remote Area Info
=====
                        AdminState : enabled
                        System ID  : 209e.f77e.2086
                        Num of Interfaces : 4
                        Num of Area Addresses : 1
                        Dynamically Learned Area : 49.0002
                        Multi-Area OperState : designated
```

## show isis spbm

Display isis spbm related info.

### Syntax

- **show isis spbm**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show isis spbm** command displays the following information:

Output field	Description
SPBM INSTANCE	Indicates the SPBM instance identifier. You can only create one SPBM instance.
B-VID	Indicates the SPBM B-VLAN associated with the SPBM instance.
PRIMARY VLAN	Indicates the primary SPBM B-VLAN.
NICK NAME	Indicates the SPBM node nickname. The nickname is used to calculate the I-SID multicast MAC address.
LSDB TRAP	Indicates the status of the IS-IS SPBM LSDB update trap on this SPBM instance. The default is disable.
IP	Indicates the status of SPBM IP shortcuts on this SPBM instance. The default is disable.
IPv6	Indicates the status of SPBM IPv6 shortcuts on this SPBM instance. The default is disable.
MULTICAST	Indicates if SPBM multicast is enabled. The default is disabled.
SPB-PIM-GW	Indicates if SPB PIM Gateway is enabled. The default is disabled.
STP-MULTI HOMING	Indicates if MSTP-Fabric Connect Multi Homing is enabled. The default is disabled.
SMLT-SPLIT-BEB	Specifies whether the switch is the primary or secondary vIST peer.
SMLT-VIRTUAL-BMAC	Specifies a virtual MAC address that can be used by both peers.
SMLT-PEER-SYSTEM-ID	Specifies the vIST peer system ID.

---

## show isis spbm ip-multicast-fib

---

Display the Intermediate-System-to-Intermediate-System (IS-IS) Shortest Path Bridging MAC (SPBM) IP multicast Forwarding Information Database (FIB) entries. If you do not use an optional parameter, the command output shows entries for the GlobalRouter (GRT).

### Syntax

- **show isis spbm ip-multicast-fib**

### Default

None

### Command Mode

User EXEC

---

## show isis spbm ip-multicast-route

---

Displays IP multicast over Fabric Connect route information.

### Syntax

- **show isis spbm ip-multicast-route**
- **show isis spbm ip-multicast-route all**
- **show isis spbm ip-multicast-route detail**

### Command Parameters

#### all

Displays all route information.

#### detail

Displays detailed route information. Shows only for L3 context when vlan/vsn-isis options are not used.

#### group {A.B.C.D}

Displays the group IP address. Shows only for L3 context when vlan/vsn-isis options are not used.

#### vlan <2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998.

#### vrf WORD<1-16>

Displays the ip-multicast-route by vrf.

**vsn-isid**

Displays the ip-multicast-route by vsn-isid.

**Default**

None

**Command Mode**

User EXEC

**Command Output**

The **show isis spbm ip-multicast-route** command displays the following information:

Output field	Description
Type	Specifies the type of interface. The options include: <ul style="list-style-type: none"> <li>routed— For IP Shortcuts and Layer 3 VSNS.</li> <li>snoop— For Layer 2 VSNS.</li> </ul>
VrfName	Specifies the VRF name of the interface.
Vlan Id	Specifies the VLAN ID of the interface.
Source	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
VSN-ISID	Specifies the VSN I-SID for Layer 2 VSNS and Layer 3 VSNS. Specifies the GRT for IP Shortcuts with IP Multicast over Fabric Connect because IP Shortcuts IP Multicast over Fabric Connect does not use a VSN I-SID.
Data ISID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives IP multicast data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
Source-BEB	Specifies the source BEB for the IP Multicast over Fabric Connect route.

**show isis spbm ip-multicast-route group**

Displays IP multicast route information by multicast group address.

**Syntax**

- show isis spbm ip-multicast-route group {A.B.C.D}**
- show isis spbm ip-multicast-route group {A.B.C.D} detail**
- show isis spbm ip-multicast-route group {A.B.C.D} source {A.B.C.D}**

- `show isis spbm ip-multicast-route group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255>`
- `show isis spbm ip-multicast-route group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255> detail`

## Command Parameters

`{A.B.C.D}`

Displays route information by multicast group address.

`detail`

Displays detailed route information.

`source {A.B.C.D}`

Displays information for the source IP address.

`source-beb WORD<0-255>`

Displays information for a specific backbone edge bridge.

## Default

None

## Command Mode

User EXEC

## show isis spbm ip-multicast-route vlan

---

Displays IP multicast route information by VLAN.

## Syntax

- `show isis spbm ip-multicast-route vlan <2-4059>`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D}`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vlan <2-4059> detail`
- `show isis spbm ip-multicast-route vlan <2-4059> detail`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D}`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} source {A.B.C.D}`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} source {A.B.C.D}`

- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255>`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255>`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255> detail`
- `show isis spbm ip-multicast-route vlan <2-4059> group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255> detail`
- `show isis spbm ip-multicast-route vlan<2-4059>`
- `show isis spbm ip-multicast-route vlan<2-4059> group {A.B.C.D} source {A.B.C.D} detail`

## Command Parameters

### <2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998.

### detail

Displays detailed route information.

### group {A.B.C.D}

Specifies the multicast group address.

### source {A.B.C.D}

Displays information for the source IP address.

### source-beb WORD<0-255>

Displays information for a specific backbone edge bridge.

## Default

None

## Command Mode

User EXEC

## show isis spbm ip-multicast-route vrf

Displays IP multicast route information by VRF.



## Syntax

- `show isis spbm ip-multicast-route vrf WORD<1-16>`
- `show isis spbm ip-multicast-route vrf WORD<1-16> detail`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D}`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} source {A.B.C.D}`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255>`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255> detail`

## Command Parameters

### detail

Displays detailed route information.

### group {A.B.C.D}

Displays route information by multicast group address.

### source {A.B.C.D}

Displays information for the source IP address.

### source-beb WORD<0-255>

Displays information for a specific backbone edge bridge.

### WORD<1-16>

Specifies the VRF name.

## Default

None

## Command Mode

User EXEC

## show isis spbm ip-multicast-route vsn-isis

---

Displays IP multicast route information by VSN I-SID.

## Syntax

- `show isis spbm ip-multicast-route vsn-isis <1-16777215>`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> detail`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D}`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} source {A.B.C.D}`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255>`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255> detail`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215>`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> detail`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D}`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} source {A.B.C.D}`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255>`
- `show isis spbm ip-multicast-route vsn-isis <1-16777215> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255> detail`

## Command Parameters

`<1-16777215>`

Specifies the VSN I-SID.

`detail`

Displays detailed route information.

`detail`

Displays detailed route information.

`group {A.B.C.D}`

Displays route information by multicast group address.

`source {A.B.C.D}`

Displays information for the source IP address.

**source-beb WORD<0-255>**

Displays information for a specific backbone edge bridge.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis spbm ip-multicast-route vsn-isid** command displays the following information:

Output field	Description
Source	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Data ISID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives the IP Multicast over Fabric Connect data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
NNI Rcvrs	Specifies the NNI receivers.
UNI Rcvrs	Specifies the UNI receivers.
Source-BEB	Specifies the source BEB for the IP Multicast over Fabric Connect route.

## show isis spbm ip-unicast-fib

Display isis spbm ip unicast-fib.

## Syntax

- **show isis spbm ip-unicast-fib**
- **show isis spbm ip-unicast-fib [all] [id <1-16777215] [spbm-nh-as-mac] [home|remote]**

## Command Parameters

**all**

Displays the IP unicast Forwarding Information Base (FIB) entries for all VRFs.

**home**

Displays the IS-IS SPBM IP unicast FIB information that the system configures in the home area.

**id** <1-16777215>

Displays the IP unicast Forwarding Information Base (FIB) for the given service instance identifier (I-SID) value.

**remote**

Displays the IS-IS SPBM IP unicast FIB information that the system configures in the remote area.

**spbm-nh-as-mac**

Displays the next hop Backbone MAC entry in the IP unicast Forwarding Information Base (FIB).

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis spbm ip-unicast-fib** command displays the following information:

Parameter	Description
VRF	Specifies the VRF ID of the IP unicast FIB entry, 0 indicates NRE.
VRF ISID	Specifies the I-SID of the IP unicast FIB entry.
DEST ISID	Specifies the destination I-SID of the IP unicast FIB entry.
Destination	Specifies the destination IP address of the IP unicast FIB entry.
NH BEB	Specifies the next hop B-MAC of the IP unicast FIB entry.
VLAN	Specifies the VLAN of the IP unicast FIB entry.
OUTGOING INTERFACE	Specifies the outgoing port of the IP unicast FIB.
SPBM COST	Specifies the B-MAC cost of the IP unicast FIB entry.
PREFIX COST	Specifies the prefix cost of the IP unicast FIB entry.
PREFIX TYPE	Specifies the prefix type of the IP unicast FIB entry.
IP ROUTE PREFERENCE	Specifies the IP route preference of the IP unicast FIB entry.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch# show isis spbm ip-unicast-fib
```

```

=====
                        SPBM IP-UNICAST FIB ENTRY INFO
=====
VRF  DEST                                OUTGOING  SPBM    PREFIX  PREFIX  IP ROUTE

```

```

VRF  ISID ISID Destination      NH BEB  VLAN INTERFACE COST  COST  TYPE      PREFERENCE AREA  AREA-NAME
-----
GRT  -    -  10.133.136.0/24  4K3(*) 4058 1/3      10    1    Internal  7        HOME  area-9.00.02
GRT  -    -  10.133.136.0/24  4K3(*) 4059 1/3      10    1    Internal  7        HOME  area-9.00.02
GRT  -    -  10.133.136.0/24  4K4(*) 4058 to_4k4 10000 1    Internal  7        HOME  area-9.00.02
GRT  -    -  10.133.136.0/24  4K4(*) 4059 to_4k4 10000 1    Internal  7        HOME  area-9.00.02
-----
Home : Total number of SPBM IP-UNICAST FIB entries 4
Remote: Total number of SPBM IP-UNICAST FIB entries 0
-----

```

## show isis spbm ipv6-unicast-fib

Display the IPv6 Unicast FIB entries for GRT. If you use `spbm-nh-as-mad`, the command output shows the b-mac address as the nexthop identifier rather than the remote host name.

### Syntax

- **show isis spbm ipv6-unicast-fib**
- **show isis spbm ipv6-unicast-fib** [**all**] [**id <1-16777215>**] [**spbm-nh-as-mac**] [**home|remote**]

### Command Parameters

#### all

Displays the IPv6 unicast Forwarding Information Base (FIB) entries for all VRFs.

#### home

Displays the IS-IS SPBM IPv6 unicast FIB information that the system configures in the home area.

#### id <1-16777215>

Displays the IPv6 unicast Forwarding Information Base (FIB) for the given service instance identifier (I-SID) value.

#### remote

Displays the IS-IS SPBM IPv6 unicast FIB information that the system configures in the remote area.

#### spbm-nh-as-mac

Displays the next hop Backbone MAC entry in the IPv6 unicast Forwarding Information Base (FIB).

### Default

None

### Command Mode

User EXEC

## Command Output

The **show isis spbm ipv6-unicast-fib** command displays the following information:

Parameter	Description
VRF	Specifies the VRF ID of the IPv6 unicast FIB entry, 0 indicates NRE.
VRF ISID	Specifies the I-SID of the IPv6 unicast FIB entry.
DEST ISID	Specifies the destination I-SID of the IPv6 unicast FIB entry.
Destination	Specifies the destination IPv6 address of the IPv6 unicast FIB entry.
NH BEB	Specifies the next hop B-MAC of the IPv6 unicast FIB entry.
VLAN	Specifies the VLAN of the IPv6 unicast FIB entry.
OUTGOING INTERFACE	Specifies the outgoing port of the IPv6 unicast FIB.
SPBM COST	Specifies the B-MAC cost of the IPv6 unicast FIB entry.
PREFIX COST	Specifies the prefix cost of the IPv6 unicast FIB entry.
METRIC TYPE	Specifies the metric type. Specifies an internal or an external metric. For internal metric type, the cost of the external routes is equal to the sum of all internal costs and the external cost. For external metric type, the cost of the external routes is equal to the external cost alone. The default is internal.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1>show isis spbm ipv6-unicast-fib
=====
SPBM IPv6-UNICAST FIB ENTRY INFO
=====
VRF      Dest      OUTGOING  SPBM  PREFIX  METRIC  IP ROUTE
VRF      ISID      ISID      Destination  NH BEB  VLAN  INTERFACE  COST  COST  TYPE  PREFERENCE  AREA  AREA-NAME
-----
GRT      -         -         00:16:ca:23:73:df  e12    10   10/22     10   1   Internal  7           HOME  area-9.00.02
GRT      -         11        00:16:ca:23:73:df  esp    20   10/22     10   1   Internal  7           HOME  area-9.00.02
vrf1    11        100       00:18:b0:bb:b3:df  e12    10   10/22     10   1   External  7           HOME  area-9.00.02
vrf1    11        11        00:14:c7:e1:33:e0  ess    20   10/22     10   1   External  7           HOME  area-9.00.02
=====
Home: Total number of SPBM IPv6-UNICAST FIB entries 4
Remote: Total number of SPBM IPv6-UNICAST FIB entries 0
=====
```

## show isis spbm i-sid

Display the Intermediate-System-to-Intermediate-System (IS-IS) Shortest Path Bridging MAC (SPBM) multicast Forwarding Information Base (FIB) calculation results by service instance identifier (I-SID).

## Syntax

- **show isis spbm i-sid { all | config | discover }**
- **show isis spbm i-sid { all | config | discover } id <1-16777215>**

- **show isis spbm i-sid { all | config | discover } nick-name x.xx.xx - 2.5 bytes**
- **show isis spbm i-sid { all | config | discover } vlan <2-4059>**

## Command Parameters

**id <1-16777215>**

Displays service instance identifier (I-SID) information for the specified I-SID.

**nick-name x.xx.xx - 2.5 bytes**

Displays service instance identifier (I-SID) information for the specified nickname.

**vlan <2-4059>**

Displays service instance identifier (I-SID) information for the specified Shortest Path Bridging MAC (SPBM) VLAN. Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis spbm i-sid** command displays the following information:

Output field	Description
ISID	Indicates the IS-IS SPBM I-SID identifier. <ul style="list-style-type: none"> <li>• all: display all SPBM I-SID</li> <li>• discover: display discovered SPBM I-SID</li> <li>• config: display configured SPBM I-SID</li> </ul>
SOURCE NAME	Indicates the nickname of the node where this I-SID was configured or discovered. <p><b>Note:</b> SOURCE NAME is equivalent to nickname.</p>
VLAN	Indicates the B-VLAN where this I-SID was configured or discovered.
SYSID	Indicates the system identifier.
TYPE	Indicates the SPBM I-SID type as either configured or discovered.
HOST_NAME	Indicates the host name of the multicast FIB entry.

Output field	Description
ISID NAME	Indicates the global I-SID name to I-SID mapping.
AREA	Indicates the type of area as home or remote.
AREA NAME	Indicates the name of the area.

## Example

The following example displays the command output.

```
Switch# show isis spbm i-sid all
=====
                                SPBM ISID INFO
=====
ISID      SOURCE NAME  VLAN  SYSID      TYPE      HOST_NAME    ISID NAME    AREA    AREA NAME
-----
101001    1.11.16     4051  0200.10ff.fff0  discover  area-0.00.10  ISID-101001  HOME    area-0.00.20
101003    1.11.16     4051  0200.10ff.fff0  discover  area-0.00.10  ISID-101003  HOME    area-0.00.20
101005    1.11.16     4051  0200.10ff.fff0  discover  area-0.00.10  ISID-101005  HOME    area-0.00.20
101007    1.11.16     4051  0200.10ff.fff0  discover  area-0.00.10  ISID-101007  HOME    area-0.00.20
101009    1.11.16     4051  0200.10ff.fff0  discover  area-0.00.10  ISID-101009  HOME    area-0.00.20
101011    1.11.16     4051  0200.10ff.fff0  discover  area-0.00.10  ISID-101011  HOME    area-0.00.20
-----
Total number of SPBM ISID entries configed: 0
-----
Total number of SPBM ISID entries discovered: 6
-----
Total number of SPBM ISID entries: 6
-----
```

## show isis spbm multicast

Displays the status of the global SPBM multicast configuration.

### Syntax

- **show isis spbm multicast**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show isis spbm multicast** command displays the following information:

Output field	Description
multicast	Specifies if multicast is enabled.
fwd-cache-timeout (seconds)	Specifies the forward cache timeout value in seconds.



## show isis spbm multicast-fib

Display the Intermediate-System-to-Intermediate-System (IS-IS) Shortest Path Bridging MAC (SPBM) multicast Forwarding Information Database (FIB) entries.

### Syntax

- **show isis spbm multicast-fib**
- **show isis spbm multicast-fib i-sid <1-16777215>**
- **show isis spbm multicast-fib nick-name x.xx.xx - 2.5 bytes**
- **show isis spbm multicast-fib summary**
- **show isis spbm multicast-fib vlan <2-4059>**

### Command Parameters

**i-sid <1-16777215>**

Displays the FIB for the specified I-SID.

**summary**

Displays a summary of the FIB.

**vlan <2-4059>**

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show isis spbm multicast-fib** command displays the following information:

Output field	Description
MCAST DA	Indicates the multicast destination MAC address of the multicast FIB entry.
ISID	Indicates the I-SID of the multicast FIB entry.
BVLAN	Indicates the B-VLAN of the multicast FIB entry.
SYSID	Indicates the system identifier of the multicast FIB entry.
HOST-NAME	Indicates the host name of the multicast FIB entry.

Output field	Description
OUTGOING INTERFACE	Indicates the outgoing port of the multicast FIB entry.
INCOMING INTERFACE	Indicates the outgoing port of the multicast FIB entry.

## show isis spbm nick-name

Display the Intermediate-System-to-Intermediate-System (IS-IS) Shortest Path Bridging MAC (SPBM) nickname entries.

### Syntax

- **show isis spbm nick-name**
- **show isis spbm nick-name count**
- **show isis spbm nick-name nick-name**
- **show isis spbm nick-name smlt-virtual-bmac  
0x00:0x00:0x00:0x00:0x00:0x00**
- **show isis spbm nick-name sysid**
- **show isis spbm nick-name [home|remote]**

### Command Parameters

#### count

Specifies the total number of SPBM nickname entries.

#### home

Specifies the ISIS SPBM nickname information that the system configures in the home area.

#### nick-name

Specifies the ISIS SPBM nickname information.

#### remote

Specifies the ISIS SPBM nickname information that the system configures in the remote area.

#### smlt-virtual-bmac 0x00:0x00:0x00:0x00:0x00:0x00

Specifies the virtual MAC address. SMLT virtual BMAC is the optional configuration. If SMLT virtual BMAC is not configured, the system derives SMLT virtual BMAC from the configured SMLT peer system ID and the nodal MAC of the device (IS-IS system ID). The system compares the nodal MAC of the device with the SMLT peer system ID configured and takes the small one, plus 0x01, as the SMTL virtual BMAC. The system also derives SMLT split BEB from the SMLT peer system ID and nodal MAC of the device. Displays the SMLT(Split MultiLink Trunking) virtual entry for the specified Backbone MAC (BMAC).

#### sysid xxxx.xxxx.xxxx

Specifies isis system ID in xxxx.xxxx.xxxx - 6 bytes format.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis spbm nick-name** command displays the following information:

Parameter	Description
LSP ID	Indicates the 8 byte LSP ID, consisting of the SystemID, Circuit ID, and Fragment Number.
LIFETIME	Indicates the remaining lifetime in seconds for the LSP.
NICK-NAME	Indicates the nickname for the SPBM node.
VIRTUAL-BMAC	Indicates the virtual MAC address.
HOST-NAME	Indicates the hostname listed in the LSP, or the system name if the host name is not configured.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1# show isis spbm nick-name
```

```
=====
ISIS SPBM NICK-NAME
=====
LSP ID                LIFETIME  NICK-NAME  VIRTUAL-BMAC  HOST-NAME  AREA  AREA NAME
-----
0011.0011.0011.00-00  743       4.22.33   00:00:00:00:00:00  BEB_A     HOME  area-9.00.02
0011.0013.0013.00-00  361       1.13.13   00:13:13:00:15:15  BEB_B     HOME  area-9.00.02
0011.0015.0015.00-00  395       1.16.17   00:13:13:00:15:15  BEB_C     HOME  area-9.00.02
0039.0039.0039.00-00  1088      0.01.39   00:00:00:00:00:00  BEB_D     HOME  area-9.00.02
0084.0084.0084.00-00  1080      0.84.77   00:00:00:00:00:00  BEB_E     HOME  area-9.00.02
8404.840c.8404.00-00  300       8.84.44   00:00:00:00:00:00  BEB_F     HOME  area-9.00.02
9200.01ff.fff0.00-00  1080      9.00.01   00:00:00:00:00:00  BEB_G     HOME  area-9.00.02
0001.0004.0005.00-00  1114      0.01.45   00:55:11:55:22:55  BEB_H     REMOTE area-9.00.01
209e.f77e.2086.00-00  1080      0.84.78   00:00:00:00:00:00  BEB_I     REMOTE area-9.00.01
5005.5005.5005.00-00  388       0.01.55   00:55:11:55:22:55  BEB_J     REMOTE area-9.00.01
840c.8404.8404.00-00  631       8.84.04   00:00:00:00:00:00  BEB_K     REMOTE area-9.00.01
9200.02ff.fff0.00-00  1080      9.00.02   00:00:00:00:00:00  BEB_L     REMOTE area-9.00.01
f46e.959f.8c86.00-00  1088      0.01.40   00:00:00:00:00:00  BEB_M     REMOTE area-9.00.01
=====
Home:    7 out of 7 Total Num of Entries
Remote:  6 out of 6 Total Num of Entries
=====
```

## show isis spbm unicast-fib

Display isis spbm unicast-fib.

## Syntax

- **show isis spbm unicast-fib**
- **show isis spbm unicast-fib [b-mac <0x00:0x00:0x00:0x00:0x00:0x00>] [vlan <2-4059>] [summary] [home|remote]**

## Command Parameters

**b-mac <0x00:0x00:0x00:0x00:0x00:0x00>**

Displays the Forwarding Information Base (FIB) entry for the specified Backbone MAC (BMAC).

**home**

Displays the IS-IS SPBM unicast FIB information that the system configures in the home area.

**remote**

Displays the IS-IS SPBM unicast FIB information that the system configures in the remote area.

**summary**

Displays a summary of the Forwarding Information Base (FIB).

**vlan <2-4059>**

Specifies the VLAN ID for which to display the FIB. Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis spbm unicast-fib** command displays the following information:

Parameter	Description
DESTINATION ADDRESS	Indicates the destination MAC Address of the unicast FIB entry.
B-VLAN	Indicates the B-VLAN of the unicast FIB entry.
SYSID	Indicates the destination system identifier of the unicast FIB entry.
HOST-NAME	Indicates the destination host name of the unicast FIB entry.
OUTGOING INTERFACE	Indicates the outgoing interface of the unicast FIB entry.
COST	Indicates the cost of the unicast FIB entry.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch# show isis spbm unicast-fib
=====
                        SPBM UNICAST FIB ENTRY INFO
=====
DESTINATION          BVLAN SYSID          HOST-NAME    OUTGOING      COST  AREA   AREA-NAME
ADDRESS
-----
00:16:ca:23:73:df   1000  0016.ca23.73df  SPBM-1       1/21         10   HOME   area-9.00.02
00:16:ca:23:73:df   2000  0016.ca23.73df  SPBM-1       1/21         10   HOME   area-9.00.02
00:18:b0:bb:b3:df   1000  0018.b0bb.b3df  SPBM-2       MLT-2        10   HOME   area-9.00.02
00:14:c7:e1:33:e0   1000  0018.b0bb.b3df  SPBM-2       MLT-2        10   HOME   area-9.00.02
00:18:b0:bb:b3:df   2000  0018.b0bb.b3df  SPBM-2       MLT-2        10   HOME   area-9.00.02
=====
Home:   Total number of SPBM UNICAST FIB entries 5
Remote: Total number of SPBM UNICAST FIB entries 0
=====
```

## show isis spbm unicast-tree

Display the Shortest Path Bridging MAC (SPBM) unicast tree.

### Syntax

- **show isis spbm unicast-tree <2-4059>**
- **show isis spbm unicast-tree <2-4059> destination xxxx.xxxx.xxxx - 6 bytes**
- **show isis spbm unicast-tree <2-4059> home**
- **show isis spbm unicast-tree <2-4059> remote**

### Command Parameters

**<2-4059>**

Displays the unicast tree for the specified destination. Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998.

**destination xxxx.xxxx.xxxx - 6 bytes**

Displays the unicast tree for the specified destination.

**home**

Displays the unicast tree for the home area.

**remote**

Displays the unicast tree for the remote area.

### Default

None

## Command Mode

User EXEC

## show isis spb-mcast summary

Displays IP multicast over Fabric Connect summary information.

## Syntax

- **show isis spb-mcast-summary**
- **show isis spb-mcast-summary count**
- **show isis spb-mcast-summary host-name WORD<0-255>**
- **show isis spb-mcast-summary lspid <xxxx.xxx.xx-xx>**

## Command Parameters

**count**

Specifies the total number of SPB Multicast entries.

**host-name WORD<0-255>**

Displays the IP Multicast over Fabric Connect summary for a given host-name.

**lspid xxxx.xxx.xx-xx**

Displays the IP Multicast over Fabric Connect summary for a given LSP ID.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show isis spb-mcast-summary** command displays the following information:

Output field	Description
SCOPE I-SID	Indicates the I-SID that specifies the multicast streams when the scope is either the Layer 3 VSN or the Layer 2 VSN or any combination.
SOURCE ADDRESS	Indicates the IP multicast source address that maps to the I-SID.
GROUP ADDRESS	Indicates the IP multicast group address that maps to the I-SID.

Output field	Description
DATA I-SID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives the IP Multicast over Fabric Connect data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVID	Indicates the ID of the SPBM backbone VLAN (B-VLAN) on which the multicast stream forwards in the SPBM cloud.
LSP FRAG	Indicates the fragment number of the LSP ID.
HOST-NAME	Specifies the host name listed in the LSP, or the system name if the host is not configured.

## show isis statistics

Display Intermediate-System-to-Intermediate-System (IS-IS) statistics.

### Syntax

- **show isis statistics**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show isis statistics** command displays the following information:

Parameter	Description
LEVEL	Shows the level of the IS-IS interface.
CORR LSPs	Shows the number of corrupted LSPs detected.
AUTH FAILS	Shows the number of times authentication has failed on the global level.
AREA DROP	Shows the number of manual addresses dropped from the area.
MAX SEQ EXCEEDED	Shows the number of attempts to exceed the maximum sequence number.
SEQ NUM SKIPS	Shows the number of times the sequence number was skipped.
OWN LSP PURGE	Shows how many times the local LSP was purged.
BAD ID LEN	Shows the number of ID field length mismatches.
PART CHANGES	Shows the number of partition link changes.

Parameter	Description
LSP DB OLOAD	Show the number of times the switch was in the overload state.
AREA	Indicates the type of area as home or remote.
AREA-NAME	Indicates the name of the area.

## Example

```
Switch:1# show isis statistics
=====
                        ISIS System Stats
=====
LEVEL   CORR   AUTH   AREA   MAX SEQ   SEQ NUM   OWN LSP   BAD ID   PART   LSP DB   AREA   AREA-NAME
  LSPs   FAILS   DROP   EXCEEDED SKIPS     PURGE    LEN     CHANGES OLOAD
-----
Level-1 0      0      0      0         1         0        0        0        0        HOME   area-9.00.02
Level-1 0      0      0      0         1         0        0        0        0        REMOTE area-9.00.02
```

## show isis system-id

Display Intermediate-System-to-Intermediate-System (IS-IS) system ID.

### Syntax

- **show isis system-id**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show isis system-id** command displays the following information:

Output field	Description
SYSTEM-ID	Shows the system ID. Output from this show command is from the global IS-IS configuration of the system ID. There is one system ID configured. The system ID is 6 bytes in length.

## show khi cpp

View key health information about the control processors.

### Syntax

- **show khi cpp port-statistics**



- **show khi cpp port-statistics** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### port-statistics

Displays port statistics.

## Default

None

## Command Mode

User EXEC

## show khi fe-ona detail

---

View ONA global information such as port numbers, IP addresses, and MTU.

## Syntax

- **show khi fe-ona detail**

## Default

None

## Command Mode

User EXEC

## show khi fe-ona status

---

View the current status of the ONA and release information.

## Syntax

- **show khi fe-ona status**

## Default

None

## Command Mode

User EXEC

## show khi mgmt statistics

---

View the management statistics of the switch by checking their key health indicators.

## Syntax

- **show khi mgmt statistics**
- **show khi mgmt statistics clip**
- **show khi mgmt statistics oob**
- **show khi mgmt statistics vlan**

## Command Parameters

### clip

Shows key health indicator management statistics for the loopback interface.

### oob

Shows key health indicator management statistics for the Out-of-Band interface.

### vlan

Shows key health indicator management statistics for the VLAN interface.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to VSP 8600 Series. The *oob* parameter does not apply to VSP 4450 Series and XA1400 Series.

## show khi performance

---

View the performance of the various components of the switch by checking their key health indicators.

## Syntax

- **show khi performance**
- **show khi performance buffer-pool**
- **show khi performance buffer-pool {slot[-slot][,...]}**
- **show khi performance cpu**
- **show khi performance cpu {slot[-slot][,...]}**
- **show khi performance memory**
- **show khi performance memory {slot[-slot][,...]}**
- **show khi performance process**
- **show khi performance process {slot[-slot][,...]}**
- **show khi performance pthread**
- **show khi performance pthread {slot[-slot][,...]}**
- **show khi performance rx-queue**
- **show khi performance slabinfo**
- **show khi performance slabinfo {slot[-slot][,...]}**

## Command Parameters

**buffer-pool {slot[-slot][,...]}**

Shows buffer performance and utilization statistics. {slot [-slot] [...]} specifies the slot number.

**cpu {slot [-slot] [...]}**

Shows current utilization, 5-minute average utilization, and 5-minute high water mark with date and time of event. {slot [-slot] [...]} specifies the slot number.

**memory {slot[-slot][,...]}**

Shows memory performance and utilization statistics. {slot [-slot] [...]} specifies the slot number.

**process {slot [-slot] [...]}**

Shows process performance and utilization statistics. {slot [-slot] [...]} specifies the slot number.

**pthread {slot[-slot][,...]}**

Shows thread performance and utilization statistics. {slot [-slot] [...]} specifies the slot number.

**rx-queue**

Shows the queue performance and utilization statistics.

**slabinfo {slot[-slot][,...]}**

Shows internal memory management resource performance and utilization statistics. {slot[-slot] [...]} specifies the slot number.

## Default

None

## Command Mode

User EXEC

## show lacp

View Link Aggregation Control Protocol (LACP) configuration information to determine the LACP parameters and to ensure your configuration is correct.

## Syntax

- `show lacp`
- `show lacp`
- `show lacp actor-admin interface`
- `show lacp actor-admin interface gigabitethernet`
- `show lacp actor-admin interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}`
- `show lacp actor-admin interface gigabitethernet vid <1-4059>`
- `show lacp actor-oper interface`
- `show lacp actor-oper interface gigabitethernet`
- `show lacp actor-oper interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}`
- `show lacp actor-oper interface gigabitethernet vid <1-4059>`
- `show lacp extension interface`
- `show lacp extension interface gigabitethernet`
- `show lacp extension interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}`
- `show lacp extension interface gigabitethernet vid <1-4059>`
- `show lacp partner-admin interface`
- `show lacp partner-admin interface gigabitethernet`
- `show lacp partner-admin interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}`
- `show lacp partner-admin interface gigabitethernet vid <1-4059>`
- `show lacp partner-oper interface`
- `show lacp partner-oper interface gigabitethernet`
- `show lacp partner-oper interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}`
- `show lacp partner-oper interface gigabitethernet vid <1-4059>`

## Command Parameters

actor-admin

Shows LACP actor administrative information for all interfaces.

**actor-oper**

Shows all LACP actor operational information for all interfaces.

**extension**

Show all LACP timer information.

**interface**

Shows all LACP port configuration information for all interfaces.

**interface mlt <64-6399>**

Shows the MLT LACP information for all MLTs or the specific MLT index.

**interface mlt id <1-512>**

Specifies the MLT ID.

**partner-admin**

Shows all LACP partner administrative information.

**partner-oper**

Shows all LACP partner operational information.

**vid <1-4059>**

Specifies the VLAN ID in the range of 2 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show lacp interface

---

View Link Aggregation Control Protocol (LACP) statistics for each port to monitor LACP performance of the port.

## Syntax

- **show lacp interface**
- **show lacp interface gigabitethernet**
- **show lacp interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show lacp interface gigabitethernet vid <1-4059>**
- **show lacp interface mlt**

- **show lacp interface mlt <64-6399>**
- **show lacp interface mlt id <1-512>**

## Command Parameters

**gigabitethernet {slot/port[/sub-port][/-slot/port[/sub-port]][,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**mlt <64-6399>**

Shows the MLT LACP information for all MLTs or the specific MLT index.

**mlt id <1-512>**

Specifies the MLT ID.

**vid <1-4059>**

Shows only ports attached to a particular VLAN ID. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show license

---

Display the existing software licenses on the platform.

## Syntax

- **show license**

## Default

None

## Command Mode

User EXEC

---

## show link-state group

---

Displays the status of the link-state group.

### Syntax

- **show link-state group <1-48>**
- **show link-state group <1-48> detail**

### Command Parameters

<1-48>

Specifies the link-state group ID.

**detail**

Displays detailed information about the LST group.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

DEMO FEATURE - Link-state tracking (LST) is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see [VOSS Feature Support Matrix](#).

---

## show logging

---

Use this command to display logging information.

### Syntax

- **show logging config**
- **show logging info**
- **show logging level**
- **show logging transferFile <1-10>**

### Command Parameters

config

Displays the global logging information.

**info**

Displays the logging information.

**level**

Displays the configuration of event logging.

**transferFile <1-10>**

Displays the current level parameter settings and next level directories. <1-10> specifies the TFTP/FTP host IP address.

## Default

None

## Command Mode

User EXEC

## show logging file

---

View log files by file name, category, severity, or CP to identify possible problems.

## Syntax

- **show logging file**
- **show logging file alarm**
- **show logging file CPU WORD<0-100>**
- **show logging file detail**
- **show logging file event-code WORD<0-10>**
- **show logging file module WORD<0-100>**
- **show logging file name-of-file WORD<1-99>**
- **show logging file save-to-file WORD<1-99>**
- **show logging file severity WORD<0-25>**
- **show logging file tail**
- **show logging file vrf WORD<0-32>**

## Command Parameters

**alarm**

Displays alarm log entries.

**CPU WORD<0-100>**

Filters and list the logs according to the CPU that generated it. Specify a string length of 0-25 characters. To specify multiple filters, separate each CPU by the vertical bar (|), for example,



CPU1|CPU2. Different hardware platforms support a different number of CPUs. For more information, see your hardware documentation.

**detail**

Displays CLI and SNMP logging information.

**event-code WORD<0-10>**

Specifies a number that precisely identifies the event reported. WORD<0-10> specifies the event code in the format: {0x0-0x00FFFFFF| 0x0-0x00FFFFFF}.

**module WORD<0-100>**

Filters and list the logs according to module. Specify a string length of 0-100 characters. Categories include SNMP, EAP, RADIUS, RMON, WEB, STG, IGMP, HW, MLT, FILTER, QOS, CLILOG, SW, CPU, IP, VLAN, IPMC, IP-RIP, OSPF, PIM, POLICY, RIP, and SNMPLOG. To specify multiple filters, separate each category by the vertical bar (|), for example, OSPF|FILTER|QOS. Use the command show logging file module clilog to view the CLI log. Use the command show logging file module snmplog to view the SNMP log.

**name-of-file WORD <1-99>**

Displays the valid logs from this file. For example, /intflash/logcopy.txt. You cannot use this command on the current log file-the file into which the messages are currently logged). Specify a string length of 1-99 characters.

**save-to-file WORD<1-99>**

Redirects the output to the specified file and removes all encrypted information. The tail option is not supported with the save-to-file option.

**severity WORD <0-25>**

Filters and list the logs according to severity. Choices include INFO, ERROR, WARNING, FATAL. To specify multiple filters, separate each severity by the vertical bar (|), for example, ERROR|WARNING|FATAL.

**tail**

Shows the last results first.

**vrf WORD<0-32>**

Specifies the name of a VRF instance to show log messages that only pertain to that VRF.

## Default

None

## Command Mode

User EXEC

## show mac-address-table aging-time

---

Display forwarding database aging time for all VLANs globally.

## Syntax

- **show mac-address-table aging-time**

## Default

None

## Command Mode

User EXEC

## show macsec

Display information about Media Access Control Security (MACsec).

## Syntax

- **show macsec**

## Command Mode

User EXEC

## Command Output

The command displays the following information:

Output field	Description
Connectivity Association Name	Specifies the name of the connectivity association (CA).
Connectivity Association Key Hash	Specifies the CA hash key.
AN_Mode / TxKeyParity	Specifies the CA mode and transmission key parity value.
Port Members	Specifies the ports that are members of a CA.
PortId	Specifies the port ID.
MACSEC Status	Specifies whether MACsec is enabled on a port.
Encryption Status	Specifies whether encryption is enabled on a port.
Replay Protect	Specifies whether replay protection is enabled.
Replay Protect W'dow	Specifies the maximum acceptable difference in packet ID numbers between out of order packets. If a packet ID number differs from the ID number of the previously received packet by more than the specified window size, the packet is dropped.
Encryption Offset	Specifies the number of bytes after the Ethernet header from which data encryption begins. Possible values are 30 (IPv4 plus TCP/UDP header) and 50 (IPv6 plus TCP/UDP header). The default is no offset.

Output field	Description
Cypher Suite	Specifies the cipher suite for encrypting traffic with MACsec. The following cipher suites are supported: <ul style="list-style-type: none"> <li>AES-GCM-128 standard, with a maximum key length of 128 bits</li> <li>AES-GCM-256 standard, with a maximum key length of 256 bits</li> </ul> The default is the AES-GCM-128 standard.
CA Name	Specifies the name of the connectivity association.
MKA-Profile Name	Specifies the MKA profile name. An MKA profile name consists only of alphanumeric characters (0-9, A-Z, and a-z). The profile name is case sensitive.

## Example

The **show macsec** command displays the following information:

```
Switch:1>show macsec

=====
MACSEC Connectivity Associations Info
=====
Connectivity      Connectivity      AN_Mode /      Port
Association Name   Association Key Hash  TxKeyParity    Members
-----
conn1              550e0fb1dec7eaa40a473b09790c8745    4AN / Even

All 1 out of 1 Total Num of Macsec connectivity associates displayed

=====
MACSEC Port Status
=====
Profile           MACSEC      Encryption  Replay      Replay      Encryption      Cipher      CA      MKA-
PortId           Status      Status      Protect      Protect W'dow  Offset          Suite      Name      Name
-----
1/1              disabled   disabled   disabled    --           none           AES-128    Nil     --
1/2              disabled   disabled   disabled    --           none           AES-128    Nil     --
1/3              disabled   disabled   disabled    --           none           AES-128    Nil     --
1/4              disabled   disabled   disabled    --           none           AES-128    Nil     --
1/5              disabled   disabled   disabled    --           none           AES-128    Nil     --
```

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show macsec connectivity-association

Display the connectivity-association (CA) details. For security reasons, the CA key is not displayed.

## Syntax

- show macsec connectivity-association**

- **show macsec connectivity-association <ca-name>**
- **show macsec connectivity-association WORD<5-15>**

## Command Parameters

**<ca-name>**

Specifies a connectivity-association name. An 80 byte alphanumeric string.

**WORD<5-15>**

Specifies a connectivity-association name. It is a 5 to 15 character alphanumeric string.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## show macsec mka participant

---

Display information about participants in an MKA session.

## Syntax

- **show macsec mka participant**
- **show macsec mka participant {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} [verbose]**

## Default

None.

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show macsec mka participant** command displays the following information:

Output field	Description
PortId	Specifies the port number of the MKA session participant.
CA Name	Specifies the Connectivity Association (CA) name associated with the MKA session participant.
MKA-Profile Name	Specifies the name of the MKA profile.
MKA Enable	Specifies whether MKA is enabled for the port.
Actor Priority	Specifies a hexadecimal value for actor priority, which determines key server selection.

## Examples

The following example displays information for all participants in an MKA session.

```
Switch:1(config)#show macsec mka participant
```

```

=====
MACsec MKA Participants
=====
Port   CA           MKA-Profile   MKA   Actor
Id     Name         Name          Enable Priority
-----
1/3    CA120022    extreme030519 Enabled   A
1/4    CA121023    extreme031519 Enabled  14
2/2    CA122024    extreme032019 Enabled  1E
=====

```

The following example displays information for a specific port participating in an MKA session.

```
Switch:1(config)#show macsec mka participant 1/3
```

```

=====
MACsec MKA Participant
=====
Port   CA           MKA-Profile   MKA   Actor
Id     Name         Name          Enable Priority
-----
1/3    CA120022    extreme030519 Enabled   A
=====

```

## show macsec mka profile

Display information about all MKA profiles configured on the switch. You can also display information for a specific MKA profile.

## Syntax

- **show macsec mka profile**
- **show macsec mka profile WORD<0-16>**

## Command Parameters

WORD<0-16>

Specifies the MKA profile name. An MKA profile name can consist only of alphanumeric characters (0-9, A-Z, and a-z). The profile name is case sensitive.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show macsec mka profile** command displays the following information:

Output field	Description
Profile-name	Specifies the profile name.
Profile ID	Specifies the profile ID number.
Cipher Suite	Specifies the encryption algorithm used to encrypt traffic on an Ethernet link that is secured with MACsec.
Confidentiality Offset	Specifies the number of unencrypted bytes that precede MACsec encryption.
Replay Protect	Specifies whether replay protect is enabled. The default is disabled.
Window Size	Specifies the size of the replay protect window.
Port	Specifies the port to which the MKA profile is applied.
Include-SCI <b>Note:</b> Exception: not supported on VSP 8600 Series.	Specifies whether SCI tagging for a MACsec enabled switch. The default is disabled.

## Examples

The following example displays MACsec MKA profile information:

```
Switch:1#show macsec mka profile
```

```
=====
MACsec MKA Profile
```

```

=====
Profile      Profile  Cipher      Confidentiality  Replay      Window      Port      Include-SCI
Name         Id       Suite       Offset          Protect     Size
-----
test030519   1        gcm-aes-128  30             Enabled    200         1/3       false
test031519   2        gcm-aes-128  50             Enabled    225         1/4       false
test032019   3        gcm-aes-128  30             Enabled    240         2/2       false
=====

```

All 3 out of 3 Total Num of MACsec MKA Profiles displayed

The following example displays MACsec MKA information for a specific profile.

```
Switch:1#show macsec mka profile test030519
```

```

=====
MACsec MKA Profile
=====
Profile      Profile  Cipher      Confidentiality  Replay      Window      Port      Include-SCI
Name         Id       Suite       Offset          Protect     Size
-----
test030519   1        gcm-aes-128  30             Enabled    200         1/3       false
=====

```

## show macsec mka statistics

Display MACsec Key Agreement (MKA) statistics for a port.

### Syntax

- **show macsec mka statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Default

None.

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show macsec mka statistics** command displays the following information:

Output field	Description
MKPDU Validated & Rx	Specifies the number of MACsec Key Agreement Protocol Data Units (MKPDU) validated and received.
Rx Distributed SAK	Specifies the number of Secure Association Keys (SAK) received.
MKPDU Transmitted	Specifies the number of MKPDUs transmitted.
Tx Distributed SAK	Specifies the number of SAKs transmitted.

## Example

The following example displays MACsec MKA statistics for a port.

```
Switch:1>show macsec mka statistics 3/5
=====
                        MKPDU Statistics on interface 3/5
=====
      MKPDUs Validated & Rx      : 1630
      Rx Distributed SAK         : 2
      MKPDUs Transmitted         : 1694
      Tx Distributed SAK         : 0
=====
=====
```

## show macsec statistics

Display MACsec statistics for all ports or for an individual port.

## Syntax

- **show macsec statistics**
- **show macsec statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **show macsec statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} secure channel <inbound | outbound>**

## Default

None.

## Command Mode

User EXEC



## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show macsec statistics** command displays the following information:

Output field	Description
Port ID	Specifies the ID of the port to which the MACsec statistics apply.
TxUntagged Packets	Specifies the number of transmitted packets without the MAC security tag (SecTAG), with MACsec disabled on the interface.
TxTooLong Packets	Specifies the number of transmitted packets discarded because the packet length is greater than the Maximum Transmission Unit (MTU) of the Common Port interface.
RxUntagged Packets	Specifies the number of received packets without the SecTAG, with MACsec not operating in strict mode.
RxNoTag Packets	Specifies the number of received packets without the SecTAG, with MACsec operating in strict mode.
RxBadTag Packets	Specifies the number of received packets discarded with an invalid SecTAG, or with a zero value Packet Number (PN)/invalid Integrity Check Value (ICV).
RxUnknown SCIPackets	Specifies the number of packets received with an unknown Secure Channel Identifier (SCI) and with MACsec not operating in strict mode.
RxNoSCI Packets	Specifies the number of packets received with an unknown SCI and with MACsec operating in strict mode.
RxOverrun Packets	Specifies the number of packets discarded because the number of received packets exceeded the cryptographic performance capabilities.

## Example

The following example displays MACsec statistics for a specific port.

```
Switch:1>show macsec statistics 1/13
```

```
=====
MACSEC Port Statistics
=====
PortId      TxUntagged  TxTooLong  RxUntagged  RxNoTag
Packets    Packets    Packets    Packets    Packets
-----
1/13        0           0           0           0

PortId      RxBadTag   RxUnknown  RxNoSCI     RxOverrun
Packets    SCIPackets Packets    Packets     Packets
-----
1/13        0           0           0           0
```

## show macsec status

Display the following information for MACsec enabled interfaces:

- MACsec status
- MACsec encryption status
- CAK in MD5 checksum format

### Syntax

- **show macsec status**
- **show macsec status {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

```
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show macsec status** command displays the following information:

Output field	Description
PortId	Specifies the port ID number.
MACSEC Status	Specifies whether MACsec is enabled.
Encryption Status	Specifies whether encryption is enabled.
Replay Protect	Specifies whether replay protection is enabled.
Replay Protect Window	Specifies the size of the replay protect window.

Output field	Description
Encryption Offset	Specifies the number of unencrypted bytes that precede MACsec encryption.
Cipher Suite	Specifies the encryption algorithm used to encrypt traffic on an Ethernet link that is secured with MACsec.
CA Name	Specifies the name of the Connectivity Association.
MKA-Profile Name	Specifies the name of the MKA profile applied to the port.
MKA Connect Status	Specifies the MKA connection status.

## Example

The following example displays MACsec status for all ports:

```
Switch:1#show macsec status

=====
MACSEC Port Status
=====
Profile      MACSEC      Encryption  Replay      Replay      Encryption  Cipher  CA      MKA-
PortId      MKA Connect  Status      Protect      Protect W'dow  Offset      Suite   Name
Name                Status
-----
1/13      disabled  disabled  disabled  --          none          AES-128  NIL
--                --
1/14      disabled  disabled  disabled  --          none          AES-128  NIL
--                --
1/15      enabled   disabled  enabled   50         ipv4Offset(30) AES-256  mkanka
extreme                pending
```

The following example displays MACsec status for a specific port:

```
Switch:1#show macsec status 1/13

=====
MACSEC Port Status
=====
Profile      MACSEC      Encryption  Replay      Replay      Encryption  Cipher  CA      MKA-
PortId      MKA Connect  Status      Protect      Protect W'dow  Offset      Suite   Name
Name                Status
-----
1/13      enabled   disabled  enabled   50         ipv4Offset(30) AES-256  mkanka
extreme                pending
```

## show mgmt dhcp-client

Shows DHCP Client configuration information for the Segmented Management Instance.

## Syntax

- **show mgmt dhcp-client**
- **show mgmt dhcp-client log**

## Command Parameters

### log

Shows log information specific to the DHCP Client for the Segmented Management Instance.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show mgmt dhcp-client** command displays the following information:

Output field	Description
DHCP-CLIENT-MODE	Specifies the DHCP Client mode as disabled, oob, vlan, or cycle.
PREFERRED-INTERFACE	Specifies the preferred interface for DHCP requests.

## Examples

```
Switch:1>show mgmt dhcp-client
=====
                          Mgmt DHCP Client Info:
=====
DHCP-CLIENT-MODE    PREFERRED-INTERFACE
-----
disabled             none
-----

Switch:1>show mgmt dhcp-client log
Jun  5 05:45:26 gemini daemon.info dhclient: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 18
Jun  5 05:45:26 gemini local0.err dhclient-fan: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 18
Jun  5 05:45:44 gemini daemon.info dhclient: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 9
Jun  5 05:45:44 gemini local0.err dhclient-fan: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 9
Jun  5 05:45:53 gemini daemon.info dhclient: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 8
Jun  5 05:45:53 gemini local0.err dhclient-fan: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 8
Jun  5 05:46:01 gemini daemon.info dhclient: No DHCP OFFERS received.
Jun  5 05:46:01 gemini daemon.info dhclient: No working leases in persistent database - sleeping.
Jun  5 05:46:01 gemini local0.err dhclient-fan: No DHCP OFFERS received.
```

```
Jun  5 05:46:01 gemini local0.err dhclient-fan: No working leases in persistent database - sleeping.
Jun  5 05:46:13 gemini daemon.info dhclient: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 6
Jun  5 05:46:13 gemini local0.err dhclient-fan: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 6
Jun  5 05:46:19 gemini daemon.info dhclient: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 15
Jun  5 05:46:19 gemini local0.err dhclient-fan: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 15
Jun  5 05:46:34 gemini daemon.info dhclient: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 17
Jun  5 05:46:34 gemini local0.err dhclient-fan: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 17
Jun  5 05:46:51 gemini daemon.info dhclient: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 17
Jun  5 05:46:51 gemini local0.err dhclient-fan: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 17
Jun  5 05:47:08 gemini daemon.info dhclient: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 6
Jun  5 05:47:08 gemini local0.err dhclient-fan: DHCPDISCOVER on linuxFAN to 255.255.255.255 port 67
interval 6
```

## Usage Guidelines

This command is not supported on VSP 8600 Series.

## show mgmt interface

Shows general configuration information about a Segmented Management Instance.

## Syntax

- **show mgmt interface**
- **show mgmt interface clip**
- **show mgmt interface oob**
- **show mgmt interface vlan**

## Command Parameters

### clip

Shows information specific to the management CLIP.

### oob

Shows information specific to the management OOB.

### vlan

Shows information specific to the management VLAN.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

VSP 8600 Series does not support the `oob` or `vlan` parameters. XA1400 Series does not support the `oob` parameter.

The command parameters do not apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

## show mgmt ip

---

Shows IPv4 address information for a Segmented Management Instance.

## Syntax

- `show mgmt ip`
- `show mgmt ip clip`
- `show mgmt ip icmp-statistics`
- `show mgmt ip ip-statistics`
- `show mgmt ip oob`
- `show mgmt ip tcp-connections`
- `show mgmt ip tcp-statistics`
- `show mgmt ip udp-endpoints`
- `show mgmt ip udp-statistics`
- `show mgmt ip vlan`

## Command Parameters

### clip

Shows information specific to the management CLIP.

### icmp-statistics

Shows information specific to the management interface ICMP statistics.

### ip-statistics

Shows information specific to the management interface IP statistics.

### oob

Shows information specific to the management OOB.

### tcp-connections

Shows information specific to the management interface TCP connections.

### tcp-statistics

Shows information specific to the management interface TCP statistics.

**udp-endpoints**

Shows information specific to the management interface UDP endpoints.

**udp-statistics**

Shows information specific to the management interface UDP statistics.

**vlan**

Shows information specific to the management VLAN.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The *icmp-statistics*, *ip-statistics*, *tcp-statistics*, *tcp-connections*, *udp-endpoints*, *udp-statistics*, and *vlan* parameters are not supported on VSP 8600 Series.

The *oob* parameter is not supported on VSP 8600 Series and XA1400 Series.

## show mgmt ip arp

---

Shows ARP information for a Segmented Management Instance.

## Syntax

- **show mgmt ip arp**
- **show mgmt ip arp clip**
- **show mgmt ip arp oob**
- **show mgmt ip arp vlan**

## Command Parameters

**clip**

Shows information specific to the management CLIP.

**oob**

Shows information specific to the management OOB.

**vlan**

Shows information specific to the management VLAN.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The command parameters do not apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

## show mgmt ip route

---

Shows operational IPv4 routes for a Segmented Management Instance.

## Syntax

- **show mgmt ip route**
- **show mgmt ip route clip**
- **show mgmt ip route oob**
- **show mgmt ip route vlan**

## Command Parameters

### clip

Shows information specific to the management CLIP.

### oob

Shows information specific to the management OOB.

### vlan

Shows information specific to the management VLAN.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines



The command parameters do not apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

## show mgmt ip icmp

---

Displays the IPv4 ICMP information for a Segmented Management Instance.

### Syntax

- **show mgmt ip icmp**
- **show mgmt ip icmp clip**
- **show mgmt ip icmp oob**
- **show mgmt ip icmp vlan**

### Command Parameters

#### clip

Displays the IPv4 ICMP information specific to the management CLIP.

#### oob

Displays the IPv4 ICMP information specific to the management OOB.

#### vlan

Displays the IPv4 ICMP information specific to the management VLAN.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

### Examples

The following example displays information of ICMP drop packet filtering for IPv4 network:

```
Switch:1>show mgmt ip icmp clip
```

```
=====
Mgmt IP ICMP Information.
=====
```

```
icmp-drop-fragments      : disable
```

---

## show mgmt ip route static

---

Shows IPv4 static routes for a management interface.

### Syntax

- **show mgmt ip route static**
- **show mgmt ip route static clip**
- **show mgmt ip route static oob**
- **show mgmt ip route static vlan**

### Command Parameters

#### clip

Shows information specific to the management CLIP.

#### oob

Shows information specific to the management OOB.

#### vlan

Shows information specific to the management VLAN.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

The command parameters do not apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## show mgmt ipv6

---

Shows IPv6 address information for a Segmented Management Instance.

### Syntax

- **show mgmt ipv6**
- **show mgmt ipv6 clip**

- `show mgmt ipv6 icmp-statistics`
- `show mgmt ipv6 ip-statistics`
- `show mgmt ipv6 oob`
- `show mgmt ipv6 tcp-connections`
- `show mgmt ipv6 tcp-statistics`
- `show mgmt ipv6 udp-endpoints`
- `show mgmt ipv6 udp-statistics`
- `show mgmt ipv6 vlan`

## Command Parameters

### `clip`

Shows information specific to the management CLIP.

### `icmp-statistics`

Shows information specific to the management interface ICMP statistics.

### `ip-statistics`

Shows information specific to the management interface IP statistics.

### `oob`

Shows information specific to the management OOB.

### `tcp-connections`

Shows information specific to the management interface TCP connections.

### `tcp-statistics`

Shows information specific to the management interface TCP statistics.

### `udp-endpoints`

Shows information specific to the management interface UDP endpoints.

### `udp-statistics`

Shows information specific to the management interface UDP statistics.

### `vlan`

Shows information specific to the management VLAN.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The *icmp-statistics*, *ip-statistics*, *tcp-statistics*, *tcp-connections*, *udp-endpoints*, *udp-statistics*, and *vlan* parameters are not supported on VSP 8600 Series.

The *oob* parameter is not supported on VSP 8600 Series and XA1400 Series.

## show mgmt ipv6 icmp

Displays the IPv6 ICMP information for a Segmented Management Instance.

## Syntax

- **show mgmt ipv6 icmp**
- **show mgmt ipv6 icmp clip**
- **show mgmt ipv6 icmp oob**
- **show mgmt ipv6 icmp vlan**

## Command Parameters

### clip

Displays the IPv6 ICMP information specific to the management CLIP.

### oob

Displays the IPv6 ICMP information specific to the management OOB.

### vlan

Displays the IPv6 ICMP information specific to the management VLAN.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Examples

The following example displays information of ICMP drop packet filtering for IPv6 network:

```
Switch:1>show mgmt ipv6 icmp clip
```

```
=====
```

```
Mgmt IPV6 ICMP Information.
-----
icmp-drop-fragments      : disable
```

## show mgmt ipv6 neighbor

---

Shows the Neighbor Discovery cache for a Segmented Management Instance.

### Syntax

- **show mgmt ipv6 neighbor**
- **show mgmt ipv6 neighbor clip**
- **show mgmt ipv6 neighbor oob**
- **show mgmt ipv6 neighbor vlan**

### Command Parameters

#### clip

Shows information specific to the management CLIP.

#### oob

Shows information specific to the management CLIP.

#### vlan

Shows information specific to the management VLAN.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

The command parameters do not apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

## show mgmt ipv6 route

---

Shows operational IPv6 routes for a Segmented Management Instance.

## Syntax

- **show mgmt ipv6 route**
- **show mgmt ipv6 route clip**
- **show mgmt ipv6 route oob**
- **show mgmt ipv6 route vlan**

## Command Parameters

### clip

Shows information specific to the management CLIP.

### oob

Shows information specific to the management OOB.

### vlan

Shows information specific to the management VLAN.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The command parameters do not apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

## show mgmt ipv6 route static

---

Shows IPv6 static routes for a management interface.

## Syntax

- **show mgmt ipv6 route static**
- **show mgmt ipv6 route static clip**
- **show mgmt ipv6 route static oob**
- **show mgmt ipv6 route static vlan**

## Command Parameters

### clip

Shows information specific to the management CLIP.

### oob

Shows information specific to the management OOB.

#### vlan

Shows information specific to the management VLAN.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

The command parameters do not apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

## show mgmt migration

---

View the designated interface addresses selected for migration to a Segmented Management Instance.

### Syntax

- **show mgmt migration**

### Default

None

### Command Mode

User EXEC

## show mgmt rmon

---

Display the RMON2 configuration state of the management interface.

### Syntax

- **show mgmt rmon**

### Command Mode

User EXEC

## Usage Guidelines

This command is not supported on VSP 8600 Series.

## Command Output

The **show mgmt rmon** command displays the following information:

Output field	Description
INST	Specifies the management instance ID.
DESCR	Specifies the interface type.
RMON-ADMIN-ENABLE	Specifies whether RMON2 is enabled on the management interface.
RMON-OPER-ENABLE	Specifies whether RMON2 is operationally enabled on the management interface, meaning that the interface itself is also enabled.
RMON-IP-ADDR	Specifies the management interface preferred IPv4 address.

## Example

```
Switch:1>show mgmt rmon
=====
Mgmt Rmon Information
=====
INST  DESCR  RMON-ADMIN-ENABLE  RMON-OPER-ENABLE  RMON-IP-ADDR
-----
1 Mgmt-oob1  disable  disable  0.0.0.0
3 Mgmt-clip  enable   enable   192.0.2.72
4 Mgmt-vlan  enable   enable   198.51.100.72
```

## show mgmt statistics

View operational statistics for a Segmented Management Instance.

## Syntax

- **show mgmt statistics**
- **show mgmt statistics clip**
- **show mgmt statistics oob**
- **show mgmt statistics vlan**

## Command Parameters

**clip**

Shows information specific to the management CLIP.

**oob**

Shows information specific to the management OOB.



**vlan**

Shows information specific to the management VLAN.

**Default**

None

**Command Mode**

User EXEC

**Usage Guidelines**

The command parameters do not apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

---

**show mgmt topology-ip**

---

View topology ip address information for a Segmented Management Instance.

**Syntax**

- **show mgmt topology-ip**

**Command Parameters**

None

**Default**

None

**Command Mode**

User EXEC

**Usage Guidelines**

The command is not supported on VSP 8600 Series. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

**show mirror-by-port**

---

Shows mirror-by-port diagnostic information.

## Syntax

- **show mirror-by-port**
- **show mirror-by-port WORD<1-1024> MirrorId List {1-479}**

## Command Parameters

MirrorID List {1-479}

Displays the requested mirrors.

WORD<1-1024>

Displays mirror-by-port diagnostic information.

## Default

None

## Command Mode

User EXEC

## show mirror-resources

---

Shows information about mirror resource usage.

## Syntax

- **show mirror-resources**

## Default

None

## Command Mode

User EXEC

## show mlt

---

Display MultiLink Trunking (MLT) information, including port type, port members and designated ports.

## Syntax

- **show mlt**
- **show mlt <1-512>**

## Command Parameters

<1-512>

Specifies the MLT ID. The value ranges from 1-512.

## Default

None

## Command Mode

User EXEC

## show mlt error collision

---

View information about collision errors to obtain information about collision errors in the specified MLT, or for all MLTs.

## Syntax

- **show mlt error collision**
- **show mlt error collision <1-512>**

## Command Parameters

<1-512>

Specifies the MLT ID. The value ranges from 1-512.

## Default

None

## Command Mode

User EXEC

## show mlt error main

---

View information about Ethernet errors to display information about the types of Ethernet errors sent and received by the specified MLT or all MLTs.

## Syntax

- **show mlt error main**
- **show mlt error main <1-512>**

## Command Parameters

<1-512>

Specifies the MLT ID. The value ranges from 1-512.

## Default

None

## Command Mode

User EXEC

## show mlt i-sid

---

Display all configured service instance identifiers (I-SID) on mlt.

## Syntax

- **show mlt i-sid <1-512>**

## Command Parameters

<1-512>

specifies the MLT ID.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show mlt i-sid** command displays the following information:

Output field	Description
MLTID	Indicates the MLT ID.
IFINDEX	Indicates the interface index.
ISID ID	Indicates the unique I-SID value.
VLANID	Indicates the platform VLAN ID associated with the I-SID endpoint.
C-VID	Indicates the customer VLAD ID.

Output field	Description
ISID TYPE	Indicates one of the following I-SID types: <ul style="list-style-type: none"> <li>T-UNI: Transparent Port UNI service.</li> <li>ELAN: any to any service (switched service).</li> <li>CVLAN: CVLAN based service.</li> </ul>
ORIGIN	Indicates the origin of the service that is associated with the I-SID interface.
ISID NAME	Indicates the name of the I-SID.
BPDU	Indicates the BPDU forward option for the untagged traffic port.

## Example

The following example displays the command output.

```
Switch:1>show mlt i-sid
=====
                        MLT Isid Info
=====
MLTID   IFINDEX   ISID   VLANID   C-VID   ISID   ORIGIN   ISID   BPDU
         ID      TYPE
-----
3       6146     3      N/A      33     ELAN   C --- - --- - ISID-3
-----
1 out of 1 Total Num of i-sid endpoints displayed

ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
M: FA management; E: discovered by EAP; A: auto-sense
l: discover by local switch  r: discover by remote VIST switch
```

## show mlt stats

View MLT statistics to display MultiLinkTrunking statistics for the switch or for the specified MLT ID.

### Syntax

- show mlt stats**
- show mlt stats <1-512>**

### Command Parameters

<1-512>

Specifies the MLT ID. The value ranges from 1-512.

### Default

None

## Command Mode

User EXEC

## Command Output

The **show mlt stats** command displays the following information:

Output field	Description
ID IN-OCTETS	The total number of inbound octets of data (including those in bad packets).
OUT-OCTETS	The total number of outbound octets of data.
IN-UNICAST	The count of inbound Unicast packets.
OUT-UNICAST	The count of outbound unicast packets.
ID IN-MULTICAST	The count of inbound multicast packets.
OUT-MULTICAST	The count of outbound multicast packets.
IN-BROADCAST	The count of inbound broadcast packets.
OUT-BROADCAST	The count of outbound broadcast packets.
MT	The MLT type: P for POS, E for Ethernet, A for ATM.

## show monitor-statistics

Display monitor timer configurations, including duration and interval.

### Syntax

- **show monitor-statistics**

### Default

None

## Command Mode

User EXEC

## show multicast software-forwarding

Show the software forwarding configuration.

### Syntax

- **show multicast software-forwarding**

## Default

None

## Command Mode

User EXEC

## show ntp

---

View the Network Time Protocol (NTP) server status statistics.

## Syntax

- **show ntp**
- **show ntp key**
- **show ntp restrict**
- **show ntp server**
- **show ntp statistics**

## Command Parameters

### key

Specifies to show NTP authentication key information.

### restrict

Displays the NTP restrict information.

### server

Specifies to show NTP server information.

### statistics

Specifies to show NTP statistics information.

## Default

None

## Command Mode

User EXEC

## show ovssdb

---

View the OVSSDB configuration information

## Syntax

- **show ovssdb configs**
- **show ovssdb controller status**
- **show ovssdb managed-interface**
- **show ovssdb replication state**

## Command Parameters

### configs

Displays the OVSSDB configuration information.

### controller status

Displays the OVSSDB controller information.

### managed-interface

Displays the OVSSDB managed-interface information.

### replication state

Displays the OVSSDB replication information.

## Default

None

## Command Mode

User EXEC

## show qos 802.1p-override

---

Display the 802.1p override status for a port or VLAN.

## Syntax

- **show qos 802.1p-override**
- **show qos 802.1p-override gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show qos 802.1p-override vlan <1-4059>**

## Command Parameters

**gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.



**vlan** <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show qos cosq-stats

---

Display the Quality of Service (QoS) egress queues statistics. The show output displays either unicast packet stats for each port, or all stats, based on your hardware platform.

## Syntax

- **show qos cosq-stats**
- **show qos cosq-stats interface {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show qos cosq-stats loopback-port <1-2>**

## Command Parameters

**interface {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Show Qos Cosq Stats on port. {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**loopback-port <1-2>**

Shows Qos Cosq Stats on loopback port.

## Default

None

## Usage Guidelines

The show command output varies based on your hardware platform. On all supported platforms except the VSP 8600 Series, the show command output displays Out Packets and Out Bytes per interface,

which shows the number of unicast packets sent out on each queue for an egress port. VSP 8600 Series uses VoQ queuing architecture, which enables to read the Accepted Packets and Accepted Bytes on each queue. The Accepted Packets and Accepted Bytes show the number of packets and bytes that enter the VoQ for a particular queue on the egress port. The Drop Packets and Drop Bytes show the number of packets and bytes that are dropped when the VoQ is full.

## Command Output

The **show qos cosq-stats** command displays the following information:

Output field	Description
Cos  <b>Note:</b> Exception: only supported on VSP 4450 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series VSP 8400 Series, and XA1400 Series	Indicates the CoS queue number.
Out Packets  <b>Note:</b> Exception: only supported on VSP 4450 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series VSP 8400 Series, and XA1400 Series	Indicates the out packets for the CoS queue.
Out Bytes  <b>Note:</b> Exception: only supported on VSP 4450 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series VSP 8400 Series, and XA1400 Series	Indicates the out bytes for the CoS queue.
Accepted Packets  <b>Note:</b> Exception: only supported on VSP 8600 Series.	Indicates the accepted packets for the Cos queue.
Accepted Bytes  <b>Note:</b> Exception: only supported on VSP 8600 Series.	Indicates the accepted bytes for the Cos queue.

Output field	Description
Drop Packets	Indicates the drop packets for the CoS queue.
Drop Bytes	Indicates the drop bytes for the CoS queue.

## Command Mode

User EXEC

## Examples

The following example displays all stats.

```
Switch:1#show qos cosq-stats interface 1/42

=====
Port:1/42  QOS CoS Queue Stats
=====
CoS  Out Packets      Out Bytes      Drop Packets    Drop Bytes
-----
0    0                0              0               0
1    0                0              0               0
2    0                0              0               0
3    0                0              0               0
4    0                0              0               0
5    0                0              0               0
6    0                0              0               0
7    0                0              0               0
Switch:1#
```

The following example displays unicast packet stats for each port.

```
Switch:1#show qos cosq-stats interface

=====
QOS Cos Queue Stats Table
=====
Port:1/1  QOS Known Unicast CoS Queue Stats
=====
CoS  Accepted Packets  Accepted Bytes  Drop Packets    Drop Bytes
-----
0    0                0              0               0
1    0                0              0               0
2    0                0              0               0
3    0                0              0               0
4    0                0              0               0
5    0                0              0               0
6    0                0              0               0
7    0                0              0               0
=====
Port:1/2  QOS Known Unicast CoS Queue Stats
=====
CoS  Accepted Packets  Accepted Bytes  Drop Packets    Drop Bytes
-----
0    0                0              0               0
1    0                0              0               0
2    0                0              0               0
3    0                0              0               0
4    0                0              0               0
```

```

5      0      0      0      0
6      0      0      0      0
7      0      0      0      0
=====
Port:1/3   QoS Known Unicast CoS Queue Stats
=====
CoS  Accepted Packets      Accepted Bytes      Drop Packets      Drop Bytes
0    0                  0                  0                  0
1    1622              124894             0                  0
2    0                  0                  0                  0
3    0                  0                  0                  0
4    0                  0                  0                  0
5    0                  0                  0                  0
6    0                  0                  0                  0
7    331              46671             0                  0
=====

```

## show qos cosq-stats cpu-port

Display the Quality of Service (QoS) egress queues statistics for the CPU port to display the statistics of the forwarded packets and bytes, and the dropped packets and bytes, for the traffic sent toward the CP. The queue assignment is based on the protocol types, not on the internal COS value. These statistics are useful for debugging purposes..

### Syntax

- **show qos cosq-stats cpu-port**

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

The show command output varies based on your hardware platform. On all supported platforms except the VSP 8600 Series, the show command output displays Out Packets and Out Bytes per interface, which shows the number of unicast packets sent out on each queue for an egress port. VSP 8600 Series uses VoQ queuing architecture, which enables to read the Accepted Packets and Accepted Bytes on each queue. The Accepted Packets and Accepted Bytes show the number of packets and bytes that enter the VoQ for a particular queue on the egress port. The Drop Packets and Drop Bytes show the number of packets and bytes that are dropped when the VoQ is full.

## Command Output

The **show qos cosq-stats cpu-port** command displays the following information:

Output field	Description
Cos  <b>Note:</b> Exception: only supported on VSP 4450 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series VSP 8400 Series, and XA1400 Series	Indicates the CoS queue number.
Protocol  <b>Note:</b> Exception: only supported on VSP 8600 Series.	Indicates the type of protocol.
Out Packets  <b>Note:</b> Exception: only supported on VSP 4450 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series VSP 8400 Series, and XA1400 Series	Indicates the out packets for the CoS queue.
Out Bytes  <b>Note:</b> Exception: only supported on VSP 4450 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series VSP 8400 Series, and XA1400 Series	Indicates the out bytes for the CoS queue.
Accepted Packets  <b>Note:</b> Exception: only supported on VSP 8600 Series.	Indicates the accepted packets for the Cos queue.
Accepted Bytes  <b>Note:</b> Exception: only supported on VSP 8600 Series.	Indicates the accepted bytes for the Cos queue.
Drop Packets	Indicates the drop packets for the CoS queue.

Output field	Description
Drop Bytes	Indicates the drop bytes for the CoS queue.
Priority  <b>Note:</b> Exception: only supported on VSP 8600 Series.	Indicates the priority of the queue for the packet going to CP.
Shape Rate (kbps)  <b>Note:</b> Exception: only supported on VSP 8600 Series.	Indicates the maximum throughput in kbps to CP when a burst occurs . Packets exceeding this limit will be dropped.

## Examples

The following examples display output for the **show qos cosq-stats cpu-port** command.



### Note

Protocols displayed vary across hardware models..

```
Switch:1>show qos cosq-stats cpu-port
```

=====

QOS CoS Queue Cpu Port Stats Table

=====

CoS	Out Packets	Out Bytes	Drop Packets	Drop Bytes
0	3670	254978	0	0
1	41839	2886814	0	0
2	0	0	0	0
3	765	52020	0	0
4	130	14552	0	0
5	0	0	0	0
6	14418	2766226	0	0
7	20727	1876222	0	0
8	15941	2074921	0	0
9	1246091	84734188	17168	1133080
10	32314	5483005	0	0
11	396323	26949964	4990	319376
12	195649	16583033	0	0
13	426754	53924425	0	0
14	0	0	0	0
15	0	0	0	0

```
Switch:1>show qos cosq-stats cpu-port
```

=====

QOS CoS Queue Cpu Port Stats Table

=====

Protocol	Accepted Packets	Accepted Bytes	Drop Packets	Drop Bytes	Priority	Shape Rate(kbps)
vrrp	0	0	0	0	7	5628
vlacp	0	0	0	0	7	2345
lacp	0	0	0	0	7	4690
cfm	16	1024	0	0	7	9380
vrrp_v6	0	0	0	0	7	5628
ist_ctl	0	0	0	0	6	9380
radius	0	0	0	0	6	2345
ntp	0	0	0	0	6	938
icmpv4	2	212	0	0	6	938
slpp	0	0	0	0	6	4690
bpdu	0	0	0	0	6	2345
tdp	78	4992	0	0	6	938

eap	0	0	0	0	6	2345
lldp	16	2800	0	0	6	938
nd_mc_v6	0	0	0	0	6	9380
nd_uc_v6	0	0	0	0	6	2345
rlogin	0	0	0	0	6	2345
frag_uc_v6	0	0	0	0	6	2345
isis	887	558782	0	0	5	9380
ospf_mc	0	0	0	0	5	11725

## show qos egressmap

Display the Quality of Service (QoS) egress mappings.

### Syntax

- **show qos egressmap**
- **show qos egressmap 1p**
- **show qos egressmap 1p <0-7>**
- **show qos egressmap ds**
- **show qos egressmap ds <0-7>**

### Command Parameters

**1p <0-7>**

Displays the QoS level to IEEE 802.1p priority mapping.

**ds <0-7>**

Displays the QoS level to DS byte mapping.

### Default

None

### Command Mode

User EXEC

## show qos ingressmap

Ensure the accuracy of the ingress configuration.

### Syntax

- **show qos ingressmap**
- **show qos ingressmap 1p**
- **show qos ingressmap 1p <0-7>**
- **show qos ingressmap ds**
- **show qos ingressmap ds <0-63>**

## Command Parameters

**1p <0-7>**

Show IEEE 1p to Qos level mapping

**ds <0-63>**

Show DS Byte to Qos level mapping

## Default

None

## Command Mode

User EXEC

# show qos queue-profile

---

Displays the queue profile.

## Syntax

- **show qos queue-profile <1-5> queue <0-7>**
- **show qos queue-profile <1-5> queue all**

## Command Parameters

**<0-7>**

Specifies the queue identifier.

**<1-5>**

Displays the qos queue parameter settings for the specified queue profile ID.

**all**

Displays the qos queue parameter settings for all queues.

**queue**

Displays the qos queue parameter settings for specified queue profile ID.

## Default

None

## Command Mode

User EXEC



---

## show qos rate-limiting

---

Show port ingress rate-limit information.

### Syntax

- **show qos rate-limiting interface gigabitEthernet**
- **show qos rate-limiting interface gigabitEthernet** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

### Command Parameters

**interface gigabitEthernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

---

## show qos shaper

---

Display egress rate-limiting information for an interface.

### Syntax

- **show qos shaper interface gigabitEthernet**
- **show qos shaper interface gigabitEthernet** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

### Command Parameters

**interface gigabitEthernet** {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/

port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## show radius

Display the global status of Remote Access Dial-In User Services (RADIUS) information.

## Syntax

- **show radius**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show radius** command displays the following information:

Output field	Description
acct-attribute-value	Specifies the accounting attribute value.
acct-enable	Specifies if the accounting attribute is enabled.
acct-include-cli-commands	Specifies if the accounting attribute includes CLI commands. The default is false.
access-priority-attribute	Specifies the value of the access priority attribute. The default is 192.
auth-info-attr-value	Specifies the value of the authentication information attribute. The default is 91.
command-access-attribute	Specifies the value of the command access attribute. The default is 194.
cli-commands-attribute	Specifies the value of the CLI commands attribute. The default is 195.
cli-cmd-count	Specifies how many CLI commands before the system sends a RADIUS accounting interim request. The default is 40.

Output field	Description
cli-profile-enable	Specifies if RADIUS CLI profiling is enabled. CLI profiling grants or denies access to users being authenticated by way of the RADIUS server. You can add a set of CLI commands to the configuration on the RADIUS server, and you can specify the command-access mode for these commands. The default is false.
enable	Specifies if RADIUS authentication is globally enabled on the switch.
igap-passwd-attr	Specifies the IGMP for user Authentication Protocol (IGAP) password attribute.
igap-timeout-log-fsize	Specifies the IGMP for user Authentication Protocol (IGAP) timeout log file size.
maxserver	Specifies the maximum number of servers allowed for the device. The default is 10.
mcast-addr-attr-value	Specifies the value of the multicast address attribute. The default is 90.
secure-flag	Specifies whether RADIUS Security (RADSec) is globally enabled. The default is disabled.
sourceip-flag <b>Note:</b> Exception: only supported on VSP 8600 Series.	Specifies if the switch can use a configured source IP address. If the outgoing interface on the switch fails, a different source IP address is used, which requires that you make configuration changes to define the new RADIUS client on the RADIUS server. To simplify RADIUS server configuration, you can configure the switch to use a circuitless IP (CLIP) address as the source IP and NAS IP address when transmitting RADIUS packets. By default, the switch uses the IP address of the outgoing interface as the source IP, and the NAS IP address for RADIUS packets that it transmits.

## show radius dynamic-server

Display configuration or statistical information about RADIUS dynamic session clients.

### Syntax

- **show radius dynamic-server client WORD<0-46>**
- **show radius dynamic-server statistics**

### Command Parameters

#### statistics

Display statistics for RADIUS Dynamic Authorization clients.

#### WORD<0-46>

Specifies the client IPv4 or IPv6 address.

### Default

None

## Command Mode

User EXEC

## Examples

The **show radius dynamic-server** command displays the following information:

```
Switch:1#show radius dynamic-server

=====
                        RADIUS Dynamic Authorization General Info
=====
CLIENT ADDRESS                UDP PORT      CLIENT ENABLED  SECRET KEY
-----
192.0.2.15                    1026        Disabled    *****
192.0.2.16                    1027        Disabled    *****
-----

All 2 out of 2 Total Num of RADIUS Dynamic Authorization clients displayed
```

The following output displays dynamic server statistics:

```
Switch:1#show radius dynamic-server statistics

=====
                        RADIUS Dynamic Authorization Global Statistics
=====
Disconnects From Invalid Client Addresses:    0
CoAs From Invalid Client Addresses:          0
-----
```

## show radius reachability

Display the RADIUS server reachability settings.

## Syntax

- **show radius reachability**

## Default

None

## Command Mode

User EXEC

## show radius snmp

Display the global status of Remote Access Dial-In User Services (RADIUS) information.

## Syntax

- **show radius snmp**

## Default

None

## Command Mode

User EXEC

---

## show radius secure-profile

---

Display information about configuration of RADIUS secure profiles.

## Syntax

- **show radius secure-profile**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show radius secure-profile** command displays the following information:

## Example

```
Switch:1>enable
Switch:1#show radius secure-profile
```

```
=====
                        Secure RADIUS profile
=====
Profile default:
  Name      : default
  RootCert  : n/a
  Cert      : n/a
  Key       : n/a
  Password  : ""
RootCertDestFile :
CertDestFile  :
KeyDestFile   :
```

## show radius-server

Display the Remote Access Dial-In User Services (RADIUS) server information.

### Syntax

- **show radius-server**

### Default

None

### Command Mode

User EXEC

### Usage Guidelines



#### Note

Not all output fields apply to all hardware platforms . For more information about feature support, see [VOSS Feature Support Matrix](#).

### Command Output

The **show radius-server** command displays the following information:

Output field	Description
NAME	Specifies the RADIUS server name.
USEDDBY	Specifies how the server functions. Configures the server for authentication for one of the following:cli <ul style="list-style-type: none"> <li>• cli</li> <li>• eapol</li> <li>• endpoint-tracking</li> <li>• snmp</li> <li>• web</li> </ul>
SECRET	Specifies the secret key.
PORT	Specifies the RADIUS server UDP port.
PRIO	Specifies the RADIUS server priority.
RETRY	Specifies the maximum number of authentication retries. The default is 3.
TIMEOUT	Specifies the number of seconds before the authentication request times out. The default is 3.
ENABLED	Specifies whether the RADIUS server is enabled.

Output field	Description
SECURE ENABLED	Specifies whether RADSec is enabled on the RADIUS server.
SECURE MODE	Specifies the protocol used for secure connection with the server. Possible values are: <ul style="list-style-type: none"> <li>• tls - Transport Layer Security (TLS) encryption over Transmission Control Protocol (TCP)</li> <li>• dtls - Datagram Transport Layer Security (DTLS) encryption over User Datagram Protocol (UDP)</li> </ul> The default is tls.
SECURE INSTANCE	Specifies the radsecproxy instance. The default is -1 (the RADIUS server is not configured for RADSec).
SECURE PROFILE	Specifies the secure profile associated with the RADIUS server.
SECURE LOG-LEVEL	Specifies the secure log level. Possible values are: <ul style="list-style-type: none"> <li>• critical</li> <li>• debug</li> <li>• error</li> <li>• info</li> <li>• warning</li> </ul>
ACCT PORT	Specifies the RADIUS accounting UDP port.
ACCT ENABLED	Specifies whether RADIUS accounting is enabled.

## Example

The following example displays RADIUS server information:

```

-----
                        Radius Server Entries
-----
NAME                USEDDBY  SECRET  PORT  Prio  Retry  Timeout  SECURE  SECURE  SECURE  SECURE  SECURE  ACCT  ACCT
                   SECRET  PORT  Prio  Retry  Timeout  ENABLED  ENABLED  MODE   INSTANCE  PROFILE  LOG-LEVEL  PORT  ENABLED
-----
192.0.2.14          cli      ***** 1812 10    1     8       true   true   tls    0       radsecp  error    1813  true
192.0.2.15          cli      ***** 1812 10    1     8       true   false  tls    -1      default  error    1813  true

```

## show radius-server statistics

Display current Remote Access Dial-In User Services (RADIUS) server configurations.

## Syntax

- **show radius-server statistics**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show radius-server statistics** command displays the following information:

Output field	Description
Radius Server(UsedBy)	The IP address of the RADIUS server.
Access Requests	Specifies the number of access-response packets sent to the server; it does not include retransmissions.
Access Accepts	Specifies the number of access-accept packets, valid or invalid, received from the server.
Access Rejects	Specifies the number of access-reject packets, valid or invalid, received from the server.
Bad Responses	Specifies the number of invalid access-response packets received from the server.
Client Retries	Specifies the number of authentication retransmissions to the server.
Pending Requests	Specifies the number of access-request packets sent to the server that have not yet received a response, or have timed out.
Acct On Requests	Specifies the number of accounting On requests sent to the server.
Acct Off Requests	Specifies the number of accounting Off requests sent to the server.
Acct Start Requests	Specifies the number of accounting Start requests sent to the server.
Acct Stop Requests	Specifies the number of accounting Stop requests sent to the server.
Acct Interim Requests	Specifies the number of accounting Interim Requests sent to the server. The AcctInterimRequests counter increments only if the parameter acctinclude- cli-commands is set to true.
Acct Bad Responses	Specifies the number of Invalid Responses from the server that are discarded.
Acct Pending Requests	Specifies the number of requests waiting to be sent to the server.
Acct Client Retries	Specifies the number of retries made to this server.
Access Challenges	Shows the number of RADIUS access-challenges packets sent to this server. This does not include retransmission.
Round-trip Time	Shows the time difference between the instance when a RADIUS request is sent and the corresponding response is received.
Nas Ip Address	Shows the RADIUS client Network Access Server (NAS) identifier for this server.



## Example

The following example displays RADIUS server statistics information:

```
Switch:1#show radius-server statistics

Responses with invalid server address: 0

Radius Server(UsedBy) : 192.0.2.14(cli)
-----
    Access Requests : 2
    Access Accepts : 1
    Access Rejects : 0
    Bad Responses : 1
    Client Retries : 1
    Pending Requests : 0
    Acct On Requests : 0
    Acct Off Requests : 0
    Acct Start Requests : 0
    Acct Stop Requests : 0
    Acct Interim Requests : 0
    Acct Bad Responses : 0
    Acct Pending Requests : 0
    Acct Client Retries : 0
    Access Challenges : 0
    Round-trip Time :
    Nas Ip Address : 192.0.2.20

Radius Server(UsedBy) : 192.0.2.15(cli)
-----
    Access Requests : 1
    Access Accepts : 0
    Access Rejects : 0
    Bad Responses : 0
    Client Retries : 0
    Pending Requests : 1
    Acct On Requests : 0
    Acct Off Requests : 0
    Acct Start Requests : 0
    Acct Stop Requests : 0
    Acct Interim Requests : 0
    Acct Bad Responses : 0
    Acct Pending Requests : 0
    Acct Client Retries : 0
    Access Challenges : 0
    Round-trip Time :
    Nas Ip Address : 192.0.2.20
```

## show rmon address-map

View Remote Network Monitoring (RMON) settings to see the maps of network layer address to physical address to interface.

## Syntax

- **show rmon address-map**

## Command Parameters

### address-map

Displays the RMON control tables on the switch.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show rmon address-map** command displays the following information:

Output field	Description
PROTOIDX	Shows a unique identifier for the entry in the table.
HOSTADDR	Shows the network address for this entry. The format of the value depends on the protocol portion of the local index.
SOURCE	Shows the interface or port on which the network address was most recently seen.
PHYADDR	Shows the physical address on which the network address was most recently seen.
LASTCHANGE	Shows when the entry was created or last changed. If this value changes frequently, it can indicate duplicate address problems.

## Example

The following example displays the RMON address map table on the switch.

```
Switch:1(config)#show rmon address-map
=====
                        Rmon Address Map Table
=====
PROTOIDX  HOSTADDR          SOURCE  PHYADDR          LASTCHANGE
-----
1         192.0.2.11       3      b0:ad:aa:42:a5:03  05/04/21 08:20:13
```

## show rmon alarm

View Remote Network Monitoring (RMON) settings to see information about alarms entries on the switch.

## Syntax

- **show rmon alarm**

## Command Parameters

### alarm

Displays RMON alarm table on the switch.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show rmon alarm** command displays the following information:

Output field	Description
ID	Uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The default is 1
INTVAL	Specifies the interval, in seconds, over which the data is sampled and compared with the rising and falling thresholds. deltaValue sampling — Configures the interval short enough that the sampled variable is unlikely to increase or decrease by more than $2^{31}-1$ during a single sampling interval.

Output field	Description
VARIABLE	<p>Specifies the object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) can be sampled. Alarm variables exist in three formats, depending on the type:</p> <ul style="list-style-type: none"> <li>• A chassis, power supply, or fan-related alarm ends in x where the x index is hard-coded. No further information is required.</li> <li>• A card, spanning tree group (STG), or EtherStat alarm ends with a dot (.). You must enter a card number, STG ID, IP address, or EtherStat information.</li> <li>• A port alarm ends with no dot or index and requires that you use the port shortcut menu. An example of a port alarm is ifInOctets (interface incoming octet count).</li> </ul> <p>Because the system articulates SNMP access control entirely in terms of the contents of MIB views, no access control mechanism exists to restrict the value of this object to identify only those objects that exist in a particular MIB view. Because no acceptable means of restricting the read access that is obtained through the alarm mechanism exists, the probe must grant only write access to this object in those views that have read access to all objects on the probe.</p> <p>After you configure a variable, if the supplied variable name is not available in the selected MIB view, the system returns a badValue error. After the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe changes the status of this alarmEntry to invalid. You cannot modify this object if the associated alarmStatus object is equal to valid</p>
VALUE	<p>Specifies the value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value is the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value is the sampled value at the end of the period. This system compares the value with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and remains available until the next period is complete.</p>
SAMPLE TYPE	<p>Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue, the value of the system compares the selected variable directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue, the system subtracts the value of the selected variable at the last sample from the current value, and the system compares the difference with the thresholds. You cannot modify this object if the associated alarmStatus object is equal to valid. The default is deltaValue</p>
STARTUP ALARM	<p>Specifies the alarm that is sent after this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to the risingAlarm or the risingOrFallingAlarm, then the system generates a single rising alarm. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to the fallingAlarm or the risingOrFallingAlarm, then the system generates a single falling alarm. You cannot modify this object if the associated alarmStatus object is equal to valid.</p>

Output field	Description
RISING THRESHOLD	Specifies a threshold for the sampled statistic. After the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, the system generates a single event. The system also generates a single event if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm or risingOrFallingAlarm. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold. You cannot modify this object if the associated alarmStatus object is equal to valid.
EVENT INDEX	Specifies the index of the eventEntry that is used after a rising threshold and a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If no corresponding entry exists in the eventTable, no association exists. In particular, if this value is zero, the system generates no associated event, as zero is not a valid event index. You cannot modify this object if the associated alarmStatus object is equal to valid.  <b>Note:</b> You must create the event prior to associating it to an alarm.
FALLING THRESHOLD	Specifies a threshold for the sampled statistic. If the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, the system generates a single event. The system also generates a single event if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm or risingOrFallingAlarm. After the system generates a falling event, the system does not generate another similar event until the sampled value rises above this threshold and reaches the alarmRisingThreshold. You cannot modify this object if the associated alarmStatus object is equal to valid.
OWNER	Specifies the entity that configured this entry and is therefore using the resources assigned to it.

## Example

The following example displays the RMON alarm entries.

```
VSP-8284XSQ:1(config)#show rmon alarm
=====
                        Rmon Alarm
=====
ID      INTVAL  VARIABLE                               VALUE  SAMPLE
-----  -----  -----                               -----  -----
4       10      rcCliNumAccessViolations.0           0      absolute

STARTUP  RISING  EVENT  FALLING  EVENT
ALARM    THRESHOLD  INDEX  THRESHOLD  INDEX  OWNER
-----  -----  -----  -----  -----  -----
rising  2       60534  0        0      cli
```

---

## show rmon application-host-stats

---

View Remote Network Monitoring (RMON) application host statistics to see traffic statistics by application protocol for each host on the switch.

### Syntax

- **show rmon application-host-stats tcp**
- **show rmon application-host-stats udp**
- **show rmon application-host-stats ftp**
- **show rmon application-host-stats ssh**
- **show rmon application-host-stats telnet**
- **show rmon application-host-stats http**
- **show rmon application-host-stats rlogin**
- **show rmon application-host-stats tftp**
- **show rmon application-host-stats snmp**
- **show rmon application-host-stats https**

### Command Parameters

#### tcp

Display TCP application host statistics to manage network performance on the switch.

#### udp

Display UDP application host statistics to manage network performance on the switch.

#### ftp

Display FTP application host statistics to manage network performance on the switch.

#### ssh

Display SSH application host statistics to manage network performance on the switch.

#### telnet

Display TELNET application host statistics to manage network performance on the switch.

#### http

Display HTTP application host statistics to manage network performance on the switch.

#### rlogin

Display rlogin application host statistics to manage network performance on the switch.

#### tftp

Display TFTP application host statistics to manage network performance on the switch.

#### snmp

Display SNMP application host statistics to manage network performance on the switch.

#### https

Display HTTPS application host statistics to manage network performance on the switch.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

Protocols displayed by the **show rmon application-host-stats** command vary across hardware models..

## Command Output

The **show rmon application-host-stats** command displays the following information:

Output field	Description
HOSTADDR	Shows the network address for this entry. The format of the value depends on the protocol portion of the local index.
INPKT	Shows the number of packets for this protocol type, without errors, transmitted to this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
OUTPKT	Shows the number of packets for this protocol type, without errors, transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
INOC	Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
OUTOCT	Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
CREATETIME	Shows when the entry was last activated.

## Example

The following example displays application host statistics protocol on the switch.

```
Switch:1(config)# show rmon application-host-stats ftp
=====
                        Rmon Application Host Stats
=====
HOSTADDR    INPKT    OUTPKT    INOCT    OUTOCT    CREATETIME
-----
192.0.2.10  0        0         0        0         10/09/15 17:29:54
```

## show rmon ctl-table

View Remote Network Monitoring (RMON) control tables to see the data source for both network layer and application layer host statistics.

### Syntax

- **show rmon ctl-table**

### Command Parameters

#### ctl-table

Displays the Protocol Directory Table, Protocol Distribution Control Table, Address Map Control Table, and Host Control Table on the switch.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show rmon ctl-table** command displays the following information:

Output field	Description
IDX	Shows a unique identifier for the entry in the table.
PROTOCOL <b>Note:</b> Protocol support can vary across hardware models.	Shows the protocols RMON2 can monitor: <ul style="list-style-type: none"><li>• Internet Protocol (IP)</li><li>• Transmission Control Protocol (TCP)</li><li>• User Datagram Protocol (UDP)</li><li>• File Transfer Protocol (FTP)</li><li>• Secure Shell version 2 (SSHv2)</li><li>• Telnet</li><li>• Hypertext Transfer Protocol (HTTP)</li><li>• Remote login (rlogin)</li><li>• Trivial File Transfer Protocol (TFTP)</li><li>• Simple Networking Management Protocol (SNMP)</li><li>• Hypertext Transfer Protocol Secure (HTTPS)</li></ul>



Output field	Description
ADDRMAPCFG	<p>Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>NOT SUPPORTED</b></li> <li>• <b>SUPPORTED OFF</b></li> <li>• <b>SUPPORTED ON</b></li> </ul> <p>If the value is <b>SUPPORTED ON</b>, the probe adds entries to the address map table that maps the network layer address to the MAC layer address.</p>
HOSTCFG	<p>Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>NOT SUPPORTED</b></li> <li>• <b>SUPPORTED OFF</b></li> <li>• <b>SUPPORTED ON</b></li> </ul> <p>If the value is <b>SUPPORTED ON</b>, the probe adds entries to the Host Control table to collect statistics for network layer and application layer hosts.</p>
MATRIXCFG	<p>Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>NOT SUPPORTED</b></li> <li>• <b>SUPPORTED OFF</b></li> <li>• <b>SUPPORTED ON</b></li> </ul>
OWNER	Shows the entity that configured this entry.
DATASOURCE	Shows the source of data for the entry.
DROPPFRAMES	Shows the total number of frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors.
CREATETIME	Shows when the entry was last activated.
NHDROPPFRAMES	Shows the total number of network host frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors.
AHDROPPFRAMES	Shows the total number of application layer host frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors.

## Example

The following example displays the RMON control table entries.

```
Switch:1(config)#show rmon ctl-table
=====
                        Rmon Control Table
=====
                        Protocol Directory Table
=====
```

IDX	PROTOCOL	ADDRMAPCFG	HOSTCFG	MATRIXCFG	OWNER
1	IP	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
2	TCP	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
3	UDP	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
4	FTP	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
5	SSH	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
6	TELNET	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
7	HTTP	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
8	RLOGIN	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
9	TFTP	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
10	SNMP	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP
11	HTTPS	SUPPORTED	SUPPORTED	NOT SUPPORTED	VSP

#### Protocol Distribution Control Table

IDX	DATASOURCE	DROPFRAMES	CREATETIME	OWNER
1	0.0.0.0	0	04/22/21 05:00:41	VSP

#### Address Map Control Table

IDX	DATASOURCE	DROPFRAMES	OWNER
1	0.0.0.0	0	VSP

#### Host Control Table

IDX	DATASOURCE	NHDROPFRAMES	AHDROPFRAMES	OWNER
1	0.0.0.0	0	0	VSP

## show rmon event

View Remote Network Monitoring (RMON) event entries on the switch.

### Syntax

- **show rmon event**

### Command Parameters

#### event

Displays RMON event entries on the switch.

### Default

None

## Command Mode

User EXEC

## Command Output

The **show rmon event** command displays the following information:

Output field	Description
INDEX	Uniquely identifies an entry in the event table. Each entry defines one event that the system generates after the appropriate conditions occur. The default is 1.
DESCRIPTION	Specifies a comment that describes this event entry.
TYPE	Specifies the type of notification that the probe makes about this event. In the case of a log, the system makes an entry in the log table for each event. In the case of SNMP traps, the system sends an SNMP trap to one or more management stations.
COMMUNITY	Specifies the SNMP community where you can send SNMP traps.
LAST_TIME_SENT	Specifies the value of sysUpTime at the time this event entry last generated an event. If this entry has not generated events, this value is zero.
OWNER	Specifies the entity that configured this entry and is therefore using the assigned resources. If this object contains a string starting with monitor and has associated entries in the log table, all connected management stations retrieve those log entries, as they have significance to all management stations connected to this device.

## Example

The following example displays the RMON event entries.

```
Switch:1(config)# show rmon event
=====
                        Rmon Event
=====
INDEX   DESCRIPTION   TYPE           COMMUNITY  OWNER           LAST_TIME_SENT
-----
60534   Rising Event   log-and-trap   public     192.0.2.155     none
60535   Falling Event  log-and-trap   public     192.0.2.155     8 day(s),19:14:32
```

## show rmon history

View Remote Network Monitoring (RMON) history entries on the switch.

## Syntax

- **show rmon history**

## Command Parameters

### history

Displays RMON history entries on the switch.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show rmon history** command displays the following information:

Output field	Description
INDEX	Specifies an index that uniquely identifies an entry in the historyControl table. Each entry defines a set of samples at a particular interval for an interface on the device. Index value ranges from 1-65535. The default value is 1.
PORT	Identifies the source for which the system collects and places historical data in a media-specific table on behalf of this historyControlEntry. The source is an interface on this device. To identify a particular interface, the object identifies the instance of the ifIndex object, defined in (4,6), for the desired interface. For example, if an entry receives data from interface 1, the object is ifIndex 1. The statistics in this group reflect all packets on the local network segment attached to the identified interface. You cannot modify this object if the associated historyControlStatus object is equal to valid(1).
BUCKET_REQUEST	Specifies the requested number of discrete time intervals over which the system save data in the part of the media-specific table associated with this historyControlEntry. After this object is created or modified, the probe configures historyControlBucketsGranted as closely to this object as possible for the particular probe implementation and available resources. The value ranges from 1-65535. The default value is 50.

Output field	Description
BUCKET_GRANTED	Specifies the number of discrete sampling intervals over which the system save data in the part of the media-specific table associated with this historyControlEntry. After the associated BucketsRequested object is created or modified, the probe sets this object as closely to the requested value as possible for the particular probe implementation and available resources. The probe must not lower this value except as a result of a modification to the associated BucketsRequested object. Occasionally, the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, the system adds a new bucket to the media-specific table. After the number of buckets reaches the value of this object and the system is going to add a new bucket to the media-specific table, the agent deletes the oldest bucket associated with this entry so the system can added the new bucket. After the value of this object changes to a value less than the current value, entries are deleted from the media-specific table associated with this entry. The agent deletes the oldest of these entries so that their number remains less than or equal to the new value of this object. After the value of this object changes to a value greater than the current value, the system allows the number of associated media-specific entries to grow.
INTERVAL	Specifies the interval in seconds over which the system samples data for each bucket in the part of the media-specific table associated with this historyControlEntry. You can set this interval between 1-3600 seconds (1 hour). Because the counters in a bucket can overflow at their maximum value with no indication, you must take into account the possibility of overflow in all of the associated counters. Consider the minimum time in which a counter can overflow on a particular media type, and then set the historyControlInterval object to a value less than this interval, which is typically most important for the octets counter in a media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter can overflow in approximately 1 hour at the maximum utilization. You cannot modify this object if the associated historyControlStatus object is equal to valid. The default value is 1800.
OWNER	Specifies the entity that configured this entry and uses the assigned resources.

## Example

The following example displays the RMON history control entries.

```
Switch:1(config)#show rmon history
=====
                        Rmon Control-History
=====
INDEX  PORT      BUCKET_REQUEST  BUCKET_GRANTED  INTERVAL  OWNER
-----
2      1/2      50              50              200      Test
-----
```

## show rmon log

View Remote Network Monitoring (RMON) log entries.

### Syntax

- **show rmon log**

### Command Parameters

#### log

Displays RMON logs on the switch.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show rmon log** command displays the following information:

Output field	Description
INDEX	Specifies an index that uniquely identifies an entry in the log table generated by the same event entries.
EVENT INDEX	Specifies an index that uniquely identifies an entry in the event table. Each entry defines one event that is generated under appropriate conditions.
TIME	Specifies the creation time for this log entry.
DESCRIPTION	Specifies an implementation dependent description of the event that activated this log entry.

### Example

The following example displays the RMON log information.

```
Switch:1(config)#show rmon log
=====
                        Rmon Log
=====
INDEX  EVENT INDEX      TIME                               DESCRIPTION
-----
1      60535            8 day(s), 19:14:45                1.3.6.1.4.1.2272.1.19.14.0 (absValue = 0, Falling
                                Threshold = 2, interval = 10)[alarmIndex.1][trap]
                                "Falling Event"
2      60535            8 day(s), 19:14:45                1.3.6.1.4.1.2272.1.19.14.0 (absValue = 0, Falling
```

```
Threshold = 1, interval = 10) [alarmIndex.2] [trap]
"Falling Event"
```

## show rmon network-host-stats

View Remote Network Monitoring (RMON) network host statistics to see Layer 3 traffic statistics for each host. The network layer host MIB monitors traffic packets in and out of hosts based on the network layer address.

### Syntax

- **show rmon network-host-stats**

### Command Parameters

#### network-host-stats

Displays RMON network host statistics on the switch.

### Default

None

### Command Mode

User EXEC

### Command Output

The **show rmon network-host-stats** command displays the following information:

Output field	Description
HOSTADDR	Shows the host address for this entry.
INPKT	Shows the number of packets without errors transmitted to this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
OUTPKT	Shows the number of packets without errors transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
INOCT	Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.

Output field	Description
OUTOCT	Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
CREATETIME	Shows when the entry was last activated.

## Example

The following example displays the RMON network host statistics entries.

```
Switch:1(config)#show rmon network-host-stats
=====
                        Rmon Network Host Stats
=====
HOSTADDR      INPKT      OUTPKT      INOCT      OUTOCT      CREATETIME
-----
192.0.2.10    107699     105658     6462728    11464146    05/04/21 08:20:13
```

## show rmon protocol-dist-stats

View Remote Network Monitoring (RMON) protocol distribution statistics to see traffic statistics that each protocol generates by local area network (LAN) segment.

## Syntax

- **show rmon protocol-dist-stats**

## Command Parameters

### protocol-dist-stats

Displays RMON protocol distribution statistics on the switch.

## Default

None

## Command Mode

User EXEC



## Command Output

The **show rmon protocol-dist-stats** command displays the following information:

Output field	Description
PROTOCOL  <b>Note:</b> Protocol support can vary across hardware models.	Shows the protocols RMON2 can monitor: <ul style="list-style-type: none"> <li>• Internet Protocol (IP)</li> <li>• Secure Shell version 2 (SSHv2)</li> <li>• Transmission Control Protocol (TCP)</li> <li>• User Datagram Protocol (UDP)</li> <li>• File Transfer Protocol (FTP)</li> <li>• Hypertext Transfer Protocol (HTTP)</li> <li>• Telnet</li> <li>• Remote login (rlogin)</li> <li>• Trivial File Transfer Protocol (TFTP)</li> <li>• Simple Networking Management Protocol (SNMP)</li> <li>• Hypertext Transfer Protocol Secure (HTTPS)</li> </ul>
PKTS	Shows the number of packets without errors received for this protocol type. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
OCTETS	Shows the number of octets in packets received for this protocol type since it was added to the table. This value does not include octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.

## Example

The following example displays the RMON protocol distribution statistics on the switch.

```
Switch:1(config)# show rmon protocol-dist-stats
=====
                        Rmon Protocol Dist Stats
=====
PROTOCOL  PKTS      OCTETS
-----
IP         0         0
TCP        0         0
UDP        0         0
FTP        0         0
SSH        0         0
TELNET    0         0
HTTP      0         0
RLOGIN    0         0
TFTP      0         0
SNMP      0         0
HTTPS     0         0
```

## show rmon stats

View Remote Network Monitoring (RMON) statistics to manage network performance.

## Syntax

- **show rmon stats**

## Command Parameters

### stats

Displays RMON statistics information on the switch.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show rmon stats** command displays the following information:

Output field	Description
INDEX	An index that uniquely identifies an entry in the Ethernet statistics table.
PORT	Identifies the source of the data that this entry analyzes.
OWNER	The entity that configured this entry and is therefore using the assign resources.

## Example

The following example displays the current RMON status on the switch.

```
Switch:1#show rmon stats
=====
                        Rmon Ether Stats
=====
INDEX   PORT   OWNER
-----
1       1/10   monitor
```

## show route-map

Display current information about the IP route policy.

## Syntax

- **show route-map**
- **show route-map [WORD <1-64>] [seq <1-65535>] [vrf WORD<1-16>] [vrfids WORD<0-512>]**

- `show route-map detail`
- `show route-map detail [vrf WORD<1-16>] [vrfids WORD<0-512>]`
- `show route-map vrf WORD<1-16>`
- `show route-map vrfids WORD<0-512>`
- `show route-map WORD<1-64>`
- `show route-map WORD<1-64> seq <1-65535>`

## Command Parameters

### detail

Specifies the long format information of the route map.

### vrf WORD<1-16>

Specifies the name of the VRF.

### vrfids WORD<0-512>

Specifies the ID of the VRF and is an integer in the range of 0 to 512.

### WORD<1-64> seq <1-65535>

Displays a route policy with a policy name and a sequence number. WORD<1-64> is the policy name. seq <1-65535> is the sequence number.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show route-map** command displays the following information:

Output field	Description
NAME	Indicates the name of the route policy.
SEQ	Indicates the second index used to identify a specific policy within the route policy group (grouped by ID). Use this field to specify different match and set parameters and an action.
MODE	Indicates the action to take when this policy is selected for a specific route. Options are permit, deny, or continue. Permit indicates to allow the route. Deny indicates to ignore the route. Continue means continue checking the next match criteria configured in the next policy sequence; if none, take the default action in the given context.
EN	Indicates whether this policy is enabled. If disabled, the policy is not used.

## show sflow

---

Display sFlow configurations.

### Syntax

- **show sflow**

### Default

None

### Command Mode

User EXEC

## show sflow collector

---

Display sFlow collector information.

### Syntax

- **show sflow collector**
- **show sflow collector <1-2>**

### Command Parameters

<1-2>

Specifies which collector ID to display.

### Default

None

### Command Mode

User EXEC

## show sflow interface

---

Display sFlow interface configurations.

### Syntax

- **show sflow interface**
- **show sflow interface enabled**

- **show sflow interface {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

### enabled

Shows information for all sFlow-enabled interfaces.

**{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## show sflow statistics

---

Display sFlow statistics.

## Syntax

- **show sflow statistics**
- **show sflow statistics collector <1-2>**

## Command Parameters

**collector <1-2>**

Specifies the collector ID to display the statistics.

## Default

None

## Command Mode

User EXEC

## show slpp

---

Use Simple Loop Prevention Protocol (SLPP) information to view loop information.

## Syntax

- **show slpp**

## Default

None

## Command Mode

User EXEC

## show slpp interface

---

Show Simple Loop Prevention Protocol (SLPP) information for a port so that you can view the loop information for a port.

## Syntax

- **show slpp interface GigabitEthernet**
- **show slpp interface GigabitEthernet [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

**GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## show slpp-guard

---

View SLPP Guard configuration status for the switch or a specific list of ports.

## Syntax

- **show slpp-guard [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## show smlt

---

View all ports for a single port SMLT to ensure the correct ports are configured.

## Syntax

- **show smlt**
- **show smlt mlt**

## Command Parameters

mlt

Displays SMLT information for the MLT interface.

## Default

None

## Command Mode

User EXEC

## show smtp

---

Shows a list of active event IDs for which the switch generates email notification. The command output includes the default list of IDs and IDs you specifically add or remove.

## Syntax

- **show smtp event-id**

## Command Parameters

### event-id

Shows a list of active event IDs for which the switch generates email notification.

## Default

None

## Command Mode

User EXEC

---

## show snmplog

View the contents of the Simple Network Management Protocol (SNMP) log.

## Syntax

- **show snmplog**

## Default

None

## Command Mode

User EXEC

---

## show snmp-server

Display Simple Network Management Protocol (SNMP) system information to view trap and authentication profiles.

## Syntax

- **show snmp-server**
- **show snmp-server community**
- **show snmp-server context**
- **show snmp-server group**
- **show snmp-server host**
- **show snmp-server notify-filter**
- **show snmp-server user**
- **show snmp-server view**
- **show snmp-server view [viewname WORD<0-32>]**



## Command Parameters

**community**

Displays the SNMP community table.

**context**

Displays vacm context table.

**group**

Displays SNMP group access table.

**host**

Displays SNMP host details.

**notify-filter**

Displays SNMP notify-filter details.

**user**

Displays SNMP users.

**view**

Displays SNMP MIB view table.

**viewname WORD<0-32>**

Displays the view for a particular view name.

## Default

None

## Command Mode

User EXEC

## **show snmp-server host**

---

Display the Simple Network Management Protocol (SNMP) server configuration information.

## Syntax

- **show snmp-server host**

## Default

None

## Command Mode

User EXEC

## show snmp-server notify-filter

---

Display a new notify filter configuration information.

### Syntax

- **show snmp-server notify-filter**

### Default

None

### Command Mode

User EXEC

## show software

---

Display unpacked software releases information.

### Syntax

- **show software**
- **show software detail**
- **show software release WORD<1-99>**
- **show software slot**

### Command Parameters

#### detail

Displays software release in detail mode.

#### release <WORD 1-99>

Specifies a specific software release to be displayed in the range of 1 to 99.

#### slot

Specifies software version running on each slot. This parameter is not available on all hardware platforms.

#### verbose

Includes a date and time stamp to indicate when you last activated a software release. The output also indicates if you manually committed the software release, or if you used the automatic commit feature.

### Default

None

## Command Mode

User EXEC

## show spanning-tree bpduguard

---

Display BPDU Guard configuration

### Syntax

- **show spanning-tree bpduguard** [{slot/port[/sub-port] [-slot/port[/subport]][,...]]
- **show spanning-tree bpduguard** [GigabitEthernet {slot/port[/sub-port] [-slot/port[/subport]][,...]]

### Command Parameters

{slot/port[/sub-port] [-slot/port[/subport]][,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

## Command Mode

User EXEC

## show spanning-tree config

---

Query the change detection setting to show the port information.

### Syntax

- **show spanning-tree config**

### Default

None

## Command Mode

User EXEC

## show spanning-tree mstp config

---

View the Multiple Spanning Tree Protocol (MSTP) configurations to display the MSTP-related bridge-level VLAN and region information.

### Syntax

- **show spanning-tree mstp config**

### Default

None

### Command Mode

User EXEC

## show spanning-tree mstp msti config

---

Display the configuration for one or all Multiple Spanning Tree Protocol (MSTP) instance IDs.

### Syntax

- **show spanning-tree mstp msti config**
- **show spanning-tree mstp msti config <1-63>**

### Command Parameters

<1-63>

Specifies the MSTP instance ID.

### Default

None

### Command Mode

User EXEC

## show spanning-tree mstp msti port

---

Shows the configuration, role, or statistics information of an MSTP port.

## Syntax

- **show spanning-tree mstp msti port config**
- **show spanning-tree mstp msti port config** [{slot/port[/sub-port]}[-slot/port[/sub-port]][,...]]
- **show spanning-tree mstp msti port role**
- **show spanning-tree mstp msti port role** [{slot/port[/sub-port]}[-slot/port[/sub-port]][,...]]
- **show spanning-tree mstp msti port statistics**
- **show spanning-tree mstp msti port statistics** [{slot/port[/sub-port]}[-slot/port[/sub-port]][,...]]

## Command Parameters

**config** {slot/port[/sub-port]}[-slot/port[/sub-port]][,...]

Shows the configuration information of an MSTP port. {slot/port[/sub-port]}[-slot/port[/sub-port]][,...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**role** {slot/port[/sub-port]}[-slot/port[/sub-port]][,...]

Shows the role information of an MSTP port. {slot/port[/sub-port]}[-slot/port[/sub-port]][,...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**statistics** {slot/port[/sub-port]}[-slot/port[/sub-port]][,...]

Shows the statistics information of an MSTP port. {slot/port[/sub-port]}[-slot/port[/sub-port]][,...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## show spanning-tree mstp port config

Show mstp port configurations.

## Syntax

- **show spanning-tree mstp port config {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Displays the MSTP port information. {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

---

## show spanning-tree mstp port role

Display Multiple Spanning Tree Protocol (MSTP) port information.

## Syntax

- **show spanning-tree mstp port role {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Displays the MSTP port configurations, which display MSTP-related bridge-level VLAN and region information.

## Default

None

## Command Mode

User EXEC

## show spanning-tree mstp port statistics

---

Display Multiple Spanning Tree Protocol (MSTP) Multiple Spanning Tree Instance (MSTI) information to ensure the feature is configured correctly for your network.

### Syntax

- **show spanning-tree mstp port statistics**
- **show spanning-tree mstp port statistics {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Displays the MSTP port information to display the MSTP, CIST port, and MSTI port information maintained by every port of the common spanning tree. {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

User EXEC

## show spanning-tree mstp statistics

---

Display Multiple Spanning Tree Protocol (MSTP) statistics to see MSTP related bridge-level statistics.

### Syntax

- **show spanning-tree mstp statistics**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show spanning-tree mstp statistics** command displays the following information:

Output field	Description
MSTP Up Count	The number of times the MSTP port has been enabled. A Trap is generated on the occurrence of this event.
MSTP Down Count	The number of times the MSTP port has been disabled. A Trap is generated on the occurrence of this event.
Region Config Change Count	The number of times the switch detects a Region Configuration Identifier Change. The switch generates a trap on the occurrence of this event.
Time since topology change	The time (in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for Common Spanning Tree context.
Topology change count	The count of at least one non zero TcWhile timers on this Bridge for Common Spanning Tree context.
New Root Bridge Count	The number of times this Bridge has detected a Root Bridge change for Common Spanning Tree context. A Trap is generated on the occurrence of this event.

## show spanning-tree mstp status

View the Multiple Spanning Tree Protocol (MSTP) status to display the MSTP- related status information known by the selected bridge.

### Syntax

- **show spanning-tree mstp status**

### Default

None

### Command Mode

User EXEC

## show spanning-tree rstp config

View the global Rapid Spanning Tree Protocol (RSTP) configuration information to display the RSTP configuration details.



## Syntax

- **show spanning-tree rstp config**

## Default

None

## Command Mode

User EXEC

---

## show spanning-tree rstp port config

Configure Ethernet Rapid Spanning Tree Protocol (RSTP) parameters to set RSTP parameters for the port.

## Syntax

- **show spanning-tree rstp port config**
- **show spanning-tree rstp port config [{slot/port[/sub-port]}[-slot/port[/sub-port]][,...}}**

## Command Parameters

{slot/port[/sub-port]}[-slot/port[/sub-port]][,...]}

Shows RSTP port configuration. {slot/port[/sub-port]}[-slot/port[/sub-port]][,...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

---

## show spanning-tree rstp port role

View the Rapid Spanning Tree Protocol (RSTP) role to display the RSTP information.

## Syntax

- **show spanning-tree rstp port role**

- **show spanning-tree rstp port role** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Shows the RSTP port role. {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## show spanning-tree rstp port statistics

---

View the Rapid Spanning Tree Protocol (RSTP) information for a selected port to display the RSTP related configuration information for the selected port.

## Syntax

- **show spanning-tree rstp port statistics**
- **show spanning-tree rstp port statistics** [{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

## Command Parameters

{slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}

Shows RSTP port statistics. {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]} identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show spanning-tree rstp port statistics** command displays the following information:

Output field	Description
RxRstBpduCount	The number of RSTP BPDUs received on this port.
RxConfigBpduCount	The number of configuration BPDUs received on this port.
RxTcnBpduCount	The number of TCN BPDUs received on this port.
TxRstBpduCount	The number of RSTP BPDUs transmitted by this port.
TxConfigBpduCount	The number of Config BPDUs transmitted by this port.
TxTcnBpduCount	The number of TCN BPDUs transmitted by this port.
InvalidRstBpduRxCount	The number of invalid RSTP BPDUs received on this port. A trap is generated on the occurrence of this event.
InvalidConfigBpduRx Count	The number of invalid configuration BPDUs received on this port. A trap is generated on the occurrence of this event.
InvalidTcnBpduRxCount	The number of invalid TCN BPDUs received on this port. A trap is generated on the occurrence of this event.
ProtocolMigrationCount	The number of times this port migrated from one STP protocol version to another. The relevant protocols are STP-Compatible and RSTP. A trap is generated on the occurrence of this event.

## show spanning-tree rstp port status

View the Rapid Spanning Tree Protocol (RSTP) status for a port to display the RSTP related status information for a selected port.

### Syntax

- **show spanning-tree rstp port status**
- **show spanning-tree rstp port status** [{slot/port[/sub-port]} [-slot/port[/sub-port]] [, ... ]}

### Command Parameters

{slot/port[/sub-port]} [-slot/port[/sub-port]] [, ... ]

Identifies the slot and port. {slot/port[/sub-port]} [-slot/port[/sub-port]] [, ... ] identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your

platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## show spanning-tree rstp statistics

View Rapid Spanning Tree Protocol (RSTP) statistics to manage network performance.

## Syntax

- **show spanning-tree rstp statistics**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show spanning-tree rstp statistics** command displays the following information:

Output field	Description
RSTP Up Count	The number of times RSTP port has been enabled. A Trap is generated on the occurrence of this event.
RSTP Down Count	The number of times RSTP port has been disabled. A Trap is generated on the occurrence of this event.
Count of Root Bridge Changes	The number of times this Bridge has detected a Root Bridge change for Common Spanning Tree context.
STP Time since Topology change	The time (in hundredths of a second) since the "TcWhile" Timer for any port in this Bridge was non zero for this spanning tree instance.
Total number of topology changes	The number of times that there have been atleast one non zero "TcWhile" Timer on this Bridge for this spanning tree instance.

## show spanning-tree rstp status

---

View the Rapid Spanning Tree Protocol (RSTP) status to display the RSTP related status information for the selected bridge.

### Syntax

- **show spanning-tree rstp status**

### Default

None

### Command Mode

User EXEC

## show spanning-tree status

---

View spanning-tree status information.

### Syntax

- **show spanning-tree status**

### Default

None

### Command Mode

User EXEC

## show spanning-tree tc-receive-alarm-threshold

---

Displays the tc-receive-alarm-threshold configuration.

### Syntax

- **show spanning-tree tc-receive-alarm-threshold**

### Default

None

## Command Mode

User EXEC

## show spbm

---

Display the status (enabled or disabled) and the ethertype for Shortest Path Bridging MAC (SPBM).

## Syntax

- **show spbm**

## Default

None

## Command Mode

User EXEC

## show spbm nick-name server leases

---

Shows the Shortest Path Bridging Media Access Control (SPBM) nick-name server leases information.

## Syntax

- **show spbm nick-name server leases**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show spbm nick-name server leases** command displays the following information:

Output field	Description
SYSTEM-ID	Indicates the system ID.
NICK-NAME	Indicates the nickname for the SPBM node.
HOST-NAME	Indicates the hostname.

## Example

The following example displays the SPBM nick-name server leases information on the switch.

```
Switch:1> show spbm nick-name server leases
=====
                        SPBM NICK-NAME SERVER LEASES
=====
SYSTEM-ID      NICK-NAME  HOST-NAME
-----
4088.2fe3.f484 a.10.0a   UNKNOWN
949b.2cb3.a484 a.10.0b   UNKNOWN
949b.2cad.4884 a.10.0c   UNKNOWN
949b.2cae.7c84 a.10.0d   VSP-7254XSQ
5c0e.8bff.5884 a.10.0e   UNKNOWN
0004.96f1.8084 a.10.0f   UNKNOWN
=====
```

## show ssh

Verify that Secure Shell (SSH) services are enabled on the switch and display SSH configuration information to ensure that the SSH parameters are properly configured.

### Syntax

- **show ssh <global|session>**
- **show ssh global**
- **show ssh session**

### Command Parameters

#### global

Displays global system SSH information.

#### session

Displays the current session SSH information.

### Default

None

### Command Mode

User EXEC

## show ssh rekey

Displays the SSH rekey configuration information on the switch.

### Syntax

- **show ssh rekey**

## Command Parameters

### info

Shows information about key exchange between server and client.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show ssh rekey** command displays the following information:

Output field	Description
Rekey status	Displays the status (TRUE or FALSE) of SSH rekeying.
Rekey data limit	Displays the configured SSH rekey data transmission limit in GB.
Rekey time interval	Displays the configured SSH rekey time interval in hours.

## Example

The following example displays the SSH rekey configuration.

```
Switch:1> enable
Switch:1#show ssh rekey
  Rekey Status      : TRUE
  Rekey data limit  : 1 GB
  Rekey time interval : 1 hours
```

## show sys control

Shows system control settings.

## Syntax

- **show sys control**

## Default

None

## Command Mode

User EXEC



## Usage Guidelines

The `tcp-keepalive-time`, `tcp-keepalive-interval`, `tcp-keepalive-probes`, and `mac-move-protection` fields are not supported on VSP 8600 Series.

## Command Output

The **show sys control** command displays the following information:

Output field	Description
<code>tcp-timestamp</code>	Displays if the timestamp is enabled or disabled.
<code>tcp-keepalive-time</code>	Displays the value of the TCP keepalive time in seconds.
<code>tcp-keepalive-interval</code>	Displays the value of the TCP keepalive interval, in seconds.
<code>tcp-keepalive-probes</code>	Displays the value for the TCP keepalive probes.
<code>mac-move-protection</code>	Displays if MAC move protection is enabled or disabled for the Virtual-IST (vIST).

## Example

The following example displays output from the **show sys control** command.

```
Switch:1>show sys control
=====
                        System Control Settings
=====
      tcp-timestamp : disable
      tcp-keepalive-time : 120
      tcp-keepalive-interval : 60
      tcp-keepalive-probes : 15
      mac-move-protection : on
```

## show sys default-ping-context

Display the default context in which you execute ping commands and traceroute commands.

## Syntax

- **show sys default-ping-context**

## Command Mode

User EXEC

## Usage Guidelines

This command is not supported on VSP 8600 Series.

## Command Output

The **show sys default-ping-context** command displays the following information:

Output field	Description
Default ping context	Displays the default context value for <b>ping</b> commands and <b>traceroute</b> commands.

## Example

The following example displays output for the **show sys default-ping-context** command.

```
Switch:1>show sys default-ping-context

      Default ping context grt
```

## show sys dns

Shows system DNS information.

The **show ip dns** command returns the same output.

## Syntax

- **show sys dns**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show sys dns** command displays the following information:

Output field	Description
DNS Default Domain Name	Displays the domain name.
DNS Default Domain Name Origin	Displays the origin of the domain name.
DNS Host Name	Displays the host name.
IP address	Displays the IP address of the primary, secondary, or tertiary server.
Status	Displays the status of the primary, secondary, or tertiary server.

Output field	Description
Total DNS Number of request made to this server	Displays the number of requests sent to the primary, secondary, or tertiary server.
Number of Successful DNS	Displays the number of successful requests sent to the primary, secondary, or tertiary server.

## Example

The following example displays output from the **show sys dns** command.

```
Switch:1>show sys dns
DNS Default Domain Name : test.company.com
DNS Default Domain Name Origin: DHCP
DNS Host Name: voss10cdae6bd000
Primary dynamic DNS server details:
=====
      IP address : 192.0.2.11
      Status      : active
      Total DNS Number of request made to this server : 0
      Number of Successful DNS : 0

Secondary dynamic DNS server details:
=====
      IP address : 192.0.2.12
      Status      : active
      Total DNS Number of request made to this server : 0
      Number of Successful DNS : 0

Tertiary dynamic DNS server details:
=====
      IP address : 192.0.2.13
      Status      : active
      Total DNS Number of request made to this server : 0
      Number of Successful DNS : 0
```

## show sys force-msg

Shows the message control force message pattern settings.

### Syntax

- **show sys force-msg**

### Default

None

### Command Mode

User EXEC

## show sys locator-led

---

Display the switch Locator LED status.

### Syntax

- **show sys locator-led**

### Default

None

### Command Mode

User EXEC

The following example displays the Locator LED in an enabled state.

```
Switch:1>show sys locator-led
Locator LED status: ON
```

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## show sys mgid-usage

---

Shows the multicast group ID (MGID) usage for VLANs, SPBM, and multicast traffic.

### Syntax

- **show sys mgid-usage**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show sys mgid-usag** command displays the following information:

Output field	Description
Number of MGIDs used for VLANs, multicast, or SPBM	Displays the number of MGIDs used for the feature.
Number of MGIDs remaining for VLANs, multicast, or SPBM	Displays the number of MGIDs still available for the feature.

## Example

The following example displays output from the **show sys mgid-usage** command.

```
Switch:1#show sys mgid-usag
  Number of MGIDs used for VLANs : (6)
  Number of MGIDs used for multicast : (0)
  Number of MGIDs used for SPBM : (0)
  Number of MGIDs remaining for VLANs : (4089)
  Number of MGIDs remaining for multicast : (6976)
  Number of MGIDs remaining for SPBM : (1024)
```

## show sys msg-control

Shows the system message control function status (activated or disabled).

## Syntax

- **show sys msg-control**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show sys msg-control** command displays the following information:

Output field	Description
action	Displays the configured message control action.
control-interval	Displays the message control interval, in minutes.

Output field	Description
max-msg-num	Displays the number of occurrences of a message after which the control action occurs.
status	Displays if the feature is enabled.

## Example

The following example displays output from the **show sys msg-control** command.

```
Switch:1#show sys msg-control

Message Control Info :
  action                : suppress-msg
  control-interval      : 5
  max-msg-num           : 5
  status                 : disable
```

## show sys mtu

Shows system maximum transmission unit (MTU) information.

### Syntax

- **show sys mtu**

### Default

None

### Command Mode

User EXEC

## show sys power

View power information for the chassis.

### Syntax

- **show sys power**
- **show sys power global**
- **show sys power power-supply**
- **show sys power slot**

### Command Parameters

global

Shows a summary of the power redundancy settings.

#### power-supply

Shows detailed power information for each power supply.

#### slot

Shows detailed power information for the slot.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The `global` parameter is only supported on VSP 8600 Series.

## Command Output

The **show sys power** command displays the following information:

Output field	Description
Chassis Power Status	Displays if the chassis contains redundant power.
Chassis Type	Displays the type of chassis.
Total Chassis Power	Displays the power currently used by the complete chassis.
Required Redundant Power	Displays the redundant power for the chassis.
Max Allocated Power	Displays the maximum power.
Reserved Power	Displays the reserved power.
Required Power	Displays the required power.
Slot # (1 through SF3)	Displays the priority of the slot for power management.
Power Supply	Displays the power supply slot.
Type	Displays the type of power used.
Input Voltage	Displays the input line voltage.
Serial Num	Displays the power supply serial number.
Part Num	Displays the power supply part number.
Oper Status	Displays the status as on (up) or off (down).
Max Power	Displays the maximum power of the power supply.
Hardware Revision	Displays the hardware revision number.
Slot No.	Displays the slot number.

Output field	Description
Present	Displays if the slot is populated.
CardType	Displays the type of module in the slot.
Priority	Displays the priority of the slot for power management.
Power Status	Displays the status as on or off.
Allocated Power	Displays the power for the slot.

## Examples

The following example displays summary power information.

```
Switch:1#show sys power

=====
                        Chassis Power Information
=====

Chassis Power Status: redundant

Chassis      Total      Required  Max
Type         Chassis  Redundant  Power
Power       Power    Power     Power
-----
SwitchXYZ   4200     1400      1851
            2349     1411      1851
=====
```

The following examples displays a summary of the power redundancy settings.

```
Switch:1#show sys power global
slot 1      : critical
slot 2      : critical
slot 3      : high
slot 4      : high
slot 5      : high
slot 6      : high
slot 7      : high
slot 8      : high
slot SF1    : critical
slot SF2    : critical
slot SF3    : critical
```

The following example displays detailed power information for each power supply.

```
Switch:1#show sys power power-supply

=====
                        Power Supply Information
=====

Power  Type   Input   Serial          Part           Oper   Max   Hardware
Supply  Type   Voltage Serial Num      Num           Status Power Revision
-----
PS#2   AC      110/220 GWXD1349000116- DPS-800RB      up     800
=====
```



The following example displays power information by slot.

```
Switch:1#show sys power slot
=====
                          Slot Power Consumption
=====
Slot      Present CardType          Max
No.       Status Power                    Power
-----
1         YES      8242XSQ          ON    208
2         YES      8242XSQ          ON    208
-----

                          Chassis Power Information
=====

Chassis Power Status: non-redundant

Chassis   Total   Required
Type      Chassis Redundant
          Power   Power
-----
8284XSQ   0       0
-----
```

## show sys priv-exec-password

Verify authentication for Privileged EXEC CLI command mode.

### Syntax

- **show sys priv-exec-password**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show sys priv-exec-password** command displays the following information:

Output field	Description
Privileged exec password status	Displays if authentication for Privileged EXEC CLI command mode access is enabled.

## Example

The following example displays an authentication request when privileged-exec mode is enabled.

```
Switch:1>show sys priv-exec-password
      Privileged exec password status : enabled
```

## show sys setting

Shows system settings.

## Syntax

- **show sys setting**

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The *default-ping-context* field is not supported on VSP 8600 Series.

## Command Output

The **show sys setting** command displays the following information:

Output field	Description
udp-checksum	Displays if the User Datagram Protocol (UDP) checksum calculation is enabled.
mroute-stream-limit	Displays if Mroute stream limit is enabled.
contact	Displays the system contact.
location	Displays the system location.
name	Displays the system name.
portlock	Displays if port lock is enabled.
sendAuthenticationTrap	Displays if the system sends the authentication success trap.
autotopology	Displays if SynOptics Network Management Protocol (SONMP) is enabled.
mtu	Displays the system maximum transmission unit (MTU).
prototype	Displays if prototype is enabled.
data-path-fault-shutdown	Displays if data path fault shutdown is enabled.

Output field	Description
secure-console	Displays if secure console access is enabled.
default-ping-context	Displays the default context in which you run <b>ping</b> and <b>traceroute</b> commands.

## Example

The following example displays output from the **show sys setting** command.

```
Switch:1#show sys setting

      udp-checksum : enable
mroute-stream-limit : disable
      contact : http://www.company.com/
      location : Anywhere, USA
          name : Switch
      portlock : off
sendAuthenticationTrap : false
      autotopology : on
          mtu : 1950
          prototype : disable
data-path-fault-shutdown : enable
      secure-console : disable
      default-ping-context : grt
```

## show sys software

Verify that the image and configuration are loaded properly.

### Syntax

- **show sys software**

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

rlogin is only supported on VSP 8600 Series.

## Command Output

The **show sys software** command displays the following information:

Output field	Description
Default Runtime Config File	Displays the default Run-time configuration file directory name.
Config File	Displays the name of a new configuration file.
Last Runtime Config Save	Displays the last run-time configuration saved.
Version	Displays the software version information.
PrimaryConfigSource	Displays the primary boot configuration file.
SecondaryConfigSource	Displays the secondary boot configuration file.
EnableFactoryDefaults	Displays if the switch will bypass the loading of the switch configuration file and load the factory defaults.
EnableDebugMode	Displays if the switch debugs the configuration file during loading configuration at system boot.
EnableRebootOnError	Displays if the switch automatically reboots on a fatal error.
EnableTelnetServer	Displays if the Telnet server is enabled.
EnableRloginServer	Displays if the Rlogin server is enabled.
EnableFtpServer	Displays if the FTP server is enabled.
EnableTftpServer	Displays if the TFTP server is enabled.

## Example

The following example displays output from the **show sys software** command.

```
Switch:1#show sys software

System Software Info :

Default Runtime Config File : /intflash/config.cfg
Config File :
Last Runtime Config Save : 0

Boot Config Table
Version : Build 4.1.0.0 (GA) on Fri May 30 18:04:13 EDT 2014
PrimaryConfigSource : /intflash/config.cfg
SecondaryConfigSource : /intflash/config.cfg
EnableFactoryDefaults : false
EnableDebugMode : false
EnableRebootOnError : true
EnableTelnetServer : true
EnableRloginServer : false
EnableFtpServer : true
EnableTftpServer : false
```

## show sys stats

Shows system statistics.

## Syntax

- **show sys stats**

## Default

None

## Command Mode

User EXEC

## show sys stats ipmc-threshold-exceeded-cnt

---

Display IP multicast exceeded threshold counters.

## Syntax

- **show sys stats ipmc-threshold-exceeded-cnt**

## Default

None

## Command Mode

User EXEC

## show sys topology-ip

---

Shows the circuitless IP set.

## Syntax

- **show sys topology-ip**

## Default

None

## Command Mode

User EXEC

## show sys vim-speed

---

Shows the speed of all ports of a VIM.

## Syntax

- **show sys vim-speed**

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Command Output

The **show sys vim-speed** command displays the following information:

Output field	Description
Card Type	Specifies the name of the VIM.
Admin Speed	Specifies the configured speed for all ports in this VIM.

## Example

The following example displays a VIM5-2Y with all ports configured at 10 Gbps.

```
Switch:1>show sys vim-speed

=====
                        VIM Speed Configuration
=====
                CardType : VIM5-2Y
                Admin Speed : 10000
```

## show sys-info

Display the system status and technical information on the hardware components of the switch.

## Syntax

- **show sys-info**
- **show sys-info card**
- **show sys-info cpld**
- **show sys-info fan**

- **show sys-info led**
- **show sys-info power**
- **show sys-info ssd**
- **show sys-info temperature**
- **show sys-info uboot**
- **show sys-info usb**

## Command Parameters

### card

Specifies information about all the installed modules, including cooling modules (fans).

### cpld

Specifies information about field programmable gate arrays (FPGA) and complex programmable logic devices (CPLD).

### fan

Specifies information about installed cooling modules (fans).

### led

Specifies system LED status.

### power

Specifies information about installed power supplies.

### ssd

Specifies information about installed modular Solid State Drives (SSD).

### temperature

Specifies information about system temperature measured in degrees Celsius.

### uboot

Specifies information about the uboot image.

### usb

Specifies information about cached USB information.

## Default

None

## Command Mode

User EXEC

## Usage Guidelines

The parameters for this command do not apply to all hardware platforms. For more information about feature support, see [VOSS User Guide](#).

## show syslog

---

View the syslog information to ensure accuracy.

### Syntax

- **show syslog**

### Default

None

### Command Mode

User EXEC

## show syslog host

---

View the syslog host information to ensure accuracy.

### Syntax

- **show syslog host <1-10>**

### Command Parameters

<1-10>

Specifies the syslog host ID.

### Default

None

### Command Mode

User EXEC

## show tacacs

---

show TACACS information.

### Syntax

- **show tacacs**



## Default

None

## Command Mode

User EXEC

## Command Output

The **show tacacs** command displays the following information:

Output field	Description
Global Status	
global enable	Displays if the TACACS+ feature is enabled globally.
authentication enabled for	Displays which application is authenticated by TACACS+. The possibilities are CLI, web, or all.
accounting enabled for	Displays if accounting is enabled. You can only enable accounting for CLI. By default, accounting is not enabled.
authorization	Displays if authorization is enabled.
User privilege levels set for command authorization	<p>Displays the privilege levels set for command authorization. When you configure command authorization for a particular level, all commands that you execute are sent to the TACACS+ server for authorization. The device can only execute the commands the TACACS+ server authorizes.</p> <p>The user privilege levels are:</p> <ul style="list-style-type: none"> <li>• 0: denied access</li> <li>• 1: read only (ro) access</li> <li>• 2: Layer 1 read and write (l1) access</li> <li>• 3: Layer 2 read and write (l2) access</li> <li>• 4: Layer 3 read and write (l3) access</li> <li>• 5: read and write (rw) access</li> <li>• 6: read and write all (rwa) access</li> <li>• 7-14: denied access</li> <li>• 15: read and write all (rwa) access</li> </ul>
Server	
Prio	Displays the priority of the TACACS+ server. The switch attempts to use the primary server first, and the secondary server second.
Status	Displays the connection status between the server and the switch – connected or not connected.
Key	Displays as ***** instead of the actual key. The key is secret and is not visible.
Port	Displays the TCP port used to establish the connection to the server. The default port is 49.
IP address	Displays the IP address for the primary and secondary TACACS+ servers.

Output field	Description
Timeout	Displays the period of time, in seconds, the switch waits for a response from the TACACS+ daemon before it times out and declares an error. The default is 10 seconds.
Single	Displays if a single open connection is maintained between the switch and TACACS+ daemon, or if the switch opens and closes the TCP connection to the TACACS+ daemon each time they communicate. The default is false, which means the device does not maintain the single open connection.
Source <b>Note:</b> Exception: only supported on VSP 8600 Series.	Displays the fixed source IP address, if you configure one, for all outgoing TACACS+ packets.
SourceEnabled <b>Note:</b> Exception: only supported on VSP 8600 Series.	Displays if the fixed source IP address is enabled for all outgoing TACACS+ packets.

## show tech

Display technical information about the status of the system and complete information about the hardware components, software components, and operation of the system.

The information available from the **show tech** command includes general information about the system (such as location), hardware (chassis, power supplies, fans, and ports), system errors, boot configuration, software versions, memory, port information (locking status, configurations, names, interface status), VLANs and STGs (numbers, port members), Virtual Router Redundancy Protocol (VRRP), and log and trace files. This command displays more information than the similar **show sys-info** command.

### Syntax

- **show tech**

### Default

None

### Command Mode

User EXEC

---

## show telnet-access

---

Show the maximum number of Telnet sessions.

### Syntax

- **show telnet-access**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show telnet-access** command displays the following information:

Output field	Description
max ipv4 sessions	Displays the maximum number of permitted IPv4 Telnet sessions.
max ipv6 sessions	Displays the maximum number of permitted IPv6 Telnet sessions.

### Example

The following example shows output from the **show telnet-access** command.

```
Switch:1#show telnet-access
  max ipv4 sessions : 8
  max ipv6 sessions : 8
```

---

## show trace cfm

---

Shows the configuration status for CFM trace.

### Syntax

- **show trace cfm**

### Default

None

## Command Mode

User EXEC

## show trace file

---

View the trace results.

### Syntax

- **show trace file**
- **show trace file tail**

### Command Parameters

**tail**

Show file from tail

### Default

None

## Command Mode

User EXEC

## show trace level

---

Show the current trace level for all modules.

### Syntax

- **show trace level**

### Default

None

## Command Mode

User EXEC

## show trace modid-list

---

Show the relationship between level number and module ID to use with the trace tool.

## Syntax

- **show trace modid-list**

## Default

None

## Command Mode

User EXEC

## show trace spbm isis

---

View trace results.

## Syntax

- **show trace spbm isis**

## Default

None

## Command Mode

User EXEC

## show trace sub-system

---

Show trace sub-system name.

## Syntax

- **show trace sub-system**

## Default

None

## Command Mode

User EXEC

## show unsupported-lastset

---

Display the last set of masked commands in the release.

## Syntax

- **show unsupported-lastset**

## Default

None

## Command Mode

User EXEC

---

## show users

Display a list of users who are logged on to the system.

## Syntax

- **show users**

## Default

None

## Command Mode

User EXEC

## Command Output

The **show users** command displays the following information:

Output field	Description
SESSION	Displays the connection method.
USER	Displays the username.
ACCESS	Displays the user access level.
IP ADDRESS	Displays the user IP address.

The following example displays the connected users.

```
Switch:1#show users
SESSION  USER          ACCESS  IP ADDRESS
Telnet0  rwa            rwa     192.0.2.24 (current)
Console  none          none     -----
```

---

## show virtual-ist

---

Show virtual IST information.

### Syntax

- **show virtual-ist**

### Default

None

### Command Mode

User EXEC

---

## show virtual-ist stat

---

Display stat for virtual ist.

### Syntax

- **show virtual-ist stat**

### Default

None

### Command Mode

User EXEC

### Command Output

The **show virtual-ist stat** command displays the following information:

Output field	Description
Ist Down	The count of how many sessions between the two peering switches went down since last boot.
Hello Sent	The count of transmitted hello messages.
Hello Recv	The count of received hello messages.
Learn MAC Address Sent	The count of transmitted learned MAC address messages.
Learn MAC Address Recv	The count of received learned MAC address messages.

Output field	Description
MAC Address AgeOut Sent	The count of transmitted aging out MAC address messages.
MAC Address AgeOut Recv	The count of received aging out MAC address messages.
MAC Address Expired Sent	The count of transmitted MAC address age expired messages.
MAC Address Expired Recv	The count of received MAC address age expired messages.
Delete Mac Address Sent	The count of transmitted MAC address deleted messages.
Delete Mac Address Recv	The count of received MAC address deleted messages.
Smlt Down Sent	The count of transmitted SMLT down messages.
Smlt Down Recv	The count of received SMLT down messages.
Smlt Up Sent	The count of transmitted SMLT up messages.
Smlt Up Recv	The count of received SMLT up messages.
Send MAC Address Sent	The count of transmitted send MAC table messages.
Send MAC Address Recv	The count of received send MAC table messages.
IGMP Sent	The count of transmitted IGMP messages.
IGMP Recv	The count of received IGMP messages.
Port Down Sent	The count of transmitted port down messages.
Port Down Recv	The count of received port down messages.
Request MAC Table Sent	The count of transmitted MAC table request messages.
Request MAC Table Recv	The count of received MAC table request messages.
Unknown Msg Type Recv	The count of received unknown message type messages.
Mlt Table Sync Req Sent	The count of transmitted MLT table sync request messages.
Mlt Table Sync Req Recv	The count of received MLT table sync request messages.
Mlt Table Sync Sent	The count of transmitted MLT table sync messages.
Mlt Table Sync Recv	The count of received MLT table sync messages.
Port Update Sent	The count of transmitted port update messages.
Port Update Recv	The count of received port update messages.
Entry Update Sent	The count of transmitted entry update messages.
Entry Update Recv	The count of received entry update messages.



Output field	Description
Dialect Negotiate Sent	The count of transmitted protocol ID messages.
Dialect Negotiate Recv	The count of received protocol ID messages.
Update Response Sent	The count of transmitted update response messages.
Update Response Recv	The count of received update response messages.
Transaction Que HiWaterM	The count of transaction queue high watermark messages.
Poll Count Hi Water Mark	The count of poll count high watermark messages.

## show virtual-service

Displays virtual service information

### Syntax

- **show virtual-service config WORD<1-80>**
- **show virtual-service install WORD<1-80>**
- **show virtual-service statistics WORD<1-80>**

### Command Parameters

**config WORD<1-80>**

Displays the virtual-service configuration.

**install WORD<1-80>**

Displays installation status for a virtual service.

**statistics WORD<1-80>**

Displays statistics for virtual services configured on the switch.

### Default

None

### Command Mode

User EXEC

### Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## show vlacp

---

Display Virtual Link Aggregation Control Protocol (VLACP) global information.

### Syntax

- **show vlacp**

### Default

None

### Command Mode

User EXEC

---

## show vlacp interface

---

Display Virtual Link Aggregation Control Protocol (VLACP) global information.

### Syntax

- **show vlacp interface**
- **show vlacp interface gigabitethernet**
- **show vlacp interface gigabitethernet [vid <1-4059>]**
- **show vlacp interface gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

**gigabitethernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**vid <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

## Command Mode

User EXEC

## show vlan advance

---

View the advanced parameters to display the advanced parameters for the specified VLAN or for all VLANs.

### Syntax

- **show vlan advance**
- **show vlan advance <1-4059>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

## Command Mode

User EXEC

## show vlan autolearn-mac

---

View autolearned MAC addresses.

### Syntax

- **show vlan autolearn-mac**

### Default

None

## Command Mode

User EXEC

## show vlan basic

---

View the VLAN information to display the basic configuration for all VLANs or a specified VLAN.

### Syntax

- **show vlan basic**
- **show vlan basic <1-4059>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

User EXEC

## show vlan brouter-port

---

View the brouter port information to display the brouter port VLAN information for all VLANs on the switch or for the specified VLAN.

### Syntax

- **show vlan brouter-port**

### Default

None

### Command Mode

User EXEC

## show vlan i-sid

---

Show the customer VLAN (C-VLAN) to instance service identifier (I-SID) associations.

## Syntax

- **show vlan i-sid**
- **show vlan i-sid <1-4059>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show vlan i-sid** command displays the following information:

Output field	Description
VLAN_ID	Specifies the VLAN IDs.
I-SID	Specifies the I-SIDs associated with the specified C-VLANs.
I-SID NAME	Specifies the name of the I-SID. By default, for an I-SID in use, the service is named ISID-x, where x correlates to the I-SID number of the service.

## Example

The following example shows the output for this command.

```
Switch:1>show vlan i-sid
=====
                Vlan I-SID
=====
VLAN_ID      I-SID      I-SID NAME
-----
1
10           100        Hospital-Server-10
90           1000       ISID-1000

3 out of 3 Total Num of Vlans displayed
```

---

## show vlan mac-address-entry

---

View forwarding database (FDB) filters to display the FDB filters for the specified VLAN.

### Syntax

- **show vlan mac-address-entry**
- **show vlan mac-address-entry <1-4059>**
- **show vlan mac-address-entry mac 0x00:0x00:0x00:0x00:0x00:0x00**
- **show vlan mac-address-entry port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**
- **show vlan mac-address-entry spbm-tunnel-as-mac**

### Command Parameters

**<1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**mac 0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC address.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**spbm-tunnel-as-mac**

Discovers where entries are learned. The TUNNEL column indicates where in the SPBM network an entry is learned.

### Default

None

### Command Mode

User EXEC

## Command Output

The **show vlan mac-address-entry** command displays the following information:

Output field	Description
VLAN ID	Indicates the VLAN for this MAC address.
STATUS	Indicates the status of this entry: <ul style="list-style-type: none"> <li>• other</li> <li>• invalid</li> <li>• learned</li> <li>• self</li> <li>• mgmt</li> </ul>
MAC ADDRESS	Indicates the MAC address.
INTERFACE	Displays the network-to-network (NNI) interface.
SMLT REMOTE	Indicates the MAC address entry for the remote vIST peer.
TUNNEL	Indicates the host name of the remote Backbone Edge Bridge (BEB).

## show vlan mac-address-static

View the database status, MAC address, and QoS levels to display the static forwarding database status.

### Syntax

- **show vlan mac-address-static**
- **show vlan mac-address-static <1-4059>**
- **show vlan mac-address-static mac 0x00:0x00:0x00:0x00:0x00:0x00**
- **show vlan mac-address-static port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

### Command Parameters

**<1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**mac 0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC address.

**port {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

---

## show vlan manual-edit-mac

Show the list of manually edited MAC addresses and the associated ports.

## Syntax

- **show vlan manual-edit-mac**

## Default

None

## Command Mode

User EXEC

---

## show vlan members

View the VLAN port member status to display the port member status for all VLANs on the switch or for the specified VLAN.

## Syntax

- **show vlan members**
- **show vlan members [null-vlan] [port {slot/port[-slot/port] [,...]}] [<1-4059>]**
- **show vlan members null-vlan**
- **show vlan members port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**null-vlan**

Displays ports in a null VLAN.



**port** {slot/port[/sub-port][**-**slot/port[/sub-port]][,...]}

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show vlan members** command displays the following information:

Output field	Description
VLAN ID	Indicates the VLAN ID.
PORT MEMBER	Indicates the set of ports that are members (static or dynamic) of this VLAN.
ACTIVE MEMBER	Indicates the set of ports that are currently active in this VLAN. Active ports include all static and dynamic ports that meet the VLAN policy.
STATIC MEMBER	Indicates the set of ports that are static members of this VLAN. A static member of a VLAN is always active and never ages.
NOT_ALLOW MEMBER	Indicates the set of ports that cannot become members of this VLAN.
VLAN PORT NUM	Indicates the VLAN port number for the passive OSPF interface.

## Example

The following example displays VLAN port data.

```
Switch1:1>show vlan members
=====
                        Vlan Port
=====
VLAN  PORT          ACTIVE          STATIC          NOT_ALLOW
ID    MEMBER          MEMBER          MEMBER          MEMBER
-----
1     1/1-1/16,1/17/1-  1/1-1/16,1/17/1-
      1/17/4,1/18/1-  1/17/4,1/18/1-
      1/18/4,2/1-2/16,  1/18/4,2/1-2/16,
      2/17/1-2/17/4,  2/17/1-2/17/4,
      2/18/1-2/18/4,3/1- 2/18/1-2/18/4,3/1-
      3/6,4/1-4/4,4/6   3/6,4/1-4/4,4/6

2     4/5              4/5
```

```
All 2 out of 2 Total Num of Port Entries displayed
```

## show vlan nodal-mep

---

Display the nodal Maintenance Endpoint (MEP) configuration. The Nodal B-VLAN MEPs created on the CP and function as if they are connected to the virtual interface of the given B-VLAN. Because of this they are supported for both port and MLT based B-VLANs. To support this behavior a MAC entry is added to the FDB and a new CFM data path table containing the B-VLAN and MP level are added to direct CFM frames to the CP as required.

### Syntax

- **show vlan nodal-mep**
- **show vlan nodal-mep <1-4059>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

User EXEC

## show vlan nodal-mip-level

---

Display the nodal Maintenance Intermediate Point (MIP) level configuration. The Nodal MIP is associated with a B-VLAN. VLAN and level are sufficient to specify the Nodal MIP entity. The Nodal MIP MAC address is the SPBM system ID for the node on which it resides. If the fastpath sends a message to the CP, the MIP responds if it is not the target and the MEP responds if it is the target.

### Syntax

- **show vlan nodal-mip-level**
- **show vlan nodal-mip-level <1-4059>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

User EXEC

## show vlan private-vlan

---

Display the list of private VLANs.

## Syntax

- **show vlan private-vlan <2-4059>**

## Command Parameters

<2-4059>

Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998.

## Default

None

## Command Mode

User EXEC

## show vlan remote-mac-table

---

Display customer VLAN (C-VLAN) remote-mac-table information.

## Syntax

- **show vlan remote-mac-table <1-4059>**

- **show vlan remote-mac-table <1-4059> alternative**

## Command Parameters

### <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### alternative

Shows the table in the alternative way.

## Default

None

## Command Mode

User EXEC

## Command Output

The **show vlan remote-mac-table** command displays the following information:

Output field	Description
VLAN	Indicates the VLAN ID for this MAC address.
STATUS	Indicates the status of this entry: <ul style="list-style-type: none"> <li>• other</li> <li>• invalid</li> <li>• learned</li> <li>• self</li> <li>• mgmt</li> </ul>
MAC-ADDRESS	Indicates the customer MAC address for which the bridge has forwarding and/or filtering information.
DEST-MAC	Indicates the provide MAC address for which the bridge has forwarding and/or filtering information.
BVLAN	Indicates the B-VLAN ID for this MAC address.
DEST-SYSNAME	Indicates the system name of the node where the MAC address entry comes from.
PORTS	Either displays the value 0 or indicates the port in which a frame comes from.
SMLT REMOTE	Indicates the MAC address entry for the remote vIST peer.

## show vlan static-mcastmac

---

Display the Layer 2 multicast media access control (MAC) filters.

### Syntax

- **show vlan static-mcastmac [<1-4059>]**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### Default

None

### Command Mode

User EXEC

## show web-server

---

Display the web server information.

### Syntax

- **show web-server**

### Default

None

### Command Mode

User EXEC

## Command Output

The **show web-server** command displays the following information:

Output field	Description
Status	Specifies whether the web server is enabled or disabled.
Secure-only	Specifies whether the web server secure-only is enabled for HTTPS access to the switch.
TLS-minimum-version	Specifies the minimum version of TLS protocol configured on the switch.
RO Username Status	Specifies if read-only user is enabled for the web server.
RO Password	Specifies the read-only password.
RWA Username	Specifies the username. The default is admin.
RWA Password	Specifies the password for the web server.
Def-display-rows	Specifies the web server default display row width.
Inactivity timeout	Specifies the web-server login session inactivity timeout.
Html help tftp source-dir	Specifies the the TFTP or FTP directory for Help files.
HttpPort	Specifies the HTTP port for web access. The default value is 80.
HttpsPort	Specifies the HTTPS port for web access. The default value is 443.
NumHits	Specifies the number of hits to the web server.
NumAccessChecks	Specifies the number of access checks performed by the web server.
NumAccessBlocks	Specifies the number of access attempts blocked by the web server.
NumRxErrors	Specifies the number of receive errors the web server encounters.
NumSetRequest	Specifies the number of set-requests sent to the web server.
Minimum password length	Specifies the minimum password length. The default is 8 characters.
Last Host Access Blocked	Specifies the IP address of the last host access blocked by the web server.
In use certificate	Specifies if the certificate is self-signed or user installed.
Certificate Trustpoint CA Name	Specifies the name of the Certificate Authority.

Output field	Description
Certificate with Subject Name	Specifies the name of the subject certificate.
Ciphers-Tls	Specifies the ciphers for preset version of TLS for the web server.

## Example

```
Switch:1(config)#show web-server
Web Server Info :

      Status                : off
      Secure-only           : enabled
      TLS-minimum-version   : tlsv12
      RO Username Status    : disabled
      RO Username           : user
      RO Password           : *****
      RWA Username          : admin
      RWA Password          : *****
      Def-display-rows      : 30
      Inactivity timeout    : 900 sec
      Html help tftp source-dir :
      HttpPort              : 80
      HttpsPort             : 443
      NumHits                : 0
      NumAccessChecks        : 0
      NumAccessBlocks        : 0
      NumRxErrors            : 0

      NumTxErrors           : 0
      NumSetRequest          : 0
      Minimum password length : 8
      Last Host Access Blocked : 0.0.0.0
      In use certificate      : Self signed
      Certificate Truspoint CA Name :
      Certificate with Subject Name : 823

      Ciphers-Tls           : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
      TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA
      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
      TLS_RSA_WITH_AES_256_CBC_SHA256
      TLS_RSA_WITH_AES_128_CBC_SHA256
      TLS_RSA_WITH_AES_256_CBC_SHA
      TLS_RSA_WITH_AES_128_CBC_SHA
```

## slot reset

Resets a slot. This command is available only on hardware platforms which supports Switch Fabric (SF) module.

## Syntax

- **slot reset**

## Default

None

## Command Mode

User EXEC

## ssh (connection)

---

Connect to a remote Secure Shell (SSH) host

## Syntax

- **ssh WORD<1-256> -l WORD<1-32> [-p <1-32768>]**

## Command Parameters

**-l WORD<1-32>**

Specifies the login name of the remote Secure Shell (SSH) server.

**-p <1-32768>**

Specifies the remote Secure Shell (SSH) server port number to which to connect. The default is 22.

**WORD<1-256>**

Specifies the IP address or host name.

## Default

None

## Command Mode

User EXEC

## tacacs switch

---

Changes the privilege level to determine what commands a user can access through TACACS+ server authorization. You must configure separate profiles in the TACACS+ server configuration file for switch level.

## Syntax

- **tacacs switch back**



- **tacacs switch level**
- **tacacs switch level <1-15>**

## Command Parameters

### back

Returns the privilege level to the original level.

### level <1-15>

Selects a specific privilege level. The switch supports levels 1 through 6:

- (1) read-only
- (2) Layer 1 read-write
- (3) Layer 2 read-write
- (4) Layer 3 read-write
- (5) read-write
- (6) read-write-all
- and level 15.

## Default

None

## Command Mode

User EXEC

## telnet

---

Use this command to access another platform remotely.

## Syntax

- **telnet**
- **telnet WORD<1-256>**

## Command Parameters

### WORD <1-256>

Specifies the host name, IPv4 address or IPv6 address.

## Default

None

## Command Mode

User EXEC

## terminal

---

Configures the CLI display.

### Syntax

- **terminal length <8-64>**
- **terminal length default**
- **terminal more disable**
- **terminal more enable**

### Command Parameters

**length <8-64>**

Configures the number of lines in the output display for the current session.

**length default**

Configures the number of lines in the output display for the current session to the default value.

**more <enable|disable>**

Configures scrolling for the output display. The default is enabled.

### Default

None

## Command Mode

User EXEC

## trace cfm

---

cfm related tracing information.

### Syntax

- **trace cfm level <0-4>**

### Command Parameters

**level <0-4>**

tracing level for cfm.

## Default

None

## Command Mode

User EXEC

## trace filter file

---

Specifies the trace messages to filter.

## Syntax

- **trace filter file WORD<0-128>**
- **trace filter file WORD<0-128> bt limit WORD<0-256>**
- **trace filter file WORD<0-128> clear**
- **trace filter file WORD<0-128> disable**
- **trace filter file WORD<0-128> lines**
- **trace filter file WORD<0-128> lines WORD<0-256>**
- **trace filter file WORD<0-128> range**
- **trace filter file WORD<0-128> range WORD<0-256> WORD<0-256>**
- **trace filter file WORD<0-128> suppress**

## Command Parameters

**bt limit WORD<0-256>**

Performs backtrace filtering for a specific limit value.

**clear**

Clears trace filter information.

**disable**

Disables the trace filter.

**lines WORD<0-256>**

Specifies the lines to filter.

**range WORD<0-256> WORD<0-256>**

Specifies the range to filter.

**suppress**

Suppresses the trace filter.

**WORD<0-128>**

Specifies the filename.

## Default

None

## Command Mode

User EXEC

## trace filter module

---

Specifies the trace messages to filter.

## Syntax

- **trace filter module <0-136>**
- **trace filter module <0-136> clear**
- **trace filter module <0-136> disable**
- **trace filter module <0-136> info**
- **trace filter module <0-136> suppress**

## Command Parameters

**<0-136>**

Specifies the module ID.

**clear**

Clears trace filter information.

**disable**

Disables the trace filter.

**info**

Shows the trace filter configuration for the module.

**suppress**

Suppresses the trace filter.

## Default

None

## Command Mode

User EXEC

## trace flags

---

Enable or disable the Intermediate-System-to-Intermediate-System trace flags. After IS-IS trace is turned on, only displays trace information about the set flag.

## Syntax

- `trace flags isis`
- `trace flags isis remove {none | tx-hello | rx-hello | tx-pkt | rx-pkt | adj | opt | tx-lsack | rx-lsack | tx-lsp | rx-lsp | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | prefix | nbr-change | intf-change | decide | fdb | dr | auth-fail | config | purge | policy | redist | tx-snp | rx-snp | timer | spbm-decide | global | perf | ucast-fib | node | mcast-fib | isid | ip-shortcut | debug | ip-multicast}`
- `trace flags isis set {none | tx-hello | rx-hello | tx-pkt | rx-pkt | adj | opt | tx-lsack | rx-lsack | tx-lsp | rx-lsp | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | prefix | nbr-change | intf-change | decide | fdb | dr | auth-fail | config | purge | policy | redist | tx-snp | rx-snp | timer | spbm-decide | global | perf | ha | ucast-fib | node | mcast-fib | isid | ip-shortcut | debug | ip-multicast}`

## Default

None

## Command Mode

User EXEC

## trace flags isis

Enable or disable the Intermediate-System-to-Intermediate-System trace flags. After IS-IS trace is turned on, only displays trace information about the set flag.

## Syntax

- `trace flags isis`
- `trace flags isis remove {none | tx-hello | rx-hello | tx-pkt | rx-pkt | adj | opt | tx-lsack | rx-lsack | tx-lsp | rx-lsp | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | prefix | nbr-change | intf-change | decide | fdb | dr | auth-fail | config | purge | policy | redist | tx-snp | rx-snp | timer | spbm-decide | global | perf | ucast-fib | node | mcast-fib | isid | ip-shortcut | debug}`
- `trace flags isis set {none | tx-hello | rx-hello | tx-pkt | rx-pkt | adj | opt | tx-lsack | rx-lsack | tx-lsp | rx-lsp | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | prefix | nbr-change | intf-change | decide | fdb | dr | auth-fail | config | purge | policy | redist | tx-snp | rx-snp | timer | spbm-decide | global | perf | ucast-fib | node | mcast-fib | isid | ip-shortcut | debug}`

## Command Parameters

**adj**

Specifies the option of adjacencies.

**auth-fail**

Specifies the option of authorization failed.

**config**

Specifies the option of configuration.

**dd-masterslave**

The current release does not use this option.

**debug**

Specifies the option of debug.

**decide**

Specifies the option of shortest path first computation.

**dr**

Specifies the option of designated router.

**fdb**

Specifies the option of filtering database.

**flood**

Specifies the option of flood.

**global**

The current release does not use this option.

**ha**

Specifies the option of High Availability.

**intf-change**

Specifies the option of IS-IS circuit (interface) events.

**ip-multicast**

Specifies the option of IP multicast.

**ip-shortcut**

Specifies the option of IP Shortcut.

**isid**

Specifies the option of I-SID.

**mcast-fib**

Specifies the option of multicast forwarding information base.

**nbr-change**

Specifies the option of neighbor change.

**nbr-mismatch**

Specifies the option of neighbor mismatch.

**node**

Specifies the option of node.

**none**

Specifies the option of none.

**opt**

Specifies the option of IS-IS TLVs.

**perf**

Specifies the option of SPBM performance.

**pkt-err**

Specifies the option of packet error.

**policy**

The current release does not use this option.

**prefix**

Specifies the option of prefix.

**purge**

Specifies the option of Link State Packet purge.

**redist**

Specifies the option of redistribute.

**remove**

Removes the Intermediate-System-to-Intermediate-System (IS-IS) trace flags for the specified option.

**rx-hello**

Specifies the option of received IS-IS hello packets.

**rx-lsack**

Specifies the option of received LSP acknowledgement.

**rx-lsp**

Specifies the option of received Link State Packet.

**rx-pkt**

Specifies the option of received packets.

**rx-snp**

Specifies the option of received sequence number packet (CSNP and PSNP).

**set**

Configures the Intermediate-System-to-Intermediate-System (IS-IS) trace flags for the specified option.

**spbm-decide**

Specifies the option of shortest path first computation for SPBM.

**spf-extern**

Specifies the option of shortest path first external.

**spf-inter**

Specifies the option of shortest path first internal.

**spf-intra**

The current release does not use this option.

**timer**

Specifies the option of timer.

**tx-hello**

Specifies the option of transmitted IS-IS hello packets.

**tx-lsack**

Specifies the option of transmitted LSP acknowledgement.

**tx-lsp**

Specifies the option of transmitted Link State Packet.

**tx-pkt**

Specifies the option of transmitted packets.

**tx-snp**

Specifies the option of transmitted sequence number PDU (CSNP and PSNP).

**ucast-fib**

Specifies the option of unicast forwarding information base.

## Default

None

## Command Mode

User EXEC

## trace flags ospf

---

Enable or disables OSPFv2 trace flags for debugging. The flags you set are used by the trace level.

## Syntax

- **trace flags ospf**
- **trace flags ospf remove** {none | all | tx-hello | rx-hello | tx-ddp-pkt | rx-ddp-pkt | tx-lsu-pkt | rx-lsu-pkt | tx-lsack | rx-lsack | tx-lsr | rx-lsr | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | spf-tree | nbr-change | intf-change | abr-lsa-generate | asbr-lsa-generate | dr | dd-masterslave | auth-fail | config | lsa | policy}
- **trace flags ospf set** <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsupkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spfextern|spf-tree|nbr-change|intf-



```
change | abr-lsa-generate | asbr-lsa-generate | dr | ddmasterslave | auth-fail |
config | lsa | policy >
```

## Command Parameters

remove <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spfextern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|ddmasterslave|auth-fail|config|lsa|policy >

Removes the OSPF trace flags for the specified option.

set <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsupkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spfextern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|ddmasterslave|auth-fail|config|lsa|policy >

Sets the OSPF trace flags for the specified option.

## Default

By default, all flags are turned off.

## Command Mode

User EXEC

## trace grep

---

Search trace results for a specific string value, for example, the word error.

## Syntax

- **trace grep**
- **trace grep WORD<0-128>**

## Command Parameters

WORD<0-128>

Specifies the search keyword. You can use a specific MAC address or search for errors, using the command, trace grep error.

## Default

None

## Command Mode

User EXEC

## trace level

---

Use trace to observe the status of a software module at a given time.

### Syntax

- `trace level`
- `trace level <<Module_ID> <0-4>`
- `trace level sub-system WORD<1-20> <0-5>`
- `trace level sub-system WORD<1-20> <0-5> process WORD<1-20>`
- `trace level sub-system WORD<1-20> <0-5> process WORD<1-20> slot <1-12>`
- `trace level sub-system WORD<1-20> <0-5> process WORD<1-20> slot SF1`
- `trace level sub-system WORD<1-20> <0-5> process WORD<1-20> slot SF2`
- `trace level sub-system WORD<1-20> <0-5> process WORD<1-20> slot SF3`
- `trace level sub-system WORD<1-20> <0-5> process WORD<1-20> slot SF4`
- `trace level sub-system WORD<1-20> <0-5> process WORD<1-20> slot SF5`
- `trace level sub-system WORD<1-20> <0-5> process WORD<1-20> slot SF6`
- `trace level sub-system WORD<1-20> <0-5> slot SF1`
- `trace level sub-system WORD<1-20> <0-5> slot SF2`
- `trace level sub-system WORD<1-20> <0-5> slot SF3`
- `trace level sub-system WORD<1-20> <0-5> slot SF4`
- `trace level sub-system WORD<1-20> <0-5> slot SF5`
- `trace level sub-system WORD<1-20> <0-5> slot SF6`

### Command Parameters

`<0-4>`

Specifies the trace level from 0 to 4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.

`<Module_ID>`

`<Module_ID>` specifies the module for the trace. Different hardware platforms support different ID ranges because of feature support differences. To see which module IDs are available on the switch, use the **show trace modid-list** command or CLI command completion Help.

`sub-system WORD<1-20>`

Specifies a sub-system ID.

`<slot>`

Specifies the valid IO slots. Different hardware platforms support different slot ranges. Use the CLI Help to see the available range for your switch.

## Default

None

## Command Mode

User EXEC

## trace route-map

---

Enable or disable trace for route-maps.

## Syntax

- **trace route-map { off | on }**
- **trace route-map { off | on } address {A.B.C.D}**
- **trace route-map { off | on } iflist WORD<1-256>**
- **trace route-map { off | on } name WORD<1-64>**
- **trace route-map { off | on } protocol any**
- **trace route-map { off | on } protocol ospf**
- **trace route-map { off | on } protocol rip**
- **trace route-map { off | on } type accept**
- **trace route-map { off | on } type announce**

## Command Parameters

**{ off | on }**

Enables or disables tracing.

**address {A.B.C.D}**

Specifies the interface address.

**iflist WORD<1-256>**

Specifies the interface list name.

**name WORD<1-64>**

Specifies the name of a route-map.

**protocol**

Specifies a routing protocol.

**type**

Specifies a route-map type.

## Default

None

## Command Mode

User EXEC

## trace save

---

Save Trace Sub-System Configuration.

### Syntax

- **trace save**

### Default

None

## Command Mode

User EXEC

## trace screen

---

Configure if the system Display trace information on screen.

### Syntax

- **trace screen disable**
- **trace screen enable**

### Command Parameters

**disable**

Prevents the trace messages from appearing on screen.

**enable**

Shows the trace messages on screen.

### Default

None

## Command Mode

User EXEC

## trace shutdown

---

Disables trace.

## Syntax

- **trace shutdown**

## Default

None

## Command Mode

User EXEC

## **trace spbm isis level**

---

Starts debug tracing for IS-IS. <0-4> specifies the trace level from 0 to 4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.

## Syntax

- **trace spbm isis level <0-4>**

## Default

None

## Command Mode

User EXEC



# VLAN Interface Configuration

---

The following topics document commands available in VLAN Interface Configuration mode of the command line interface (CLI).

## dsapssap

---

Configure the multiple DSAP and SSAP to create a protocol-based VLAN.

### Syntax

- **default dsapssap** <0x0-0xffff | 0x0-0x0>
- **dsapssap** <0x0-0xffff | 0x0-0x0>
- **no dsapssap** <0x0-0xffff | 0x0-0x0>

### Command Parameters

<0x0-0xffff | 0x0-0x0>

Configures a table used to maintain DSAP/SSAP values assigned to an sna802dot2 or user defined VLAN.

### Default

None

### Command Mode

VLAN Interface Configuration

## ip address (on a VLAN)

---

Assign an IP address to a VLAN to configure the VLAN.

### Syntax

- **ip address** {A.B.C.D/X}
- **ip address** {A.B.C.D} {A.B.C.D}
- **ip address** {A.B.C.D} {A.B.C.D} **dvr-one-ip**
- **ip address** {A.B.C.D} {A.B.C.D} <MAC-offset>

- **ip address {A.B.C.D} {A.B.C.D} name WORD<0-64>**
- **no ip address {A.B.C.D}**

## Command Parameters

**<A.B.C.D/X>|<A.B.C.D> <A.B.C.D>**

Specifies the IP address and subnet mask in the format A.B.C.D/X or A.B.C.D A.B.C.D.

### dvr-one-ip

Specifies that the IP address will be used as the DvR gateway IP address and will be used by all other DvR Controllers for the DvR VLAN subnet.

**<MAC-offset>**

Specifies a number by which to offset the MAC address from the chassis MAC address. This ensures that each IP address has a different MAC address. If you omit this variable, a unique MAC offset is automatically generated. Different hardware platforms support different ranges. To see which range is available on the switch, use the CLI command completion Help.

This parameter does not apply to all hardware platforms.

**name WORD <0-64>**

Specifies the name associated with the IP address on a VLAN.

## Default

None

## Command Mode

VLAN Interface Configuration

## Usage Guidelines

The *name* parameter is not supported on VSP 8600 Series or XA1400 Series.

## ip arp-inspection enable

---

Enables DAI on a particular VLAN.

## Syntax

- **default ip arp-inspection enable**
- **ip arp-inspection enable**
- **no ip arp-inspection enable**

## Default

Disabled

## Command Mode

VLAN Interface Configuration

### ip arp-proxy enable (for a VLAN)

---

Configure an ARP proxy to allow a router to answer a local ARP request for a remote destination.

#### Syntax

- **ip arp-proxy enable**
- **no ip arp-proxy**
- **no ip arp-proxy enable**

#### Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

### ip arp-response (for a VLAN)

---

Enable Address Resolution Protocol (ARP) on the switch to allow a router to answer a local ARP request.

#### Syntax

- **default ip arp-response**
- **ip arp-response**
- **no ip arp-response**

#### Default

None

## Command Mode

VLAN Interface Configuration

### ip bfd (for a VLAN)

---

Enable and configure Bidirectional Forwarding Detection (BFD) on a VLAN.



## Syntax

- **default ip bfd enable**
- **default ip bfd interval**
- **default ip bfd min-rx**
- **default ip bfd multiplier**
- **default ip bfd vlan**
- **ip bfd enable**
- **ip bfd interval**
- **ip bfd min-rx**
- **ip bfd multiplier**
- **ip bfd vlan**
- **no ip bfd**
- **no ip bfd vlan**

## Command Parameters

### enable

Enable BFD on a VLAN.

### interval

Specifies the transmit interval in milliseconds. The default is 200 ms.

The minimum value for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure the remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.



#### Note

For XA1400 Series, the default is 1000 ms.

### min-rx

Specifies the receive interval in milliseconds. The default is 200 ms.

The minimum value for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure the remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.



#### Note

For XA1400 Series, the default is 1000 ms.

### multiplier

Specifies the multiplier used to calculate the amount of time BFD waits before it declares a receive timeout. The default is 3.

If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

### vlan <1-4094>

Specifies the VLAN ID in the range of 1-4094.

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip dhcp-relay (for a VLAN)

---

Configure Dynamic Host Configuration Protocol (DHCP) relay on an interface.



### Note

The command `no ip dhcp-relay` disables DHCP relay but does not delete the DHCP entry.

## Syntax

- `default ip dhcp-relay`
- `ip dhcp-relay`
- `no ip dhcp-relay`

## Default

None

## Command Mode

VLAN Interface Configuration

## ip dhcp-relay broadcast (for a VLAN)

---

Configures Dynamic Host Configuration Protocol (DHCP) relay on an interface to send the server reply as a broadcast to the end station.



### Note

The command `no ip dhcp-relay` disables broadcast DHCP relay but does not delete the DHCP entry.

## Syntax

- `default ip dhcp-relay broadcast`
- `ip dhcp-relay broadcast`
- `no ip dhcp-relay broadcast`

## Default

None

## Command Mode

VLAN Interface Configuration

## ip dhcp-relay circuitId (for a VLAN)

---

Configure Dynamic Host Configuration Protocol (DHCP) relay to insert the Option 82 Circuit ID on an interface.



### Note

The command `no ip dhcp-relay` disables circuitId DHCP relay but does not delete the DHCP entry.

## Syntax

- **default ip dhcp-relay circuitId**
- **ip dhcp-relay circuitId**
- **no ip dhcp-relay circuitId**

## Default

None

## Command Mode

VLAN Interface Configuration

## ip dhcp-relay clear-counters (for a VLAN)

---

Configure Dynamic Host Configuration Protocol (DHCP) relay to clear the dhcp-relay counter on an interface.

## Syntax

- **ip dhcp-relay clear-counters**

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip dhcp-relay fwd-path {A.B.C.D} (for a VLAN)

---

Create the forwarding path from the client to the server.

### Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D}**
- **ip dhcp-relay fwd-path {A.B.C.D}**
- **no ip dhcp-relay fwd-path {A.B.C.D}**

### Command Parameters

{A.B.C.D}

Creates a forwarding path to the Dynamic Host Configuration Protocol (DHCP) server with a mode and a state. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface.



#### Tip

If the relay is a Virtual Router configured on this interface, you must set the vrid.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip dhcp-relay fwd-path {A.B.C.D} disable

---

Disables the forwarding path on a VLAN.

### Syntax

- **ip dhcp-relay fwd-path {A.B.C.D} disable**

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip dhcp-relay fwd-path {A.B.C.D} enable

---

Enables the forwarding path on a VLAN.

### Syntax

- **ip dhcp-relay fwd-path {A.B.C.D} enable**

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip dhcp-relay fwd-path {A.B.C.D} mode (for a VLAN)

---

Modify Dynamic Host Configuration Protocol (DHCP) mode to forward Bootstrap Protocol (BOOTP) messages only, DHCP messages only, or both.

### Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D} mode**
- **ip dhcp-relay fwd-path {A.B.C.D} mode bootp**
- **ip dhcp-relay fwd-path {A.B.C.D} mode bootp\_dhcp**
- **ip dhcp-relay fwd-path {A.B.C.D} mode dhcp**

### Command Parameter

{bootp|dhcp|bootp\_dhcp}

Configures DHCP mode to forward BOOTP messages only, DHCP messages only, or both. The default is both.

### Default

The default mode is both.

### Command Mode

VLAN Interface Configuration

---

## ip dhcp-relay fwd-path {A.B.C.D} src-port-67 (for a VLAN)

---

Configure a forwarding path with source port 67 in a User Datagram Protocol (UDP) on a VLAN.

## Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D} src-port-67**
- **ip dhcp-relay fwd-path {A.B.C.D} src-port-67**
- **no ip dhcp-relay fwd-path {A.B.C.D} src-port-67**

## Command Parameters

**{A.B.C.D}**

Creates a forwarding path to the DHCP server with a mode and a state. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface.



### Tip

If the relay is a Virtual Router configured on this interface, you must set the vrid.

**src-port-67**

Specifies that the UDP source port is 67 for BOOTP request. The default is 68.

## Default

None

## Command Mode

VLAN Interface Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255> (for a VLAN)

---

Creates a forward path server with a virtual router ID (or VRRP ID), a mode, and a state.

## Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>**
- **ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>**
- **no ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>**

## Command Parameters

**<1-255>**

Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses. The range is 1 to 255.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip dhcp-relay max-hop (for a VLAN)

---

Configures the maximum number of hops before a BOOTP/DHCP packet is discarded on an interface.

## Syntax

- **default ip dhcp-relay max-hop**
- **ip dhcp-relay max-hop <1-16>**

## Command Parameters

<1-16>

Configures the maximum number of hops before a BOOTP/DHCP packet is discarded. The range is 1 to 16. The default is 4.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip dhcp-relay min-sec (for a VLAN)

---

Configures the minimum seconds count for Dynamic Host Configuration Protocol (DHCP) on an interface.

## Syntax

- **default ip dhcp-relay min-sec**
- **ip dhcp-relay min-sec <0-65535>**

## Command Parameters

<0-65535>

Configures the minimum seconds count for DHCP. If the secs field in the Bootstrap Protocol (BOOTP)/DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped. The range is 0 - 65535. The default is 0 seconds.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip dhcp-relay mode (for a VLAN)

---

Configures Dynamic Host Configuration Protocol (DHCP) mode to forward BOOTP messages only, DHCP messages only, or both.

## Syntax

- **default ip dhcp-relay mode**
- **ip dhcp-relay mode { bootp | dhcp | bootp\_dhcp }**

## Command Parameters

{bootp|dhcp|bootp\_dhcp}

Configures DHCP mode to forward BOOTP messages only, DHCP messages only, or both. The default is both.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip dhcp-relay remoteld (for a VLAN)

---

Enables Option82 remote ID on the interface.

## Syntax

- **default ip dhcp-relay remoteld**
- **ip dhcp-relay remoteld**
- **no ip dhcp-relay remoteld**

## Default

None



## Command Mode

VLAN Interface Configuration

### ip dhcp-relay trusted (for a VLAN)

---

Configures the Dynamic Host Configuration Protocol (DHCP) circuit as trusted on an interface.

#### Syntax

- **default ip dhcp-relay trusted**
- **ip dhcp-relay trusted**
- **no ip dhcp-relay trusted**

#### Default

None

## Command Mode

VLAN Interface Configuration

### ip dhcp-snooping enable (for VLAN)

---

Enables DHCP Snooping on a specific VLAN.

#### Syntax

- **ip dhcp-snooping enable**
- **ip dhcp-snooping enable**
- **no ip dhcp-snooping enable**

#### Default

Disabled

## Command Mode

VLAN Interface Configuration

### ip directed-broadcast (for a VLAN)

---

Configure the device to forward directed broadcasts for a VLAN.

## Syntax

- **default ip directed-broadcast**
- **default ip directed-broadcast enable**
- **ip directed-broadcast**
- **ip directed-broadcast enable**
- **no ip directed-broadcast**
- **no ip directed-broadcast enable**

## Command Parameters

### enable

Allows the device to forward directed broadcast frames to the specified VLAN. The default setting for this feature is enabled.

## Default

The default is enabled.

## Command Mode

VLAN Interface Configuration

## ip forward-protocol udp (on a VLAN)

---

Configure UDP protocols to determine which UDP broadcasts are forwarded

## Syntax

- **default ip forward-protocol udp**
- **default ip forward-protocol udp vlan <1-4059>**
- **ip forward-protocol udp vlan <1-4059>**
- **no ip forward-protocol udp**
- **no ip forward-protocol udp vlan <1-4059>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

VLAN Interface Configuration

# ip forward-protocol udp broadcastmask

---

Configure the broadcast mask on the IP forwarding list.

## Syntax

- `default ip forward-protocol udp broadcastmask`
- `default ip forward-protocol udp broadcastmask {A.B.C.D}`
- `ip forward-protocol udp broadcastmask {A.B.C.D}`
- `ip forward-protocol udp vlan <1-4059> broadcastmask {A.B.C.D}`
- `no ip forward-protocol udp broadcastmask`
- `no ip forward-protocol udp broadcastmask {A.B.C.D}`

## Command Parameters

<A.B.C.D>

Sets the interface broadcast mask (the interface broadcast mask can be different from the interface mask). A.B.C.D is an IP address in a.b.c.d format.

## Default

None

## Command Mode

VLAN Interface Configuration

# ip forward-protocol udp maxttl

---

Set the maximum time to live.

## Syntax

- `default ip forward-protocol udp maxttl`
- `default ip forward-protocol udp maxttl <1-16>`
- `ip forward-protocol udp maxttl <1-16>`
- `ip forward-protocol udp vlan <1-4059> maxttl <1-16>`

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 0 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

maxttl <1-16>

Sets the maximum time-to-live value (TTL) for the UDP broadcast forwarded by the interface. The range is 1 to 16.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip forward-protocol udp portfwddlist (on a VLAN)

---

Configure the UDP port forwarding list.

## Syntax

- **ip forward-protocol udp portfwddlist <1-1000>**
- **ip forward-protocol udp vlan <1-4059> portfwddlist <1-1000>**
- **no ip forward-protocol udp portfwddlist**
- **no ip forward-protocol udp portfwddlist <1-1000>**

## Command Parameters

<1-1000>

Creates a UDP port forwarding list in the range of 1 to 1000.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

VLAN Interface Configuration

### ip igmp access-list (for a VLAN)

---

Configure multicast access control for a VLAN to restrict access to certain multicast streams and to protect multicast streams from spoofing (injecting data to the existing streams).

#### Syntax

- **default ip igmp access-list WORD<1-64> {A.B.C.D/X}**
- **ip igmp access-list WORD<1-64> {A.B.C.D/X} {deny-tx | deny-rx | deny-both | allow-only-tx | allow-only-rx | allow-only-both}**
- **no ip igmp access-list WORD<1-64> {A.B.C.D/X}**

#### Command Parameters

**{A.B.C.D/X}**

Creates an access control group entry for a specific Internet Group Management Protocol (IGMP) interface. Specifies the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.

**deny-tx | deny-rx | deny-both | allowonly-tx | allowonly-rx | allowonly-both**

Indicates the action for the specified Internet Group Management Protocol (IGMP) interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.

**WORD<1-64>**

Specifies the name of the access list from 1-64 characters.

#### Default

None

## Command Mode

VLAN Interface Configuration

### ip igmp access-list mode (for a VLAN)

---

Change an existing access list on the VLAN interface.

#### Syntax

- **default ip igmp access-list WORD<1-64> {A.B.C.D/X}**
- **ip igmp access-list WORD<1-64> {A.B.C.D/X} mode {deny-tx | deny-rx | deny-both | allowonly-tx | allow-only-rx | allow-only-both}**

- **no ip igmp access-list WORD<1-64> {A.B.C.D/X}**

## Command Parameters

**{A.B.C.D/X}**

Creates an access control group entry for a specific Internet Group Management Protocol (IGMP) interface. Specifies the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.

**deny-tx | deny-rx | deny-both | allowonly-tx | allowonly-rx | allowonly-both**

Indicates the action for the specified Internet Group Management Protocol (IGMP) interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.

**WORD<1-64>**

Specifies the name of the access list from 1-64 characters.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip igmp compatibility-mode (for a VLAN)

---

Enables IGMP v2-v3 compatibility mode.

## Syntax

- **default ip igmp compatibility-mode**
- **ip igmp compatibility-mode**
- **no ip igmp compatibility-mode**

## Default

The default value is disabled, which means IGMPv3 is not compatible with IGMPv1 or IGMPv2.

## Command Mode

VLAN Interface Configuration

## ip igmp dynamic-downgrade-version (for a VLAN)

---

Configures the version of Internet Group Management Protocol (IGMP) to handle older query messages if the system downgrades. If the system downgrades, the host with IGMPv3 only capability does not work. If you do not configure the system to downgrade the version of IGMP, the system logs a warning.

## Syntax

- **default ip igmp dynamic-downgrade-version**
- **ip igmp dynamic-downgrade-version**
- **no ip igmp dynamic-downgrade-version**

## Default

Enabled

## Command Mode

VLAN Interface Configuration

## ip igmp igmpv3-explicit-host-tracking (for a VLAN)

---

Track all the source and group members. You must enable explicit-host-tracking to use fast leave for IGMPv3.

## Syntax

- **default ip igmp igmpv3-explicit-host-tracking**
- **ip igmp igmpv3-explicit-host-tracking**
- **no ip igmp igmpv3-explicit-host-tracking**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip igmp immediate-leave (for a VLAN)

---

Enable fast (immediate) leave mode to specify if a VLAN receives a leave message from a member of a group.

## Syntax

- **default ip igmp immediate-leave**
- **ip igmp immediate-leave**
- **no ip igmp immediate-leave**

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip igmp immediate-leave-members

Configure fast leave members on a VLAN to specify fast leave capable ports.

## Syntax

- **default ip igmp immediate-leave-members {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **ip igmp immediate-leave-members {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no ip igmp immediate-leave-members {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip igmp mrdisc

Configure the multicast route discovery options to enable the automatic discovery of multicast-capable routers.

## Syntax

- **default ip igmp mrdisc**
- **default ip igmp mrdisc maxadvertinterval**



- `default ip igmp mrdisc maxinitadvertinterval`
- `default ip igmp mrdisc maxinitadvertisements`
- `default ip igmp mrdisc minadvertinterval`
- `default ip igmp mrdisc neighdeadinterval`
- `ip igmp mrdisc`
- `ip igmp mrdisc maxadvertinterval <2-180>`
- `ip igmp mrdisc maxinitadvertinterval <2-180>`
- `ip igmp mrdisc maxinitadvertisements <2-15>`
- `ip igmp mrdisc minadvertinterval <3-180>`
- `ip igmp mrdisc neighdeadinterval <2-180>`
- `no ip igmp mrdisc`

## Command Parameters

### `maxadvertinterval <2-180>`

Configures the maximum number (in seconds) between successive advertisements. For this change to take effect, you must save the configuration, and then reset the switch. The default is 20.

### `maxinitadvertinterval <2-180>`

Configures the maximum number (in seconds) between successive initial advertisements. For this change to take effect, you must save the configuration, and then reset the switch. The default is 2.

### `maxinitadvertisements <2-15>`

Configures the maximum number of initial multicast advertisements after initialization. For this change to take effect, you must save the configuration, and then reset the switch. The default is 3.

### `minadvertinterval <3-180>`

Configures the minimum number (in seconds) between successive advertisements. For this change to take effect, you must save the configuration, and then reset the switch. The default is 15.

### `neighdeadinterval <2-180>`

Configures the multicast router discovery dead interval-the number of seconds the multicast route neighbors for the switch must wait before assuming that the multicast router is down. The default is 60.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip igmp mrouter (for a VLAN)

---

Configures the multicast router ports.

### Syntax

- **default ip igmp mrouter**
- **ip igmp mrouter {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no ip igmp mrouter {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**

### Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip igmp proxy (for a VLAN)

---

Configure the proxy-snoop option globally for a VLAN.

### Syntax

- **default ip igmp proxy**
- **ip igmp proxy**
- **no ip igmp proxy**

### Default

Disabled

### Command Mode

VLAN Interface Configuration

## ip igmp query-interval (for a VLAN)

---

Configure the frequency (in seconds) at which the VLAN transmits host query packets.

### Syntax

- **default ip igmp query-interval**
- **ip igmp query-interval <1-65535>**

### Command Parameters

<1-65535>

Specifies the frequency (in seconds) at which the VLAN transmits host query packets. The default is 125 seconds.

### Default

The default is 125 seconds.

### Command Mode

VLAN Interface Configuration

## ip igmp query-max-response (for a VLAN)

---

Configure the maximum response time advertised in IGMPv2 general queries on a VLAN interface. You cannot configure this value for IGMPv1.

### Syntax

- **default ip igmp query-max-response**
- **ip igmp query-max-response <0-255>**

### Command Parameters

<0-255>

Specifies the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1. Smaller values enable a router to prune groups faster.



#### Important

You must configure this value lower than the query-interval.

### Default

None

## Command Mode

VLAN Interface Configuration

## ip igmp robust-value (for a VLAN)

---

Configure the expected packet loss of a network.

### Syntax

- **default ip igmp robust-value**
- **ip igmp robust-value <2-255>**

### Command Parameters

<2-255>

Specifies the expected packet loss of a network. Increase the value if you expect the network to experience packet loss. The default is 2 seconds.

### Default

The default is 2 seconds.

## Command Mode

VLAN Interface Configuration

## ip igmp router-alert (for a VLAN)

---

Configure the router to ignore Internet Group Management Protocol (IGMP) packets that do not contain the router alert IP option. The default is disabled. When disabled, the router processes IGMP packets regardless of the status of the router alert IP option.

### Syntax

- **default ip igmp router-alert**
- **ip igmp router-alert**
- **no ip igmp router-alert**

### Default

Disabled

## Command Mode

VLAN Interface Configuration

## Usage Guidelines

To maximize network performance, configure this parameter according to the version of IGMP currently in use:

- IGMPv1 - Disable
- IGMPv2 - Enable
- IGMPv3 - Enable

## ip igmp snooping (for a VLAN)

---

Configure the snoop option for the VLAN.

### Syntax

- **default ip igmp snooping**
- **ip igmp snooping**
- **no ip igmp snooping**

### Default

Disabled

### Command Mode

VLAN Interface Configuration

## ip igmp snoop-querier

---

Enables the Layer 2 querier on a VLAN interface.

### Syntax

- **default ip igmp snoop-querier**
- **ip igmp snoop-querier**
- **no ip igmp snoop-querier**

### Default

The default is disabled.

### Command Mode

VLAN Interface Configuration

---

## ip igmp snoop-querier-addr

---

Configures the address of the IGMP snoop querier.

### Syntax

- `default ip igmp snoop-querier-addr`
- `ip igmp snoop-querier-addr {A.B.C.D}`
- `no ip igmp snoop-querier-addr`

### Command Parameters

{A.B.C.D}

Specifies the IP address.

### Default

The default value is 0.0.0.0.

### Command Mode

VLAN Interface Configuration

---

## ip igmp static-group

---

Configure IGMP static members to add members to a snoop group.

### Syntax

- `default ip igmp static-group {A.B.C.D}`
- `default ip igmp static-group {A.B.C.D} {A.B.C.D}`
- `default ip igmp static-group {A.B.C.D} {A.B.C.D} {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} { static | blocked }`
- `default ip igmp static-group {A.B.C.D} {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} { static | blocked }`
- `ip igmp static-group {A.B.C.D} {A.B.C.D} {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} { static | blocked }`
- `ip igmp static-group {A.B.C.D} {A.B.C.D} port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} { static | blocked }`
- `ip igmp static-group {A.B.C.D} {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} { static | blocked }`
- `ip igmp static-group {A.B.C.D} port {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} { static | blocked }`
- `no ip igmp static-group {A.B.C.D}`

- **no ip igmp static-group {A.B.C.D} {A.B.C.D}**
- **no ip igmp static-group {A.B.C.D} {A.B.C.D} {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} { static | blocked }**

## Command Parameters

[static|blocked]

Adds a static-member entry to the Internet Group Management Protocol (IGMP) interface. value is the port or list of ports to which you want to redirect the multicast stream for this multicast group. static|blocked configures the route to static or blocked.

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

<A.B.C.D> <A.B.C.D>

Indicates the IP address range from <A.B.C.D> to <A.B.C.D> of the selected multicast group.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip igmp stream-limit (for a VLAN)

Configure multicast stream limitation on a VLAN to limit the number of concurrent multicast streams on the VLAN.

## Syntax

- **default ip igmp stream-limit**
- **ip igmp stream-limit**
- **ip igmp stream-limit stream-limit-max-streams <0-65535>**
- **no ip igmp stream-limit**

## Command Parameters

stream-limit-max-streams <0-65535>

Sets the maximum number of streams allowed on an interface. The value ranges from 0 to 65535.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip igmp stream-limit-group

---

Configure multicast stream limitation members on ports of a specific VLAN to limit the number of multicast groups that can join a VLAN.

## Syntax

- **default ip igmp stream-limit-group {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**
- **default ip igmp stream-limit-group {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} enable**
- **ip igmp stream-limit-group {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} enable max-streams <0-65535>**
- **ip igmp stream-limit-group {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} max-streams <0-65535>**
- **no ip igmp stream-limit-group {slot/port[/sub-port] [-slot/port[/sub-port]][,...]}**
- **no ip igmp stream-limit-group {slot/port[/sub-port] [-slot/port[/sub-port]][,...]} enable**

## Command Parameters

*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**max-streams <0-65535>**

Configures the maximum number of allowed streams for the specified ports on this VLAN. The range is from 0-65535 and the default is 4. To use the default configuration, use the default option in the command: default ip igmp stream-limit-group <ports>

## Default

None



## Command Mode

VLAN Interface Configuration

### ip igmp upnp-filter (for a VLAN)

---

Configure Universal Plug and Play (uPnP) Filtering on a IGMP-enabled interface to drop all incoming multicast packets destined for any multicast group residing in a specific range.

#### Syntax

- **default ip igmp upnp-filter [ip <A.B.C.D/X>]**
- **ip igmp upnp-filter [ip <A.B.C.D/X>]**
- **no ip igmp upnp-filter**

#### Command Parameters

ip <A.B.C.D/X>

Specifies the multicast destination IP address range to filter. The default multicast group address is 239.255.255.250/32.

#### Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

### ip igmp version (for a VLAN)

---

Configure the version of Internet Group Management Protocol (IGMP) on the interface.

#### Syntax

- **default ip igmp version**
- **ip igmp version <1-3>**

#### Command Parameters

<1-3>

Specifies the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is 2 (IGMPv2).

## Default

The default is 2 (IGMPv2).

## Command Mode

VLAN Interface Configuration

## ip ipsec enable (for a VLAN)

---

Enable Internet Protocol Security (IPsec) for IPv4 on a VLAN.

## Syntax

- **default ip ipsec enable**
- **ip ipsec enable**
- **no ip ipsec enable**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip ipsec policy (for a VLAN)

---

Link an Internet Protocol Security (IPsec) IPv4 policy to a VLAN.

## Syntax

- **default ip ipsec policy WORD<1-32>**
- **ip ipsec policy WORD<1-32>**
- **ip ipsec policy WORD<1-32> dir both**
- **ip ipsec policy WORD<1-32> dir in**
- **ip ipsec policy WORD<1-32> dir out**
- **no ip ipsec policy WORD<1-32> dir both**
- **no ip ipsec policy WORD<1-32> dir in**
- **no ip ipsec policy WORD<1-32> dir out**

## Command Parameters

**dir <both|in|out>**

Specifies the direction to which IPsec applies. Both specifies both ingress and egress traffic, in specifies ingress traffic, and out specifies egress traffic. By default, the direction is both.

WORD<1-32>

Specifies the IPsec policy name.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip irdp address (for a VLAN)

---

Configure Internet Control Message Protocol (ICMP) Router Discovery to enable hosts attached to multicast or broadcast networks to discover the IP addresses of their neighboring routers.

## Syntax

- **default ip irdp address**
- **default ip irdp address <A.B.C.D>**
- **default ip irdp vlan <1-4059> address**
- **ip irdp address <A.B.C.D>**
- **ip irdp vlan <1-4059> address {A.B.C.D}**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**address <A.B.C.D>**

Specifies the IP destination address use for broadcast or multicast router advertisements sent from the interface. The address is the all-systems multicast address, 224.0.0.1, or the limited-broadcast address, 255.255.255.255.

## Default

The default address is 255.255.255.255.

## Command Mode

VLAN Interface Configuration

---

## ip irdp holdtime (for a VLAN)

---

Configure the lifetime for advertisements.

### Syntax

- **default ip irdp holdtime**
- **default ip irdp vlan <1-4059> holdtime**
- **ip irdp holdtime <4-9000>**
- **ip irdp vlan <1-4059> holdtime <4-9000>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

<4-4000>

Specifies the lifetime.

### Default

The default is 1800.

### Command Mode

VLAN Interface Configuration

---

## ip irdp maxadvertinterval (for a VLAN)

---

Specify the maximum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the router interface.

### Syntax

- **default ip irdp maxadvertinterval**
- **default ip irdp vlan <1-4059> maxadvertinterval**
- **ip irdp maxadvertinterval <4-1800>**
- **ip irdp vlan <1-4059> maxadvertinterval <4-1800>**

### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

<4-1800>

Specifies the maximum time in seconds.

## Default

The default is 600 seconds.

## Command Mode

VLAN Interface Configuration

## ip irdp minadvertinterval (for a VLAN)

---

Specify the minimum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the interface. The range is 3 seconds to maxadvertinterval.

## Syntax

- **default ip irdp minadvertinterval**
- **default ip irdp vlan <1-4059> minadvertinterval**
- **ip irdp minadvertinterval <3-1800>**
- **ip irdp vlan <1-4059> minadvertinterval <3-1800>**

## Command Parameters

<3-1800>

Specifies the minimum time in seconds.

## Default

The default is 450 seconds.

## Command Mode

VLAN Interface Configuration

### ip irdp multicast (for a VLAN)

---

Specify if multicast advertisements are sent.

#### Syntax

- **default ip irdp multicast**
- **default ip irdp vlan <1-4059> multicast**
- **ip irdp multicast**
- **ip irdp vlan <1-4059> multicast**
- **no ip irdp multicast**
- **no ip irdp vlan <1-4059> multicast**

#### Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

#### Default

The default is enabled (true).

## Command Mode

VLAN Interface Configuration

### ip irdp preference (for a VLAN)

---

Specify the preference (a higher number indicates more preferred) of the address as a default router address relative to other router addresses on the same subnet.

#### Syntax

- **default ip irdp preference**
- **default ip irdp vlan <1-4059> preference**
- **ip irdp preference <-2147483648-2147483647>**
- **ip irdp vlan <1-4059> preference <-2147483648-2147483647>**

## Command Parameters

<1-4059>

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

<-2147483648-2147483647>

Specifies the preference value.

## Default

The default is 0.

## Command Mode

VLAN Interface Configuration

---

## ip ospf advertise-when-down enable (for a VLAN)

Enable or disable AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. When you configure a VLAN with no link and enable advertise-when-down, the route is not advertised until the VLAN is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

## Syntax

- **default ip ospf advertise-when-down enable**
- **ip ospf advertise-when-down enable**
- **no ip ospf advertise-when-down enable**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

---

## ip ospf area (for a VLAN)

Configure OSPF parameters on a VLAN to control how OSPF behaves.

## Syntax

- **default ip ospf area**
- **ip ospf area {A.B.C.D}**
- **no ip ospf area**

## Command Parameters

<A.B.C.D>

Configures the OSPF identification number for the area, typically formatted as an IP address.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip ospf authentication-key (for a VLAN)

Configure the eight-character simple password authentication key for the VLAN.

## Syntax

- **ip ospf authentication-key WORD<0-8>**

## Command Parameters

WORD<0-8>

Specifies the authentication key.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip ospf authentication-type (for a VLAN)

Configure the OSPF authentication type for the VLAN. If you choose simple, you must configure the password with the ip ospf authentication-key WORD<0-8> command. If you choose MD5, you must configure the MD5 key with the ip ospf message-digest-key <1-255> md5 WORD<0-16> command.



## Syntax

- **default ip ospf authentication-type**
- **ip ospf authentication-type message-digest**
- **ip ospf authentication-type none**
- **ip ospf authentication-type sha-1**
- **ip ospf authentication-type sha-2**
- **ip ospf authentication-type simple**
- **no ip ospf authentication-type**

## Command Parameters

### message-digest

Configures the authentication-type to message-digest. If you choose MD5, you must configure the MD5 key with the `ip ospf message-digest-key <1-255> md5 WORD<0-16>` command. Message Digest 5 (MD5) provides standards-based authentication using 128-bit encryption. If you use MD5, each OSPF packet has a message digest appended to it. The digest must match between sending and receiving routers, or the packet is discarded.

### none

Configures the authentication-type to none.

### sha-1

Configures the authentication-type to secure hash algorithm 1 (SHA-1). SHA-1 provides standards-based authentication using 128-bit encryption.

### sha-2

sha-2—Specifies SHA-2, which offers the hash function SHA-256.



#### Note

The command parameter sha-2, an update of SHA-1, can offer six hash functions that include SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA 512/256, with hash values that are 224, 256, 384, or 512 bits. However, the current release supports only SHA-256.

### simple

Configures the authentication-type to simple, which is a simple-text password. Only routers that contain the same authentication ID in their LSA can communicate with each other. Using a simple-text password is not a best practice for security. If you choose simple, you must configure the password with the `ip ospf authentication-key WORD<0-8>` command.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip ospf bfd

---

Enable Bidirectional Forwarding Detection (BFD) for an OSPF VLAN interface.

### Syntax

- **ip ospf bfd**
- **ip ospf bfd disable**

### Default

The default is disable.

### Command Mode

VLAN Interface Configuration

---

## ip ospf cost (for a VLAN)

---

Configure the OSPF cost associated with this interface and advertised in router link advertisements.

### Syntax

- **default ip ospf cost**
- **ip ospf cost <0-65535>**

### Command Parameters

<1-65535>

Specifies the cost range.

### Default

The default is 0.

### Command Mode

VLAN Interface Configuration

---

## ip ospf dead-interval (for a VLAN)

---

Configure the router OSPF dead interval-the number of seconds the OSPF neighbors of a switch must wait before assuming that the OSPF router is down. The value must be at least four times the Hello interval.

## Syntax

- **default ip ospf dead-interval**
- **ip ospf dead-interval <0-2147483647>**

## Command Parameters

<0-2147483647>

Specifies the number of seconds the OSPF neighbors of a switch must wait before assuming that the OSPF router is down. The value must be at least four times the Hello interval.

## Default

The default is 40.

## Command Mode

VLAN Interface Configuration

---

## ip ospf digest-key (for a VLAN)

Configure the Digest algorithm key which can be of type MD5, SHA-1 or SHA-2. At most, you can configure two digest keys for an interface.

## Syntax

- **default ip ospf digest-key <1-255>**
- **ip ospf digest-key <1-255> key WORD<0-16>**
- **no ip ospf digest-key <1-255>**

## Command Parameters

<1-255>

Specifies the ID for the digest key.

<WORD> <0-16>

Specifies an alphanumeric password of up to 16 bytes (string length 0 to 16).

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip ospf enable (for a VLAN)

---

Enable OSPF on the VLAN.

### Syntax

- **default ip ospf enable**
- **ip ospf enable**
- **no ip ospf**
- **no ip ospf enable**

### Default

The default is disabled.

### Command Mode

VLAN Interface Configuration

---

## ip ospf hello-interval (for a VLAN)

---

Configure the OSPF Hello interval, which is the number of seconds between Hello packets sent on this interface.

### Syntax

- **default ip ospf hello-interval**
- **ip ospf hello-interval <1-65535>**

### Command Parameters

<1-65535>

Specifies the Hello interval range in seconds. Dead Interval must be a multiple of Hello Interval.

### Default

The default is 10.

### Command Mode

VLAN Interface Configuration

---

## ip ospf mtu-ignore enable (for a VLAN)

---

Enable maximum transmission unit (MTU) ignore. To allow the switch to accept OSPF database description (DBD) packets with a different MTU size, enable mtu-ignore. Incoming OSPF DBD packets are dropped if their MTU is greater than 1500 bytes.

### Syntax

- **default ip ospf mtu-ignore enable**
- **ip ospf mtu-ignore enable**
- **no ip ospf mtu-ignore enable**

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip ospf network (for a VLAN)

---

Specify the type of OSPF interface.

### Syntax

- **default ip ospf network**
- **ip ospf network { broadcast | nbma | passive }**

### Command Parameters

<broadcast|nbma|passive>

Specifies the interface type.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip ospf poll-interval (for a VLAN)

---

Configure the OSPF poll interval in seconds.

## Syntax

- **default ip ospf poll-interval**
- **ip ospf poll-interval <0-2147483647>**

## Command Parameters

<0-2147483647>

Specifies the poll interval range in seconds.

## Default

The default is 120.

## Command Mode

VLAN Interface Configuration

---

## ip ospf primary-digest-key (for a VLAN)

Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the new digest key.

## Syntax

- **default ip ospf primary-digest-key**
- **ip ospf primary-digest-key <1-255>**

## Command Parameters

<1-255>

Specifies the primay md5 key range.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip ospf priority (for a VLAN)

Configure the OSPF priority for the VLAN during the election process for the designated router. The VLAN with the highest priority number is the best candidate for the designated router. If you configure the priority to 0, the VLAN cannot become either the designated router or a backup designated router.

## Syntax

- **default ip ospf priority**
- **ip ospf priority <0-255>**

## Command Parameters

<0-255>

Specifies the priority range.

## Default

The default is 1.

## Command Mode

VLAN Interface Configuration

---

## ip ospf retransmit-interval (for a VLAN)

Configure the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions.

## Syntax

- **default ip ospf retransmit-interval**
- **ip ospf retransmit-interval <0-3600>**

## Command Parameters

<0-3600>

Specifies the retransmit interval range in seconds.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ip ospf transit-delay (for a VLAN)

Configure the transit delay for the virtual interface, which is the estimated number of seconds required to transmit a link-state update over the interface.

## Syntax

- **default ip ospf transit-delay**
- **default ip ospf transit-delay cost**
- **default ip ospf transit-delay mtu-ignore enable**
- **default ip ospf transit-delay priority**
- **ip ospf transit-delay <0-3600>**
- **ip ospf transit-delay <0-3600> cost <0-65535>**
- **ip ospf transit-delay <0-3600> mtu-ignore enable**
- **ip ospf transit-delay <0-3600> priority <0-255>**

## Command Parameters

### <0-3600>

Specifies the transit delay range.

### cost <0-65535>

Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. The default is 1.

### mtu-ignore enable

Enables maximum transmission unit (MTU) ignore. To allow the switch to accept OSPF database description (DBD) packets with a different MTU size, enable mtu-ignore. Incoming OSPF DBD packets are dropped if their MTU is greater than 1500 bytes.

### priority <0-255>

Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The default is 1.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip ospf vlan (for a VLAN)

---

Configure OSPF on a VLAN.



## Syntax

- **default ip ospf vlan <1-4059>**
- **ip ospf vlan <1-4059> advertise-when-down enable**
- **ip ospf vlan <1-4059> area {A.B.C.D}**
- **ip ospf vlan <1-4059> authentication-key WORD<0-8>**
- **ip ospf vlan <1-4059> authentication-type message-digest**
- **ip ospf vlan <1-4059> authentication-type none**
- **ip ospf vlan <1-4059> authentication-type simple**
- **ip ospf vlan <1-4059> cost <0-65535>**
- **ip ospf vlan <1-4059> dead-interval <0-2147483647>**
- **ip ospf vlan <1-4059> enable**
- **ip ospf vlan <1-4059> hello-interval <1-65535>**
- **ip ospf vlan <1-4059> mtu-ignore enable**
- **ip ospf vlan <1-4059> network { broadcast | nbma | passive }**
- **ip ospf vlan <1-4059> poll-interval <0-2147483647>**
- **ip ospf vlan <1-4059> primary-md5-key <1-255>**
- **ip ospf vlan <1-4059> priority <0-255>**
- **ip ospf vlan <1-4059> retransmit-interval <0-3600>**
- **ip ospf vlan <1-4059> transit-delay <0-3600>**
- **no ip ospf vlan <1-4059>**

## Command Parameters

**<1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

### **advertise-when-down enable**

Enables or disables AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. When you configure a VLAN with no link and enable advertise-when-down, the route is not advertised until the VLAN is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled. The default is disabled.

### **area {A.B.C.D}**

Configures OSPF parameters on a VLAN to control how OSPF behaves.

### **authentication-key WORD<0-8>**

Configures the eight-character simple password authentication key for the VLAN.

### **authentication-type**

Configures the OSPF authentication type for the VLAN. If simple, all OSPF updates the interface receives must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key. The default is none.

**cost <0-65535>**

Configures the OSPF cost associated with this interface and advertised in router link advertisements. The default is 0.

**dead-interval <0-2147483647>**

Configures the router OSPF dead interval-the number of seconds the OSPF neighbors of a switch must wait before assuming that the OSPF router is down. The value must be at least four times the Hello interval. The default is 40.

**enable**

Enables OSPF on the VLAN. The default is disabled.

**hello-interval <1-65535>**

Configures the OSPF Hello interval, which is the number of seconds between Hello packets sent on this interface. The default is 10.

**mtu-ignore enable**

Enables maximum transmission unit (MTU) ignore. To allow the switch to accept OSPF database description (DBD) packets with a different MTU size, enable mtu-ignore. Incoming OSPF DBD packets are dropped if their MTU is greater than 1500 bytes.

**network { broadcast | nbma | passive }**

Specifies the type of OSPF interface.

**poll-interval <0-2147483647>**

Configures the OSPF poll interval in seconds. The default is 120.

**primary-md5-key <1-255>**

Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the new message digest key.

**priority <0-255>**

Configures the OSPF priority for the VLAN during the election process for the designated router. The VLAN with the highest priority number is the best candidate for the designated router. If you configure the priority to 0, the VLAN cannot become either the designated router or a backup designated router. The default is 1.

**retransmit-interval <0-3600>**

Configures the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions.

**transit-delay <0-3600>**

Configures the transit delay for the virtual interface, which is the estimated number of seconds required to transmit a link-state update over the interface.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip pim (for a VLAN)

---

Enable PIM on the specified VLAN.

### Syntax

- **default ip pim enable**
- **default ip pim hello-interval**
- **default ip pim join-prune-interval**
- **ip pim active**
- **ip pim enable**
- **ip pim hello-interval <0-18724>**
- **ip pim join-prune-interval <1-18724>**
- **ip pim passive**
- **no ip pim enable**

### Command Parameters

#### active

Enable PIM and configure the interface type to active or passive to perform multicasting operations.

#### enable

Configure PIM for each interface to enable the interface to perform multicasting operations.

#### hello-interval <0-18724>

Specify how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches.

#### join-prune-interval <1-18724>

Specify how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors.

#### passive

Enable PIM and Configure the interface type to passive simultaneously. By default, an enabled interface is active.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip pim bsr-candidate preference (for a VLAN)

---

Configure additional routers as candidate BSRs (C-BSR) to provide backup protection in the event that the primary BSR fails.

### Syntax

- **default ip pim bsr-candidate**
- **ip pim bsr-candidate preference <0-255>**
- **no ip pim bsr-candidate**

### Command Parameters

**preference <0-255>**

Configure additional routers as candidate BSRs (C-BSR) to provide backup protection in the event that the primary BSR fails.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip pim interface-type (for a VLAN)

---

Specify whether the selected interface is active or passive. You can change the state of a PIM interface after you create the interface but only if you disable PIM on the interface. An active interface accepts PIM control transmitted and received traffic. A passive interface prevents PIM control traffic from transmitting or receiving, thereby reducing the load on a system. Use this feature when a high number of PIM interfaces exist and connect to end users, not to other switches.

### Syntax

- **default ip pim interface-type**
- **ip pim interface-type active**
- **ip pim interface-type passive**

### Command Parameters

**<active|passive>**

Specifies the interface type.

## Default

The default is active.

## Command Mode

VLAN Interface Configuration

## ip rip advertise-when-down enable (for a VLAN)

---

Enable or disable AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

## Syntax

- **default ip rip advertise-when-down enable**
- **ip rip advertise-when-down enable**
- **no ip rip advertise-when-down enable**

## Command Parameters

<enable|disable>

Enables or disables AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip rip auto-aggregation enable (for a VLAN)

---

Enable or disable automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disabled.

## Syntax

- **default ip rip auto-aggregation enable**

- **ip rip auto-aggregation enable**
- **no ip rip auto-aggregation enable**

## Command Parameters

### enable

Enables or disables automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disabled.

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip rip cost (for a VLAN)

---

Configure the RIP cost for this port (link).

## Syntax

- **default ip rip cost**
- **ip rip cost <1-15>**

## Command Parameters

<1-15>

Configures the RIP cost for this interface.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip rip default-listen enable (for a VLAN)

---

Enable default listen: the switch accepts the default route learned through RIP on this interface. The default is disabled.

## Syntax

- **default ip rip default-listen enable**
- **ip rip default-listen enable**
- **no ip rip default-listen enable**

## Command Parameters

### enable

Enables DefaultListen: the switch accepts the default route learned through RIP on this interface. The default is disabled.

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

---

## ip rip default-supply enable (for a VLAN)

---

Enable default supply. If enabled, a default route must be advertised from this interface. The default is false. The default route is advertised only if it exists in the routing table. The default route will not be advertised on RIP interfaces by default. You need to redistribute the default route, and then configure the default-supply at the interface for the default route to be advertised to the neighbor.

## Syntax

- **default ip rip default-supply enable**
- **ip rip default-supply enable**
- **no ip rip default-supply enable**

## Command Parameters

### enable

Enables DefaultSupply. If enabled, a default route must be advertised from this interface. The default is false. The default route is advertised only if it exists in the routing table.

## Default

The default is false.

## Command Mode

VLAN Interface Configuration

---

## ip rip enable (for a VLAN)

---

Enable RIP routing on the interface.

### Syntax

- **ip rip enable**
- **no ip rip enable**

### Command Parameters

**enable**

Enables RIP routing on the interface.

### Default

The default is disabled.

### Command Mode

VLAN Interface Configuration

---

## ip rip holddown (for a VLAN)

---

Configure the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.

### Syntax

- **default ip rip holddown**
- **ip rip holddown <0-360>**

### Command Parameters

**<0-360>**

Configures the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.

### Default

The default is 120.

### Command Mode

VLAN Interface Configuration



---

## ip rip in-policy (for a VLAN)

---

Configure the port RIP in-policy. The policy name for inbound filtering on this RIP interface. This policy determines whether to learn a route on this interface. It also specifies the parameters of the route when it is added to the routing table.

### Syntax

- **default ip rip in-policy**
- **ip rip in-policy WORD<0-64>**

### Command Parameters

**WORD<0-64>**

Configures the port RIP in-policy. The policy name for inbound filtering on this RIP interface. This policy determines whether to learn a route on this interface. It also specifies the parameters of the route when it is added to the routing table.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip rip listen enable (for a VLAN)

---

If enabled, the switch listens for a default route without listening for all routes. Specify that the routing switch learns RIP routes through this interface. The default is enable.

### Syntax

- **default ip rip listen enable**
- **ip rip listen enable**
- **no ip rip listen enable**

### Default

The default is enabled.

### Command Mode

VLAN Interface Configuration

---

## ip rip out-policy (for a VLAN)

---

Configure the port RIP out-policy. The policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also Specify the parameters of the advertisement. policy name is a string of length 0 to 64 characters.

### Syntax

- **default ip rip out-policy**
- **ip rip out-policy WORD<0-64>**

### Command Parameters

WORD<0-64>

Configures the port RIP out-policy. The policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also specifies the parameters of the advertisement. policy name is a string of length 0 to 64 characters.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ip rip poison enable (for a VLAN)

---

Enable Poison Reverse. If you disable Poison Reverse (no poison enable), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an immediate neighbor are not advertised back to the neighbor. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. These mechanisms prevent routing loops.

### Syntax

- **default ip rip poison enable**
- **ip rip poison enable**
- **no ip rip poison enable**

### Command Parameters

enable

Enables Poison Reverse. If you disable Poison Reverse (no poison enable), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an

immediate neighbor are not advertised back to the neighbor. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. These mechanisms prevent routing loops.

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip rip receive version (for a VLAN)

---

Indicate which RIP update version is accepted on this interface. The default is rip1orrip2.

## Syntax

- **default ip rip receive version**
- **ip rip receive version { rip1 | rip2 | rip1orrip2 }**

## Command Parameters

<rip1|rip2|rip1orrip2>

Indicates which RIP update version is accepted on this interface. The default is rip1orrip2.

## Default

The default is rip1orrip 2.

## Command Mode

VLAN Interface Configuration

## ip rip send (for a VLAN)

---

Indicate which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible

## Syntax

- **ip rip send version { notsend | rip1 | rip1comp | rip2 }**
- **ip rip send version { notsend | rip1 | rip1comp | rip2 } timeout <15-259200>**

## Command Parameters

<notsend|rip1|rip2|rip1comp|rip2>

Indicates which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible

## Default

The default is rip1Compatible.

## Command Mode

VLAN Interface Configuration

---

## ip rip supply (for a VLAN)

Specify that the switch advertises RIP routes through the port. The default is enable.

## Syntax

- **default ip rip supply enable**
- **ip rip supply enable**
- **no ip rip supply enable**

## Command Parameters

<enable|disable>

Specifies that the switch advertises RIP routes through the port. The default is enable.

## Default

The default is enabled.

## Command Mode

VLAN Interface Configuration

---

## ip rip timeout (for a VLAN)

Configure the RIP timeout interval in seconds.

## Syntax

- **ip rip timeout <15-259200>**

## Command Parameters

<15-259200>

Configures the RIP timeout interval in seconds.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip rip triggered (for a VLAN)

---

Enable automatic triggered updates for RIP.

## Syntax

- **default ip rip triggered enable**
- **ip rip triggered enable**
- **no ip rip triggered enable**

## Command Parameters

**enable**

Enables automatically triggered updates for RIP.

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip rsmlt

---

Configure Routed Split MultiLink Trunking (RSMLT) on an IPv4 VLAN interface.

## Syntax

- **default ip rsmlt**
- **default ip rsmlt holddown-timer**
- **default ip rsmlt holddown-timer holdup-timer**
- **default ip rsmlt holdup-timer**

- **ip rsmlt**
- **ip rsmlt holddown-timer <0-3600>**
- **ip rsmlt holddown-timer <0-3600> holdup-timer <0-9999>**
- **ip rsmlt holdup-timer <0-9999>**
- **no ip rsmlt**

## Command Parameters

### holddown-timer<0-3600>

Defines how long the RSMLT switch does not participate in Layer 3 forwarding. <0-3600> is the timer value in seconds. Configure this value to be longer than the anticipated routing protocol convergence. The default holddown timer is 60.

### holdup-timer<0-3600|9999>

Defines how long the RSMLT switch maintains forwarding for its peer. 0-3600 is the timer value in seconds. 9999 means infinity. The default holdup timer is 1800.

## Default

None

## Command Mode

VLAN Interface Configuration

## ip spb-multicast enable (for a VLAN)

---

Enables Layer 3 VSN IP multicast over SPBM.

## Syntax

- **default ip spb-multicast enable**
- **ip spb-multicast enable**
- **no ip spb-multicast enable**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip spb-pim-gw enable (for a VLAN)

---

Enable SPB-PIM Gateway on a VLAN interface.

## Syntax

- `default p spb-pim-gw enable`
- `ip spb-pim-gw enable`
- `no ip spb-pim-gw enable`

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ip spb-pim-gw hello-interval (for a VLAN)

---

Configures the SPB-PIM Gateway VLAN HELLO interval.

## Syntax

- `default ip spb-pim-gw hello-interval <0-18724>`
- `ip spb-pim-gw hello-interval <0-18724>`
- `no ip spb-pim-gw hello-interval <0-18724>`

## Command Parameters

<0-18724>

Specifies the HELLO interval in seconds. The default value is 30 seconds.

## Default

The default value is 30 seconds.

## Command Mode

VLAN Interface Configuration

## ip spb-pim-gw ip join-prune-interval (for a VLAN)

---

Configures the SPB-PIM Gateway VLAN JOIN PRUNE interval.

## Syntax

- `default ip spb-pim-gw ip join-prune-interval <1-18724>`
- `ip spb-pim-gw ip join-prune-interval <1-18724>`
- `no ip spb-pim-gw ip join-prune-interval <1-18724>`

## Command Parameters

<1-18724>

Specifies the JOIN PRUNE interval in seconds. The default value is 60 seconds.

## Default

The default value is 60 seconds.

## Command Mode

VLAN Interface Configuration

## ip vrrp (for a VLAN)

---

Configure Virtual Router Redundancy Protocol (VRRP) on a VLAN.

## Syntax

- **default ip vrrp <1-255>**
- **default ip vrrp <1-255> action**
- **default ip vrrp <1-255> adver-int**
- **default ip vrrp <1-255> backup-master enable**
- **default ip vrrp <1-255> critical-ip enable**
- **default ip vrrp <1-255> critical-ip-addr**
- **default ip vrrp <1-255> fast-adv enable**
- **default ip vrrp <1-255> fast-adv-int**
- **default ip vrrp <1-255> holddown-timer**
- **default ip vrrp <1-255> priority**
- **default ip vrrp <1-255> enable**
- **default ip vrrp address <1-255>**
- **default ip vrrp address <1-255> {A.B.C.D}**
- **ip vrrp <1-255> action none**
- **ip vrrp <1-255> action preempt**
- **ip vrrp <1-255> adver-int <1-255>**
- **ip vrrp <1-255> backup-master enable**
- **ip vrrp <1-255> critical-ip enable**
- **ip vrrp <1-255> critical-ip-addr {A.B.C.D}**
- **ip vrrp <1-255> enable**
- **ip vrrp <1-255> fast-adv enable**
- **ip vrrp <1-255> fast-adv-int <200-1000>**
- **ip vrrp <1-255> holddown-timer <0-21600>**



- **ip vrrp <1-255> priority <1-255>**
- **ip vrrp <1-255> enable**
- **ip vrrp address <1-255> {A.B.C.D}**
- **no ip vrrp <1-255>**
- **no ip vrrp <1-255> backup-master enable**
- **no ip vrrp <1-255> critical-ip enable**
- **no ip vrrp <1-255> enable**
- **no ip vrrp <1-255> fast-adv enable**
- **no ip vrrp address <1-255>**
- **no ip vrrp address <1-255> {A.B.C.D}**

## Command Parameters

### **action {none|preempt}**

Manually overrides the hold-down timer and force preemption. none|preempt can be set to preempt the timer or set to none to allow the timer to keep working.

### **address <1-255> <A.B.C.D>**

Sets the IP address of the Virtual Router Redundancy Protocol (VRRP) interface that forwards packets to the virtual IP addresses associated with the virtual router. A.B.C.D is the IP address of the master VRRP.

### **adver-int <1-255>**

Sets the the time interval between sending Virtual Router Redundancy Protocol (VRRP) advertisement messages. The range is between 1 and 255 seconds. This value must be the same on all of the participating routers. The default is 1.

### **backup-master enable**

Enables the Virtual Router Redundancy Protocol (VRRP) backup master. This option is supported only on Split MultiLink Trunking (SMLT) ports. Do not enable Backup Master if Critical IP is enabled.

### **critical-ip enable**

Enables the critical IP address option. Do not enable Critical IP if Backup Master is enabled.

### **critical-ip-addr <A.B.C.D>**

Sets the critical IP address for Virtual Router Redundancy Protocol (VRRP). A.B.C.D is the IP address on the local router, which is configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface goes down).

### **enable**

Enables Virtual Router Redundancy Protocol (VRRP) on the interface.

### **fast-adv enable**

Enables the Fast Advertisement Interval. The default is disabled.

### **fast-adv-int <200-1000>**

Sets the Fast Advertisement Interval, in milliseconds, the time interval between sending Virtual Router Redundancy Protocol (VRRP) advertisement messages. The range must be the same on

all participating routers. The default is 200. You must enter values in multiples of 200 milliseconds.

**holddown-timer<0-21600>**

Modifies the behavior of the Virtual Router Redundancy Protocol (VRRP) failover mechanism by allowing the router enough time to detect the OSPF or RIP routes. 0-21600 is the time interval (in seconds) a router is delayed when changing to master state.

**priority <1-255>**

Sets the port Virtual Router Redundancy Protocol (VRRP) priority. 1-255 is the value used by the VRRP router. The default is 100. Assign the value 255 to the router that owns the IP address associated with the virtual router.

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 bfd (for a VLAN)

---

Enable and configure Bidirectional Forwarding Detection (BFD) on a VLAN.

**Note**

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see [VOSS Feature Support Matrix](#).

## Syntax

- **default ipv6 bfd enable**
- **default ipv6 bfd interval**
- **default ipv6 bfd min-rx**
- **default ipv6 bfd multiplier**
- **default ipv6 bfd vlan**
- **ipv6 bfd enable**
- **ipv6 bfd interval**
- **ipv6 bfd min-rx**
- **ipv6 bfd multiplier**
- **ipv6 bfd vlan**
- **no ipv6 bfd**
- **no ipv6 bfd vlan**

## Command Parameters

### enable

Enable BFD on a VLAN.

### interval

Specifies the transmit interval in milliseconds. The default is 200 ms.

The minimum value for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure the remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.

### min-rx

Specifies the receive interval in milliseconds. The default is 200 ms.

The minimum value for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure the remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.

### multiplier

Specifies the multiplier used to calculate the amount of time BFD waits before it declares a receive timeout. The default is 3.

If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

### vlan <1-4094>

Specifies the VLAN ID in the range of 1-4094.

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ipv6 dhcp-relay (for a VLAN)

---

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command `no ipv6 dhcp-relay` disables DHCP on the interface; it does not delete the entry.

## Syntax

- **default ipv6 dhcp-relay**
- **default ipv6 dhcp-relay fwd-path WORD<0-255>**
- **default ipv6 dhcp-relay max-hop**
- **default ipv6 dhcp-relay remote-id**
- **ipv6 dhcp-relay**
- **ipv6 dhcp-relay fwd-path WORD<0-255>**

- **ipv6 dhcp-relay fwd-path WORD<0-255> enable**
- **ipv6 dhcp-relay fwd-path WORD<0-255> vrid WORD<1-255>**
- **ipv6 dhcp-relay max-hop <1-32>**
- **ipv6 dhcp-relay remoteId**
- **no ipv6 dhcp-relay**
- **no ipv6 dhcp-relay fwd-path WORD<0-255>**
- **no ipv6 dhcp-relay fwd-path WORD<0-255> enable**
- **no ipv6 dhcp-relay remoteId**

## Command Parameters

**max-hop <1-32>**

Configures the maximum number of hops before a BootP/DHCP packet is discarded. The default is 32.

**remoteId**

Enables the Remote ID. The default is disabled.

**vrid WORD<1-255>**

Specifies the ID of the virtual router and is an integer from 1-255.

**WORD<0-255>**

Creates a forwarding path to the Dynamic Host Configuration Protocol (DHCP) server with a mode and a state. WORD<0-255> is the IPv6 address of the server. The default IP address of the relay is the address of the interface. If the relay is a Virtual Router configured on this interface, you must set the vrid. By default, the forwarding path is disabled.

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 fhs nd-inspection enable (for a VLAN)

---

Enables neighbor discovery (ND) inspection on a VLAN.

## Syntax

- **default ipv6 fhs nd-inspection enable**
- **ipv6 fhs nd-inspection enable**
- **no ipv6 fhs nd-inspection enable**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ipv6 fhs snooping dhcp enable (for a VLAN)

---

Enables or disables IPv6 DHCP snooping on a particular VLAN.

## Syntax

- **default ipv6 fhs snooping dhcp enable**
- **ipv6 fhs snooping dhcp enable**
- **no ipv6 fhs snooping dhcp enable**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ipv6 forwarding (for a VLAN)

---

Configure IPv6 forwarding. By default, IPv6 forwarding is globally disabled, which means you can only use local IPv6 connections, and traffic does not traverse an IPv6 network.

## Syntax

- **default ipv6 forwarding**
- **ipv6 forwarding**
- **no ipv6 forwarding**

## Default

By default, forwarding is enabled on an interface. You must enable it globally before the interface configuration takes effect.

## Command Mode

VLAN Interface Configuration

---

## ipv6 interface address (for a VLAN)

---

Configure the IPv6 address for a VLAN.

### Syntax

- **ipv6 interface address WORD<0-255>**
- **no ipv6 interface address WORD<0-255>**

### Command Parameters

WORD<0-255>

Assigns an IPv6 address to the VLAN.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ipv6 interface enable (for a VLAN)

---

Enable IPv6 route advertisement on a VLAN.

### Syntax

- **default ipv6 interface enable**
- **ipv6 interface enable**
- **no ipv6 interface enable**

### Default

The default is disabled.

### Command Mode

VLAN Interface Configuration

---

## ipv6 interface hop-limit (for a VLAN)

---

Configure the maximum number of hops before packets drop.

## Syntax

- **default ipv6 interface hop-limit**
- **ipv6 interface hop-limit <1-255>**
- **ipv6 interface link-local WORD<0-19>**

## Command Parameters

<1-255>

Configures the maximum hops.

## Default

The default is 64 hops.

## Command Mode

VLAN Interface Configuration

---

## ipv6 interface link-local (for a VLAN)

Create a link-local address for the VLAN.

## Syntax

- **ipv6 interface link-local WORD<0-19>**

## Command Parameters

WORD<0-19>

Specifies the 64-bit interface ID used to calculate the actual link-local address.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ipv6 interface mac-offset

Request a MAC for an IPv6 VLAN.

## Syntax

- **ipv6 interface mac-offset <MAC-offset>**

## Command Parameters

*<MAC-offset>*

Specifies a number by which to offset the MAC address from the chassis MAC address. This ensures that each IP address has a different MAC address. If you omit this variable, a unique MAC offset is automatically generated. Different hardware platforms support different ranges. To see which range is available on the switch, use the CLI command completion Help.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ipv6 interface mtu (for a VLAN)

Configure the maximum transmission unit for the VLAN.

## Syntax

- **default ipv6 interface mtu**
- **ipv6 interface mtu <1280-9500>**

## Command Parameters

*<1280-9500>*

Configures the maximum transmission unit for the interface: 1280-1500, 1850, or 9500.

## Default

The default is 1500.

## Command Mode

VLAN Interface Configuration

## Usage Guidelines

The MTU value is not configurable on 5420 Series.

---

## ipv6 interface name (for a VLAN)

Configure an interface description for the VLAN.



## Syntax

- **ipv6 interface name WORD<0-255>**

## Command Parameters

WORD<0-255>

Assigns a descriptive name to the VLAN.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ipv6 interface reachable-time (for a VLAN)

Configure the time a neighbor is considered reachable after receiving a reachability confirmation.

## Syntax

- **default ipv6 interface reachable-time**
- **ipv6 interface reachable-time <1-3600000>**

## Command Parameters

<1-3600000>

Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.

## Default

The default is 30000.

## Command Mode

VLAN Interface Configuration

---

## ipv6 interface retransmit-timer (for a VLAN)

Configure the time, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

## Syntax

- **default ipv6 interface retransmit-timer**
- **ipv6 interface retransmit-timer <1-4294967295>**

## Command Parameters

<1-4294967295>

Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

## Default

The default is 1000.

## Command Mode

VLAN Interface Configuration

## ipv6 ipsec enable (for a VLAN)

---

Enable Internet Protocol Security (IPsec) for IPv6 on a VLAN.

## Syntax

- **default ipv6 ipsec enable**
- **ipv6 ipsec enable**
- **no ipv6 ipsec enable**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ipv6 ipsec policy (for a VLAN)

---

Link an Internet Protocol Security (IPsec) IPv6 policy to a VLAN.

## Syntax

- **default ipv6 ipsec policy WORD<1-32>**
- **ipv6 ipsec policy WORD<1-32>**
- **ipv6 ipsec policy WORD<1-32> dir both**

- **ipv6 ipsec policy WORD<1-32> dir in**
- **ipv6 ipsec policy WORD<1-32> dir out**
- **no ipv6 ipsec policy WORD<1-32> dir both**
- **no ipv6 ipsec policy WORD<1-32> dir in**
- **no ipv6 ipsec policy WORD<1-32> dir out**

## Command Parameters

**dir <both|in|out>**

Specifies the direction to which IPsec applies. Both specifies both ingress and egress traffic, in specifies ingress traffic, and out specifies egress traffic. By default, the direction is both.

**WORD<1-32>**

Specifies the IPsec policy name.

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 mld last-listener-query-interval (for a VLAN)

---

Configure the last listener query interval for the MLD

## Syntax

- **default ipv6 mld last-member-query-interval**
- **ipv6 mld last-listener-query-interval <0-60>**
- **no ipv6 mld last-member-query-interval**

## Command Parameters

**<0-60>**

Indicates the last listener query interval in seconds.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ipv6 mld query-interval (for a VLAN)

---

Configure the query interval for the MLD interface

### Syntax

- **default ipv6 mld query-interval**
- **ipv6 mld query-interval <1-65535>**
- **no ipv6 mld query-interval**

### Command Parameters

<1-65535>

Indicates the frequency at which MLD host query packets transmit on this interface.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ipv6 mld query-max-response (for a VLAN)

---

Configure the query maximum response time for mld interface

### Syntax

- **default ipv6 mld query-max-response**
- **ipv6 mld query-max-response <0-60>**
- **no ipv6 mld query-max-response**

### Command Parameters

<0-60>

Indicates the query maximum response interval time in seconds.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ipv6 mld robust-value (for a VLAN)

---

Configure the MLD robustness

### Syntax

- **default ipv6 mld robust-value**
- **ipv6 mld robust-value <2-255>**
- **no ipv6 mld robust-value**

### Command Parameters

**<2-255>**

Specifies a numerical value for MLD snooping robustness.

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ipv6 mld snooping

---

Enable MLD snooping

### Syntax

- **default ipv6 mld snooping**
- **ipv6 mld snooping**
- **no ipv6 mld snooping**

### Default

None

### Command Mode

VLAN Interface Configuration

---

## ipv6 mld ssm-snoop

---

Enable MLD ssm-snooping

## Syntax

- **default ipv6 mld ssm-snoop**
- **ipv6 mld ssm-snoop**
- **no ipv6 mld ssm-snoop**

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 mld version (for a VLAN)

---

Configure MLD version

## Syntax

- **default ipv6 mld version**
- **ipv6 mld version <1-2>**
- **no ipv6 mld version**

## Command Parameters

<1-2>

Indicates the version of MLD that runs on this interface.

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 nd dad-ns (for a VLAN)

---

Configure the number of neighbor solicitation messages from duplicate address detection.

## Syntax

- **default ipv6 nd dad-ns**
- **ipv6 nd dad-ns <0-600>**
- **ipv6 nd dad-ns <0-600> other-config-flag**

## Command Parameters

<0-600>

Configures the number of neighbor solicitation messages from duplicate address detection. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions.

## Default

The default is 1.

## Command Mode

VLAN Interface Configuration

---

## ipv6 nd hop-limit (for a VLAN)

Configure the hop limit sent in router advertisements.

## Syntax

- **default ipv6 nd hop-limit**
- **ipv6 nd hop-limit <0-255>**
- **no ipv6 nd hop-limit**

## Command Parameters

hoplimit <0-255>

Specifies the current hop limit field sent in router advertisements from this interface. The value must be the current diameter of the Internet. A value of zero indicates that the advertisement does not specify a hop-limit value.

## Default

The default is 64.

## Command Mode

VLAN Interface Configuration

---

## ipv6 nd managed-config-flag (for a VLAN)

Enable M-bit (managed address configuration) on the router.

## Syntax

- **default ipv6 nd managed-config-flag**

- **ipv6 nd managed-config-flag**
- **no ipv6 nd managed-config-flag**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

---

## ipv6 nd other-config-flag (for a VLAN)

Enable the O-bit (other stateful configuration) in the router advertisement. Other stateful configuration autoConfigure received information without addresses.

## Syntax

- **default ipv6 nd other-config-flag**
- **ipv6 nd other-config-flag**
- **no ipv6 nd other-config-flag**

## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

---

## ipv6 nd prefix (for a VLAN)

Configure neighbor discovery prefixes. IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by ARP and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

## Syntax

- **default ipv6 nd prefix WORD<0-255> [no-advertise] [preferred-life] [valid-life]**
- **ipv6 nd prefix WORD<0-255> infinite**
- **ipv6 nd prefix WORD<0-255> no-advertise**
- **ipv6 nd prefix WORD<0-255> preferred-life <0-4294967295>**



- **ipv6 nd prefix WORD<0-255> valid-life <0-4294967295>**
- **no ipv6 nd prefix WORD<0-255> [no-advertise]**

## Command Parameters

### **infinite**

Configures the prefix as infinite.

### **no-advertise**

Removes the prefix from the neighbor advertisement. The default for noadvertise is disabled.

### **preferred-life <0-4294967295>**

Configures the preferred life, in seconds. The valid range is 0-4294967295. The default preferred-life is 604800.

### **valid-life <0-4294967295>**

Configures the valid life, in seconds. The valid range is 0-4294967295. The default valid-life is 2592000.

### **WORD <0-255>**

Specifies the IPv6 address prefix.

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 nd ra-lifetime (for a VLAN)

---

Configure the router lifetime included in router advertisement. Other devices use this information to determine if the router can be reached.

## Syntax

- **default ipv6 nd ra-lifetime**
- **ipv6 nd ra-lifetime <0-9000>**

## Command Parameters

### **<0-9000>**

Configures the router lifetime included in router advertisement. The range is 0 or <4-9000>.

## Default

The default is 1800.

## Command Mode

VLAN Interface Configuration

## ipv6 nd rtr-advert-max-interval (for a VLAN)

---

Configure the maximum time allowed between sending unsolicited multicast router advertisements.

### Syntax

- **default ipv6 nd rtr-advert-max-interval**
- **ipv6 nd rtr-advert-max-interval <4-1800>**

### Command Parameters

<4-1800>

Specifies the maximum interval value.

### Default

The default is 600.

## Command Mode

VLAN Interface Configuration

## ipv6 nd rtr-advert-min-interval (for a VLAN)

---

Configure the minimum time allowed between sending unsolicited multicast router advertisements from the interface.

### Syntax

- **default ipv6 nd rtr-advert-min-interval**
- **ipv6 nd rtr-advert-min-interval <3-1350>**

### Command Parameters

<3-1350>

Configures the minimum time, in seconds.

### Default

The default is 200.

## Command Mode

VLAN Interface Configuration

### ipv6 nd send-ra (for a VLAN)

---

Enable or disables periodic router advertisement messages.

#### Syntax

- **default ipv6 nd send-ra**
- **ipv6 nd send-ra**
- **no ipv6 nd send-ra**

#### Default

The default is enabled.

## Command Mode

VLAN Interface Configuration

### ipv6 ospf (for a VLAN)

---

Configure OSPFv3 on an interface.

#### Syntax

- **default ipv6 ospf**
- **default ipv6 ospf cost**
- **default ipv6 ospf dead-interval**
- **default ipv6 ospf enable**
- **default ipv6 ospf hello-interval**
- **default ipv6 ospf nbma-nbr WORD<0-43>**
- **default ipv6 ospf poll-interval**
- **default ipv6 ospf priority**
- **default ipv6 ospf retransmit-interval**
- **default ipv6 ospf transit-delay**
- **ipv6 ospf cost <0-65535>**
- **ipv6 ospf dead-interval <1-65535>**
- **ipv6 ospf enable**
- **ipv6 ospf hello-interval <1-65535>**
- **ipv6 ospf nbma-nbr WORD<0-43> <0-255>**
- **ipv6 ospf nbma-nbr WORD<0-43> priority <0-255>**

- **ipv6 ospf poll-interval <0-65535>**
- **ipv6 ospf priority <0-255>**
- **ipv6 ospf retransmit-interval <1-1800>**
- **ipv6 ospf transit-delay <1-1800>**
- **no ipv6 ospf**
- **no ipv6 ospf enable**
- **no ipv6 ospf nbma-nbr WORD<0-43>**

## Command Parameters

### **cost <0-65535>**

Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. The default is 1.

### **dead-interval <1-65535>**

Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default is 40.

### **enable**

Enables the OSPF on the IPv6 interface.

### **hello-interval <1-65535>**

Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default is 10.

### **nbma-nbr WORD<0-43>**

Configures an NBMA neighbor. WORD<0-43> specifies the IPv6 address. Use priority <0-255> to change an existing priority value for an NBMA neighbor. Use <0-255> to assign the priority value when you create the neighbor.

### **network <eth | nbma | p2mp | p2p | passive>**

Configures the type of interface as one of the following: eth: broadcast, nbma: NBMA, p2mp: point-to-multipoint, p2p: point-to-point, or passive: passive interface.

### **poll-interval <0-65535>**

Configures the polling interval for the OSPF interface in seconds. The default is 120.

### **priority <0-255>**

Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The default is 1.

### **retransmit-interval <1-1800>**

Specifies the retransmit interval, in seconds, for link-state advertisements. The default is 5.

### **transit-delay <1-1800>**

Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default is 1.

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 ospf area (for a VLAN)

---

Configure an OSPFv3 area on an interface.

## Syntax

- **ipv6 ospf area {A.B.C.D}**
- **ipv6 ospf area {A.B.C.D} cost <0-65535>**
- **ipv6 ospf area {A.B.C.D} dead-interval <1-65535>**
- **ipv6 ospf area {A.B.C.D} hello-interval <1-65535>**
- **ipv6 ospf area {A.B.C.D} network eth**
- **ipv6 ospf area {A.B.C.D} network nbma**
- **ipv6 ospf area {A.B.C.D} network p2mp**
- **ipv6 ospf area {A.B.C.D} network p2p**
- **ipv6 ospf area {A.B.C.D} network passive**
- **ipv6 ospf area {A.B.C.D} priority <0-255>**
- **ipv6 ospf area {A.B.C.D} retransmit-interval <1-1800>**
- **ipv6 ospf area {A.B.C.D} transit-delay <1-1800>**

## Command Parameters

**area {A.B.C.D}**

Creates an IPv6 OSPF area.

**cost <0-65535>**

Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. The default is 1.

**dead-interval <1-65535>**

Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default is 40.

**hello-interval <1-65535>**

Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default is 10.

**network <eth|nbma|p2mp|p2p|passive>**

Configures the type of interface as one of the following: eth: broadcast, nbma: NBMA, p2mp: point-to-multipoint, p2p: point-to-point, or passive: passive interface.

**priority <0-255>**

Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The default is 1.

**retransmit-interval <1-1800>**

Specifies the retransmit interval, in seconds, for link-state advertisements. The default is 5.

**transit-delay <1-1800>**

Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default is 1.

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 ospf bfd

---

Enable Bidirectional Forwarding Detection (BFD) for an OSPF VLAN IPv6 interface.

## Syntax

- **ipv6 ospf bfd**
- **ipv6 ospf bfd disable**

## Default

The default is disable.

## Command Mode

VLAN Interface Configuration

## Usage Guidelines

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipv6 pim enable (for a VLAN)

---

Enable PIM globally on the switch

## Syntax

- `default ipv6 pim enable`
- `ipv6 pim enable`
- `no ipv6 pim enable`

## Default

The default is disabled

## Command Mode

VLAN Interface Configuration

## ipv6 pim hello-interval (for a VLAN)

---

Configure the time between hello messages

## Syntax

- `default ipv6 pim hello-interval`
- `ipv6 pim hello-interval <0-18724>`

## Command Parameters

`<0-18724>`

Specifies the duration in seconds before the PIM router sends out the next hello message to neighboring switches.

## Default

The default is 30 seconds

## Command Mode

VLAN Interface Configuration

## ipv6 pim join-prune-interval (for a VLAN)

---

Configure the interval for join and prune messages

## Syntax

- `default ipv6 pim join-prune-interval`
- `ipv6 pim join-prune-interval <1-18724>`

## Command Parameters

<1-18724>

Specifies the duration in seconds before the PIM router sends out the next join or prune message to its upstream neighbors.

## Default

The default is disabled

## Command Mode

VLAN Interface Configuration

---

## ipv6 rip cost (for a VLAN)

Configure the RIPng cost for this port (link).

## Syntax

- **default ipv6 rip cost**
- **ipv6 rip cost <1-15>**

## Command Parameters

<1-15>

Specifies the cost value.

## Default

None

## Command Mode

VLAN Interface Configuration

---

## ipv6 rip poison enable (for a VLAN)

Enable poison reverse.

## Syntax

- **default ipv6 rip poison enable**
- **ipv6 rip poison enable**
- **no ipv6 rip poison enable**



## Default

The default is disabled.

## Command Mode

VLAN Interface Configuration

## ipv6 vrrp (for a VLAN)

Configure Virtual Router Redundancy Protocol (VRRP) to provide fast failover of a default router for IPv6 LAN hosts. VRRP supports a virtual IPv6 address shared between two or more routers that connect the common subnet to the enterprise network. VRRP for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol.

## Syntax

- **default ipv6 vrrp <1-255> [enable]**
- **default ipv6 vrrp <1-255> accept-mode enable**
- **default ipv6 vrrp <1-255> action**
- **default ipv6 vrrp <1-255> adver-int**
- **default ipv6 vrrp <1-255> backup-master enable**
- **default ipv6 vrrp <1-255> critical-ipv6-addr [critical ipv6 enable]**
- **default ipv6 vrrp <1-255> fast-adv enable [fast-adv-int]**
- **default ipv6 vrrp <1-255> holddown-timer**
- **default ipv6 vrrp <1-255> priority**
- **ipv6 vrrp <1-255> accept-mode enable**
- **ipv6 vrrp <1-255> action none**
- **ipv6 vrrp <1-255> action preempt**
- **ipv6 vrrp <1-255> adver-int <1..40>**
- **ipv6 vrrp <1-255> backup-master enable**
- **ipv6 vrrp <1-255> critical-ipv6 enable**
- **ipv6 vrrp <1-255> critical-ipv6-addr WORD<0-46>**
- **ipv6 vrrp <1-255> enable**
- **ipv6 vrrp <1-255> fast-adv enable**
- **ipv6 vrrp <1-255> fast-adv-int <200-1000>**
- **ipv6 vrrp <1-255> holddown-timer <0-21600>**
- **ipv6 vrrp <1-255> priority <1-255>**
- **no ipv6 vrrp <1-255> [enable]**
- **no ipv6 vrrp <1-255> accept-mode enable**
- **no ipv6 vrrp <1-255> backup-master enable**

- **no ipv6 vrrp <1-255> critical ipv6 enable**
- **no ipv6 vrrp <1-255> fast-adv enable**

## Command Parameters

### <1-255>

Specifies a number that uniquely identifies a virtual router on an interface. The virtual router acts as the default router for one or more assigned addresses.

### accept-mode enable

Controls whether a master router accepts packets addressed to the IPv6 address of the address owner as its own if it is not the IPv6 address owner. The default accept-mode enable is disabled.

### action <none|preempt>

Lists options to override the holddown timer manually and force preemption. None does not override the timer. preempt preempts the timer. This parameter applies only if the holddown timer is active.

### adver-int <1-40>

Specifies the time interval, in seconds, between sending advertisement messages. Only the master router sends advertisements. The default is 1.

### backup-master enable

Uses the backup Virtual Router Redundancy Protocol (VRRP) switch for traffic forwarding. This option reduces the traffic on the IST link. The default backupmaster enable is disabled.

### critical-ip enable

Enables or disables the use of critical IP. When disabled, the Virtual Router Redundancy Protocol (VRRP) ignores the availability of the address configured as critical IP. This address must be a local address. The default critical-ip enable is disabled.

### critical-ip-addr WORD<0-46>

Specifies an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface stops responding.

### enable

Enables IPv6 Virtual Router Redundancy Protocol (VRRP). The default is disabled.

### fast-adv enable

Enables or disables the fast advertisement interval. When disabled, the regular advertisement interval is used. The default is disabled.

### fast-adv-int <200-1000>

Configures the interval between Virtual Router Redundancy Protocol (VRRP) advertisement messages. You must configure the same value on all participating routers. This unit of measure must be in multiples of 200 milliseconds. The default is 200.

### holddown-timer<0-21600>

Configures the amount of time, in seconds, to wait before preempting the current Virtual Router Redundancy Protocol (VRRP) master.

### priority <1-255>

Specifies the priority value used by this Virtual Router Redundancy Protocol (VRRP) router. The value 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default priority is 100.

## Default

None

## Command Mode

VLAN Interface Configuration

## ipv6 vrrp address (for a VLAN)

---

Specify a link-local address to associate with the virtual router. Optionally, you can also assign global unicast IPv6 addresses to associate with the virtual router. Network prefixes for the virtual router are derived from the global IPv6 addresses assigned to the virtual router.

## Syntax

- **default ipv6 vrrp address <1-255>**
- **ipv6 vrrp address <1-255> link-local WORD<0-127>**
- **ipv6 vrrp address <1-255> global WORD<0-225>**
- **no ipv6 vrrp address <1-255>**
- **no ipv6 vrrp address <1-255> global WORD<0-225>**

## Command Parameters

**<1-255>**

Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.

**global WORD<0-225>**

Specifies a global IPv6 address and mask to associate with the virtual router. The range is 0 to 255.

**link-local WORD<0-127>**

Specifies a link-local IPv6 address to associate with the virtual router. The range is 0 to 127.

## Default

None

## Command Mode

VLAN Interface Configuration

## migrate-to-mgmt (for a VLAN)

---

Before upgrading to VOSS Release 8.1.60 or later, you can use this command to designate an existing VLAN interface for use as a Segmented Management Instance. Save the configuration. During the upgrade this migration configuration moves the selected interface from the VOSS routing stack to the management stack for use with management applications.

After upgrading to VOSS Release 8.1.60 or later, you can use this command to move an existing Segmented Management Instance VLAN interface to a different VLAN. Save the configuration. During a reboot the migration configuration moves the selected interface to the management stack for use with management applications.



### Note

Do not migrate an interface used for routing purposes, such as where you configured Layer 3 routing protocols. The selected interface routing configuration is reset during a migration.

### Syntax

- **migrate-to-mgmt**
- **no migrate-to-mgmt**

### Default

None

### Command Mode

VLAN Interface Configuration

## nlb-mode

---

Configure the NLB support on an IP interface to enable or disable the Network Load Balancer (NLB) support.

### Syntax

- **default nlb-mode**
- **nlb-mode multicast**
- **nlb-mode unicast**
- **no nlb-mode**

### Command Parameters

**multicast**

Configures the mode as multicast.

**unicast**

Configures the mode as unicast.

## Default

By default, NLB is disabled.

## Command Mode

VLAN Interface Configuration

## slpp (on a VLAN)

---

Enable the Simple Loop Prevention Protocol (SLPP) globally and for a VLAN to detect a loop and automatically stop it. The VLAN configuration controls the boundary of SLPP-PDU transmission.

## Syntax

- **default slpp**
- **default slpp enable**
- **default slpp tx-interval**
- **no slpp**
- **no slpp enable**
- **no slpp vid <1-4059>**
- **slpp enable**
- **slpp tx-interval <500-5000>**
- **slpp vid <1-4059>**

## Command Parameters

### enable

Enables or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process. If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets. The default is disabled.

### tx-interval <500-5000>

Configures the SLPP packet transmit interval, expressed in milliseconds, in a range from 500-5000. The default is 500.

### vid <1-4059>

Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN. You cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

VLAN Interface Configuration

## vrf (for a VLAN)

---

Associate a VLAN to a Virtual Router Forwarding (VRF) so that the VLAN becomes a member of the VRF instance.

## Syntax

- **no vrf**
- **vrf WORD<1-16>**

## Command Parameters

**vrf WORD<1-16>**

Specifies the VRF name.

## Default

None

## Command Mode

VLAN Interface Configuration



# VRF Router Configuration

---

The following topics document commands available in VRF Router Configuration mode of the command line interface (CLI).

## dvr inject-default-route-disable

---

Disables injection of default routes for a specific VRF instance, on the DvR Controller.

### Syntax

- **default dvr inject-default-route-disable**
- **dvr inject-default-route-disable**
- **no dvr inject-default-route-disable**

### Default

The default is enable

### Command Mode

VRF Router Configuration

## dvr redistribute direct (for a VRF)

---

Enables route redistribution of direct routes on a VRF instance. The route type is internal.

### Syntax

- **dvr redistribute direct enable**
- **dvr redistribute direct metric <0-65535>**
- **dvr redistribute direct route-map**

### Command Parameters

**enable**

Enables route redistribution of direct routes on a VRF instance. The route type is internal.

**metric <0-65535>**

Configures the route redistribution metric for direct routes on a VRF instance.

**route-map**

Configures the route policy for route redistribution of direct routes, on a VRF instance.

**Default**

The default is disable

**Command Mode**

VRF Router Configuration

**dvr redistribute static (for a VRF)**

---

Enables route redistribution of direct routes on a VRF instance. The route type is external.

**Syntax**

- **dvr redistribute static enable**
- **dvr redistribute static metric <0-65535>**
- **dvr redistribute static route-map**

**Command Parameters****enable**

Enables route redistribution of static routes on a VRF instance. The route type is external.

**metric <0-65535>**

Configures the route redistribution metric for static routes on a VRF instance.

**route-map**

Configures the route policy for route redistribution of static routes on a VRF instance.

**Default**

The default is disable

**Command Mode**

VRF Router Configuration

**ip alternative-route (on a VRF)**

---

Enable the alternative route feature for a VRF context.

**Syntax**

- **default ip alternative-route**



- **ip alternative-route**
- **no ip alternative-route**

## Command Parameters

### alternative-route

Enables or disables the Alternative Route feature. The default value is enabled. If the alternative-route parameter is disabled, all existing alternative routes are removed. When the parameter is enabled, all alternative routes are re-added.

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

## ip arp (for a VRF)

---

Configure ARP static entries to modify the ARP parameters on the device. The only way to change a static ARP is to delete the static ARP entry and create a new entry with new information.

## Syntax

- **default ip arp {A.B.C.D}**
- **default ip arp timeout**
- **ip arp {A.B.C.D} 0x00:0x00:0x00:0x00:0x00:0x00 {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**
- **ip arp {A.B.C.D} 0x00:0x00:0x00:0x00:0x00:0x00 {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]} vid <1-4059>**
- **ip arp timeout <1-32767>**
- **no ip arp {A.B.C.D}**

## Command Parameters

**{A.B.C.D}**

Specifies the IP address.

**{slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}**

Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

**{slot[-slot][, ...]}**

Specifies the port that receives the flooding.

**0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC address in hexadecimal format. The MAC address parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive).

**timeout <1-32767>**

Configures the timeout value.

**vid <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

## Default

None

## Command Mode

VRF Router Configuration

## ip as-list (for a VRF)

---

Use an asynchronous (AS) path list to restrict the routing information a router learns or advertises to and from a neighbor. The AS path list acts as a filter that Match AS paths.

## Syntax

- **no ip as-list <1-1024> as-path WORD<0-1536>**
- **no ip as-list <1-1024> memberid <0-65535>**

## Command Parameters

**{ permit | deny }**

Permits or denies access for matching conditions.

**<1-1024>**

Creates the specified AS-path list entry.

**<prefix/len>**

Specifies the IPv4 address and an integer value in the range of 1 to 256.

**advertisemap WORD<0-1536>**

Specifies the route map name for route advertisements.

**as-path WORD<0-1536>**

Specifies an integer value between 0 and 1536 placed within quotation marks " ."

**as-set**

Enables autonomous system (AS) information.

**Attributemap WORD<0-1536>**

Specifies the route map name.

**memberid <0-65535>**

Adds a regular expression entry to the specified AS-path list.

**summaryonly**

Enables the summarization of routes not included in routing updates. This parameter creates the aggregate route and suppresses advertisements of more specific routes to all neighbors. The default value is disable.

**suppress-map WORD<0-1536>**

Specifies the route map name for the suppressed route list.

## Default

None

## Command Mode

VRF Router Configuration

## ip bgp

---

Enables BGP on the VRF.

## Syntax

- **default ip bgp**
- **ip bgp**
- **no ip bgp**

## Default

The default value is disabled.

## Command Mode

VRF Router Configuration

## ip bgp aggregate-address

---

Add or delete an aggregate address in a BGP routing table.

## Syntax

- `default ip bgp aggregate-address WORD <1-256>`
- `default ip bgp aggregate-address WORD <1-256> advertise-map`
- `default ip bgp aggregate-address WORD <1-256> as-set`
- `default ip bgp aggregate-address WORD <1-256> attribute-map`
- `default ip bgp aggregate-address WORD <1-256> summary-only`
- `default ip bgp aggregate-address WORD <1-256> suppress-map`
- `ip bgp aggregate-address WORD <1-256>`
- `ip bgp aggregate-address WORD <1-256> advertise-map WORD<0-1536>`
- `ip bgp aggregate-address WORD <1-256> as-set`
- `ip bgp aggregate-address WORD <1-256> attribute-map WORD<0-1536>`
- `ip bgp aggregate-address WORD <1-256> summary-only`
- `ip bgp aggregate-address WORD <1-256> suppress-map WORD<0-1536>`
- `no ip bgp aggregate-address WORD <1-256>`
- `no ip bgp aggregate-address WORD <1-256> advertise-map`
- `no ip bgp aggregate-address WORD <1-256> as-set`
- `no ip bgp aggregate-address WORD <1-256> attribute-map`
- `no ip bgp aggregate-address WORD <1-256> summary-only`
- `no ip bgp aggregate-address WORD <1-256> suppress-map`

## Command Parameters

### `advertise-map WORD<0-1536>`

Specifies the route map name (any string length between 0 and 64 characters) for route advertisements.

### `as-set`

Enables autonomous system (AS) information.

### `attribute-map WORD <0-1536>`

Specifies the route map name (string length between 0 and 64 characters).

### `summary-only`

Enables the summarization of routes not included in routing updates. This parameter creates the aggregate route and suppresses advertisements of more specific routes to all neighbors. The default value is disable.

### `suppress-map WORD<0-1536>`

Specifies the route map name (string length between 0 and 64 characters) for the suppressed route list.

### `WORD <1-256>`

Specifies the IPv4 or the IPv6 address and an integer value in the range of 1 to 256.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ip bgp aggregation

---

Enable or disable automatic route aggregation on the port. When enabled, the router automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network.

## Syntax

- **default ip bgp aggregation**
- **default ip bgp aggregation enable**
- **ip bgp aggregation**
- **ip bgp aggregation enable**
- **no ip bgp aggregation**
- **no ip bgp aggregation enable**

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ip bgp always-compare-med

---

When enabled, compares multiexit discriminator (MED) attributes from neighbors in different autonomous systems.

## Syntax

- **default ip bgp always-compare-med**
- **ip bgp always-compare-med**
- **no ip bgp always-compare-med**

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

### ip bgp auto-peer-restart enable

---

Enable the process that automatically restarts a connection to a BGP neighbor.

#### Syntax

- **default ip bgp auto-peer-restart**
- **default ip bgp auto-peer-restart enable**
- **ip bgp auto-peer-restart enable**
- **no ip bgp auto-peer-restart**
- **no ip bgp auto-peer-restart enable**

#### Default

The default is enabled.

## Command Mode

VRF Router Configuration

### ip bgp auto-summary

---

Summarize the networks based on class limits after BGP is enabled. (For example, Class A, B, C networks).

#### Syntax

- **default ip bgp auto-summary**
- **ip bgp auto-summary**
- **no ip bgp auto-summary**

#### Default

The default is enabled.

## Command Mode

VRF Router Configuration

### ip bgp debug-screen

---

Display debug messages on the console, or saves them in a log file.

## Syntax

- **default ip bgp debug-screen**
- **ip bgp debug-screen { off | on }**
- **no ip bgp debug-screen**

## Default

The default is off.

## Command Mode

VRF Router Configuration

## ip bgp default local-preference

---

Specifies the default value of the local preference attribute.

## Syntax

- **default ip bgp default local-preference**
- **ip bgp default local-preference <0-2147483647>**
- **no ip bgp default local-preference**

## Command Parameters

<0-2147483647>

Specifies the preference value.

## Default

The default is 0.

## Command Mode

VRF Router Configuration

## ip bgp default-information

---

Enable the advertisement of a default route to peers, if it is present in the routing table.

## Syntax

- **default ip bgp default-information originate**
- **default ip bgp default-information ipv6-originate**
- **ip bgp default-information originate**

- `ip bgp default-information ipv6-originate`
- `no ip bgp default-information originate`
- `no ip bgp default-information ipv6-originate`

## Command Parameters

### originate

Enables the origination default route.

### ipv6-originate

Enables the origination of an IPv6 default route.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ip bgp default-metric

---

Configure a value that is sent to a BGP neighbor to determine the cost of a route a neighbor is using.

## Syntax

- `default ip bgp default-metric`
- `ip bgp default-metric <-1-2147483647>`
- `no ip bgp default-metric`

## Command Parameters

### <-1-2147483647>

Specifies the range of the default metric. A default metric value helps solve the problems associated with redistributing routes that have incompatible metrics.

## Default

The default value is -1.

## Command Mode

VRF Router Configuration



---

## ip bgp deterministic-med enable

---

Enables deterministic MED. Deterministic MED, when enabled, means that the first AS of the multiple paths must be the same.

### Syntax

- `default ip bgp deterministic-med`
- `default ip bgp deterministic-med enable`
- `ip bgp deterministic-med enable`
- `no ip bgp deterministic-med`
- `no ip bgp deterministic-med enable`

### Default

The default is disabled.

### Command Mode

VRF Router Configuration

---

## ip bgp enable

---

Enabled BGP on the VRF.

### Syntax

- `default ip bgp enable`
- `ip bgp enable`
- `no ip bgp enable`

### Default

The default is disabled.

### Command Mode

VRF Router Configuration

---

## ip bgp flap-dampening

---

Enable route suppression for routes that flap on and off.

## Syntax

- **default ip bgp flap-dampening**
- **default ip bgp flap-dampening enable**
- **ip bgp flap-dampening**
- **ip bgp flap-dampening enable**
- **no ip bgp flap-dampening**
- **no ip bgp flap-dampening enable**

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

## ip bgp global-debug mask

---

Display specific debug messages for your global BGP configuration.

## Syntax

- **default ip bgp global-debug mask**
- **ip bgp global-debug mask WORD<1-100>**
- **no ip bgp global-debug mask**

## Default

None

## Command Mode

VRF Router Configuration

## ip bgp ibgp-report-import-rt enable

---

Configure BGP to advertise imported routes to an interior BGP (IBGP) peer. This command enable or disables the advertisement of non-BGP imported routes to other IBGP neighbors.

## Syntax

- **default ip bgp ibgp-report-import-rt enable**
- **ip bgp ibgp-report-import-rt enable**
- **no ip bgp ibgp-report-import-rt enable**

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

# ip bgp ignore-illegal-rtrid enable

---

Overlook an illegal router id after enabling BGP.

## Syntax

- **default ip bgp ignore-illegal-rtrid**
- **default ip bgp ignore-illegal-rtrid enable**
- **ip bgp ignore-illegal-rtrid enable**
- **no ip bgp ignore-illegal-rtrid**
- **no ip bgp ignore-illegal-rtrid enable**

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

# ip bgp multiple-paths

---

Configures the maximum number of equal-cost-paths that are available to a BGP router by limiting the number of equal-cost-paths the routing table can store.

## Syntax

- **ip bgp multiple-paths <1-8>**

## Default

The default is 1.

## Command Mode

VRF Router Configuration

## ip bgp neighbor

---

Configure BGP neighbors for a VRF context.

### Syntax

- `default ip bgp neighbor WORD<0-1536>`
- `default ip bgp neighbor WORD<0-1536> advertisement-interval`
- `default ip bgp neighbor WORD<0-1536> allow-as-in`
- `default ip bgp neighbor WORD<0-1536> as-override`
- `default ip bgp neighbor WORD<0-1536> default-ipv6-originate`
- `default ip bgp neighbor WORD<0-1536> default-originate`
- `default ip bgp neighbor WORD<0-1536> ebgp-multihop`
- `default ip bgp neighbor WORD<0-1536> enable`
- `default ip bgp neighbor WORD<0-1536> in-route-map`
- `default ip bgp neighbor WORD<0-1536> ipv6-in-route-map`
- `default ip bgp neighbor WORD<0-1536> ipv6-max-prefix`
- `default ip bgp neighbor WORD<0-1536> ipv6-out-route-map`
- `default ip bgp neighbor WORD<0-1536> max-prefix`
- `default ip bgp neighbor WORD<0-1536> MD5-authentication enable`
- `default ip bgp neighbor WORD<0-1536> neighbor-debug-mask`
- `default ip bgp neighbor WORD<0-1536> next-hop-self`
- `default ip bgp neighbor WORD<0-1536> out-route-map`
- `default ip bgp neighbor WORD<0-1536> remote-as`
- `default ip bgp neighbor WORD<0-1536> remove-private-as enable`
- `default ip bgp neighbor WORD<0-1536> retry-interval`
- `default ip bgp neighbor WORD<0-1536> send-community`
- `default ip bgp neighbor WORD<0-1536> site-of-origin`
- `default ip bgp neighbor WORD<0-1536> soft-reconfiguration-in enable`
- `default ip bgp neighbor WORD<0-1536> timers`
- `default ip bgp neighbor WORD<0-1536> update-source`
- `default ip bgp neighbor WORD<0-1536> weight`
- `ip bgp neighbor WORD<0-1536>`
- `ip bgp neighbor WORD<0-1536> advertisement-interval <5-120>`
- `ip bgp neighbor WORD<0-1536> allow-as-in <0-10>`
- `ip bgp neighbor WORD<0-1536> as-override`
- `ip bgp neighbor WORD<0-1536> default-ipv6-originate`
- `ip bgp neighbor WORD<0-1536> default-originate`
- `ip bgp neighbor WORD<0-1536> ebgp-multihop`
- `ip bgp neighbor WORD<0-1536> enable`

- ip bgp neighbor WORD<0-1536> in-route-map WORD<0-256>
- ip bgp neighbor WORD<0-1536> ipv6-in-route-map
- ip bgp neighbor WORD<0-1536> ipv6-max-prefix
- ip bgp neighbor WORD<0-1536> ipv6-out-route-map
- ip bgp neighbor WORD<0-1536> max-prefix <0-2147483647>
- ip bgp neighbor WORD<0-1536> MD5-authentication enable
- ip bgp neighbor WORD<0-1536> neighbor-debug-mask WORD<1-100>
- ip bgp neighbor WORD<0-1536> next-hop-self
- ip bgp neighbor WORD<0-1536> out-route-map WORD<0-256>
- ip bgp neighbor WORD<0-1536> peer-group WORD<0-1536>
- ip bgp neighbor WORD<0-1536> remote-as WORD<0-11>
- ip bgp neighbor WORD<0-1536> remove-private-as enable
- ip bgp neighbor WORD<0-1536> retry-interval <1-65535>
- ip bgp neighbor WORD<0-1536> send-community
- ip bgp neighbor WORD<0-1536> site-of-origin <0-65535> <0-2147483647>
- ip bgp neighbor WORD<0-1536> site-of-origin {A.B.C.D} <0-65535>
- ip bgp neighbor WORD<0-1536> soft-reconfiguration-in enable
- ip bgp neighbor WORD<0-1536> timers <0-21845> <0-65535>
- ip bgp neighbor WORD<0-1536> update-source {A.B.C.D}
- ip bgp neighbor WORD<0-1536> weight <0-65535>
- no ip bgp neighbor WORD<0-1536>
- no ip bgp neighbor WORD<0-1536> as-override
- no ip bgp neighbor WORD<0-1536> default-ipv6-originate
- no ip bgp neighbor WORD<0-1536> default-originate
- no ip bgp neighbor WORD<0-1536> ebgp-multihop
- no ip bgp neighbor WORD<0-1536> enable
- no ip bgp neighbor WORD<0-1536> in-route-map
- no ip bgp neighbor WORD<0-1536> ipv6-in-route-map
- no ip bgp neighbor WORD<0-1536> ipv6-max-prefix
- no ip bgp neighbor WORD<0-1536> ipv6-out-route-map
- no ip bgp neighbor WORD<0-1536> MD5-authentication enable
- no ip bgp neighbor WORD<0-1536> neighbor-debug-mask
- no ip bgp neighbor WORD<0-1536> next-hop-self
- no ip bgp neighbor WORD<0-1536> out-route-map
- no ip bgp neighbor WORD<0-1536> peer-group
- no ip bgp neighbor WORD<0-1536> remove-private-as enable
- no ip bgp neighbor WORD<0-1536> send-community
- no ip bgp neighbor WORD<0-1536> site-of-origin

- **no ip bgp neighbor WORD<0-1536> soft-reconfiguration-in enable**
- **no ip bgp neighbor WORD<0-1536> update-source**

## Command Parameters

### **advertisement-interval <5-120>**

Specifies the IP Border Gateway Protocol (BGP) route advertisement interval.

### **allow-as-in <0-10>**

Specifies the IP Border Gateway Protocol (BGP) neighbor allow-as-in.

### **as-override**

Specifies the as-override.

### **default-ipv6-originate**

Enables the IPv6 bgp neighbor default-originate.

### **default-originate**

Specifies the default-originate.

### **ebgp-multihop**

Specifies EBGp-multihop.

### **enable**

Enables the command.

### **in-route-map WORD<0-256>**

Specifies the in-route-map.

### **ipv6-in-route-map**

Specifies the IPv6 in-route-map.

### **ipv6-max-prefix**

Specifies the IPv6 max-prefix.

### **ipv6-out-route-map**

Specifies the IPv6 out-route-map.

### **max-prefix <0-2147483647>**

Specifies the max-prefix.

### **MD5-authentication enable**

Enables the Message Digest 5 (MD5)-authentication.

### **neighbor-debug-mask WORD<1-100>**

Specifies the neighbor-debug-mask.

### **next-hop-self**

Specifies the next-hop-self.

### **out-route-map WORD<0-256>**

Specifies the out-route-map.

### **peer-group WORD<0-1536>**

Specifies the peer group.

**remote-as WORD<0-11>**

Specifies the remote-as.

**remove-private-as enable**

Enables the remote-private-as enable.

**retry-interval <1-65535>**

Specifies the retry-interval.

**send-community**

Specifies the send-community.

**site-of-origin {A.B.C.D} <0-65535>**

Specifies the site-of-origin.

**timers <0-21845> <0-65535>**

Specifies the timers.

**update-source WORD<1-256>**

Specifies the IPv4 or IPv6 address of the update-source.

**weight <0-65535>**

Specifies the weight.

**WORD<0-1536>**

Specifies the neighbor IP address, neighbor IPv6 address, or the neighbor group name.

## Default

None

## Command Mode

VRF Router Configuration

## ip bgp neighbor password

---

Specify the password for IP BGP.

## Syntax

- **default ip bgp neighbor password <nbr\_ipaddr|peer-group-name> WORD<0-1536>**
- **ip bgp neighbor password <nbr\_ipaddr|peer-group-name> WORD<0-1536>**
- **no ip bgp neighbor password <nbr\_ipaddr|peer-group-name> WORD<0-1536>**

## Command Parameters

**<nbr\_ipaddr|peer-group-name>**

Specifies the peer IP address or the peer group name.

**password**

Configures the IP BGP neighbor password.

**WORD<0-1536>**

Specifies a password for IP BGP.

## Default

None

## Command Mode

VRF Router Configuration

## ip bgp network

---

Specify the Interior Gateway Protocol (IGP) network prefixes for Border Gateway Protocol (BGP) to advertise for redistribution.

## Syntax

- **default ip bgp network WORD<1-256>**
- **ip bgp network WORD<1-256>**
- **ip bgp network WORD<1-256> metric <0-65535>**
- **no ip bgp network WORD<1-256>**

## Command Parameters

**WORD<1-256>**

Specifies IGP network prefixes for Border Gateway Protocol (BGP) to advertise for redistribution. This command imports routes into BGP. WORD <1-256> is the IPv4 or IPv6 network address and mask.

**metric <0-65535>**

Corresponds to the multiexit discriminator (MED) BGP attribute for the route.

## Default

None

## Command Mode

VRF Router Configuration



---

## ip bgp no-med-path-is-worst enable

---

Enable Border Gateway Protocol (BGP) to treat an update without a multiexit discriminator (MED) attribute as the worst path.

### Syntax

- **default ip bgp no-med-path-is-worst**
- **default ip bgp no-med-path-is-worst enable**
- **ip bgp no-med-path-is-worst enable**
- **no ip bgp no-med-path-is-worst**
- **no ip bgp no-med-path-is-worst enable**

### Default

The default value is enable.

### Command Mode

VRF Router Configuration

---

## ip bgp quick-start enable

---

Enables the quick-start flag for exponential backoff.

### Syntax

- **default ip bgp quick-start**
- **default ip bgp quick-start enable**
- **ip bgp quick-start enable**
- **no ip bgp quick-start**
- **no ip bgp quick-start enable**

### Default

The default value is enable.

### Command Mode

VRF Router Configuration

---

## ip bgp redistribute

---

Configure and enable redistribution entries to allow a protocol to announce routes of a certain source type, for example, static, RIP, or direct.

## Syntax

- **default ip bgp redistribute** {{direct | dvr | ipv6-direct | ipv6-isis | ipv6-static | isis | ospf | ospfv3 | rip | static} {enable | metric | metric-type | route-map WORD | vrf-src WORD <1-16>}
- **ip bgp redistribute** {{direct | dvr | ipv6-direct | ipv6-isis | ipv6-static | isis | ospf | ospfv3 | rip | static} {enable | metric <0-65535> | metric-type live-metric | route-map WORD<0-64> | vrf-src WORD <1-16>}
- **no ip bgp redistribute** {{direct | dvr | ipv6-direct | ipv6-isis | ipv6-static | isis | ospf | ospfv3 | rip | static} [enable] vrf-src WORD <1-16>

## Command Parameters

### direct

Ip bgp redistribute direct command

### dvr

Ip bgp redistribute dvr command

### enable

Enables the route redistribution instance.

### ipv6-direct

Ip bgp redistribute ipv6-direct command

### ipv6-isis

Ip bgp redistribution ipv6-isis command

### ipv6-static

Ip bgp redistribute ipv6-static command

### isis

Ip bgp redistribute isis command

### metric <0-65535>

Configures the metric to apply to redistributed routes.

### metric-type live-metric

Configures default bgp redistribute direct metric-type value

### ospf

Ip bgp redistribute ospf command

### ospfv3

Ip bgp redistribute ospfv3 command

### rip

Ip bgp redistribute rip command

### route-map WORD<0-64>

Configures the route map to apply to redistributed routes.

**static**

Ip bgp redistribute static command

**vrf-src WORD<1-16>**

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

None

## Command Mode

VRF Router Configuration

## ip bgp router-id {A.B.C.D}

---

Specify the BGP router ID in IP address format.

## Syntax

- **default ip bgp router-id**
- **ip bgp router-id {A.B.C.D}**
- **no ip bgp router-id**

## Command Parameters

{A.B.C.D}

Identifies the router IP address.

## Default

None

## Command Mode

VRF Router Configuration

## ip bgp synchronization

---

Enables the router to accept routes from BGP peers without waiting for an update from the IGP.

## Syntax

- **default ip bgp synchronization**
- **ip bgp synchronization**

- `no ip bgp synchronization`

## Default

The default value is enable.

## Command Mode

VRF Router Configuration

---

## ip bgp traps enable

Enables BGP traps.

## Syntax

- `default ip bgp traps`
- `default ip bgp traps enable`
- `ip bgp traps enable`
- `no ip bgp traps`
- `no ip bgp traps enable`

## Default

The default value is disable.

## Command Mode

VRF Router Configuration

---

## ip bgp vrf-as WORD<0-11>

Configures an autonomous system (AS) number on a particular VRF.

## Syntax

- `default ip bgp vrf-as`
- `ip bgp vrf-as WORD<0-11>`
- `no ip bgp vrf-as`

## Default

The default value is 0. By default, the VRF context will inherit the AS number configured in the BGP Router Configuration mode, but you can use this command to configure a different AS number.

## Command Mode

VRF Router Configuration

### ip community-list (for a VRF)

---

Show the community lists on the VRF Router.

#### Syntax

- **no ip community-list <1-1024>**
- **no ip community-list <1-1024> community-string WORD<0-256>**
- **no ip community-list <1-1024> memberid <0-65535>**

#### Command Parameters

**<permit|deny>**

Sets the access mode, which permits or denies access for matching conditions.

**community-list <1-1024>**

Creates the specified community list entry. <1-1024> specifies the list id.

**community-string WORD<0-256>**

Specifies an alphanumeric string value with a string length of 0 to 1536 characters. This string value is either an AS num: community-value or a well-known community string. Well known communities include: internet no-export no-advertise local-as (known as NO\_EXPORT\_SUBCONFED).

**memberid <0-65535>**

Adds an entry to the community list. <0-65535> is an integer value that represents the member ID in the community list.

#### Default

None

## Command Mode

VRF Router Configuration

### ip dhcp-relay fwd-path (for a VRF)

---

Create the forwarding path from the client to the server.

#### Syntax

- **default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}**
- **default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode**

- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} disable`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} enable`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode bootp`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode bootp_dhcp`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode dhcp`
- `no ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D}`

## Command Parameters

**{A.B.C.D}**

Creates a forwarding path to the Dynamic Host Configuration Protocol (DHCP) server. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface.



### Tip

If the relay is a virtual router configured on this interface, you must set the vrid.

**disable**

Disables the forwarding path.

**enable**

Enables the forwarding path.

**mode <bootp|dhcp|bootp\_dhcp>**

Configures DHCP mode to forward BootP messages only, Dynamic Host Configuration Protocol (DHCP) messages only, or both. The default is both.

## Default

None

## Command Mode

VRF Router Configuration

## ip dhcp-relay fwd-path mode (for a VRF)

Modify Dynamic Host Configuration Protocol (DHCP) mode to forward BootP messages only, DHCP messages only, or both.

## Syntax

- `default ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode bootp`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode bootp_dhcp`
- `ip dhcp-relay fwd-path {A.B.C.D} {A.B.C.D} mode dhcp`

## Command Parameters

<bootp|dhcp|bootp\_dhcp>

Configures DHCP mode to forward BootP messages only, Dynamic Host Configuration Protocol (DHCP) messages only, or both. The default is both.

## Default

The default mode is both.

## Command Mode

VRF Router Configuration

## ip icmp (for a VRF)

---

Enable Internet Control Message Protocol (ICMP) redirect and unreachable messages.

## Syntax

- **default ip icmp**
- **default ip icmp drop-fragments**
- **default ip icmp unreachable**
- **ip icmp unreachable**
- **ip icmp drop-fragments**
- **no ip icmp**
- **no ip icmp drop-fragments**
- **no ip icmp unreachable**

## Command Parameters

**unreachable**

Enables the switch to send Internet Control Message Protocol (ICMP) unreachable messages. When enabled, generates Internet Control Message Protocol (ICMP) network unreachable messages if the destination network is not reachable from this router. These messages help determine if the routing switch is reachable over the network. The default is disabled.

**drop-fragments**

The parameter enables to drop the Fragmented ICMP packet filtering at the switch.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ip icmp echo-broadcast-request (for a VRF)

---

Enables or disables the processing of IPv4 ICMP messages sent to a broadcast address for a non-zero VRF.

## Syntax

- **default ip icmp echo-broadcast-request**
- **ip icmp echo-broadcast-request**
- **no ip icmp echo-broadcast-request**

## Command Parameters

echo broadcast-request

Enables or disables the processing of IPv4 ICMP messages sent to a broadcast address for a non-zero VRF. The default value is enabled.

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

## ip igmp (for a VRF)

---

Configure Internet Group Management Protocol (IGMP) for each interface to change default multicasting operations.

## Syntax

- **default ip igmp ssm-map {A.B.C.D} {A.B.C.D}**
- **default ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]**
- **ip igmp generate-log**
- **ip igmp generate-trap**
- **ip igmp immediate-leave-mode <multiple-user|one-user>**



- **ip igmp ssm [dynamic-learning] [group-range {A.B.C.D/X}]**
- **ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]**
- **ip igmp ssm-map all**
- **no ip igmp ssm-map {A.B.C.D} {A.B.C.D}**
- **no ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]**

## Command Parameters

### **generate-log**

Sets the Internet Group Management Protocol (IGMP) log.

### **generate-trap**

Sets the Internet Group Management Protocol (IGMP) trap.

### **immediate-leave-mode <multiple-user|one-user**

Enables immediate leave mode to users which is either a single user or multiple users.

### **ssm [dynamic-learning] [group-range {A.B.C.D/X}]**

Enables and sets the Source Specific Multicast (SSM) features. The parameter, dynamic-learning enables SSM dynamic learning. The parameter, group range {A.B.C.D/X} configures the range group address and mask. The SSM range parameter extends the default SSM range of 232/8 to include an IP multicast address. You can configure existing applications without having to change their group configurations. This parameter specifies an IP multicast address within the range of 224.0.0.0 and 239.255.255.255. The default is 232.0.0.0. The address mask is the IP address mask of the multicast group. The default is 255.0.0.0.

### **ssm-map all**

Enables the Source Specific Multicast (SSM) map table for all static entries.

### **ssm-map{A.B.C.D} {A.B.C.D}[enable]**

Enables the Source Specific Multicast (SSM) map table for a specific entry or creates a static entry for a specific group. The parameter, {A.B.C.D} {A.B.C.D} creates a static SSM channel table entry by specifying the group and source IP addresses. The first IP address is an IP multicast address within the SSM range. The second IP address is the source IP address and it is an IP host address that sends traffic to the group. The default for {A.B.C.D}{A.B.C.D} enable is enable for each entry. The default is enable for each entry.

### **ssm-map{A.B.C.D}[enable]**

Enables the administrative state for a specific entry (group). This variable does not affect the dynamically-learned entries. This state determines whether the switch uses the static entry or saves it for future use. The default is enable for each entry.

## Default

None

## Command Mode

VRF Router Configuration

---

## ip igmp generate-log (for a VRF)

---

Enables the generation of IGMP log messages.

### Syntax

- **default ip igmp generate-log**
- **ip igmp generate-log**
- **no ip igmp generate-log**

### Default

The default is disabled.

### Command Mode

VRF Router Configuration

---

## ip igmp generate-trap (for a VRF)

---

Enables the generation of IGMP traps.

### Syntax

- **default ip igmp generate-trap**
- **ip igmp generate-trap**
- **no ip igmp generate-trap**

### Default

The default is disabled.

### Command Mode

VRF Router Configuration

---

## ip igmp immediate-leave-mode (for a VRF)

---

Configures the fast leave mode.

### Syntax

- **default ip igmp immediate-leave-mode multiple-user**
- **default ip igmp immediate-leave-mode one-user**
- **ip igmp immediate-leave-mode multiple-user**
- **ip igmp immediate-leave-mode one-user**

- **no ip igmp immediate-leave-mode multiple-user**
- **no ip igmp immediate-leave-mode one-user**

## Command Parameters

### multiple-user

Removes all group members on a fast leave-enabled interface port after receiving the first leave message from a member. This behavior is the same as the conventional fast leave process.

### one-user

Removes from the group only the IGMP member who sent the leave message. Traffic does not stop if other receivers exist on the interface port.

## Default

The default is multiple-user.

## Command Mode

VRF Router Configuration

## ip igmp ssm dynamic-learning (for a VRF)

---

Enables SSM dynamic learning for the VRF.

## Syntax

- **default ip igmp ssm dynamic-learning**
- **ip igmp ssm dynamic-learning**
- **ip igmp ssm dynamic-learning group-range {A.B.C.D/X}**
- **no ip igmp ssm dynamic-learning**

## Command Parameters

### group-range {A.B.C.D/X}

Extends the default SSM range of 232/8 to include an IP multicast address. You can configure existing applications without changing their group configuration.

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

## ip igmp ssm group-range (for a VRF)

---

Extends the default SSM range of 232/8 to include an IP multicast address. You can configure existing applications without changing their group configuration.

### Syntax

- **default ip igmp ssm**
- **ip igmp ssm group-range {A.B.C.D/X}**
- **no ip igmp ssm**

### Command Parameters

{A.B.C.D/X}

Specifies the IP address. The IP address must be within the range of 224.0.0.0 and 239.255.255.255.

### Default

The default IP address is 0.0.0.232. The default mask is 0.0.0.255.

### Command Mode

VRF Router Configuration

## ip igmp ssm-map (for a VRF)

---

Configures the SSM map table to map groups to their sending source.

### Syntax

- **default ip igmp ssm-map {A.B.C.D} {A.B.C.D}**
- **default ip igmp ssm-map {A.B.C.D} {A.B.C.D} enable**
- **default ip igmp ssm-map all**
- **ip igmp ssm-map {A.B.C.D} {A.B.C.D}**
- **ip igmp ssm-map {A.B.C.D} {A.B.C.D} enable**
- **ip igmp ssm-map all**
- **no ip igmp ssm-map {A.B.C.D} {A.B.C.D}**
- **no ip igmp ssm-map {A.B.C.D} {A.B.C.D} enable**
- **no ip igmp ssm-map all**

### Command Parameters

{A.B.C.D} {A.B.C.D}

Enables the SSM map table for a specific entry or creates a static entry for a specific group. {A.B.C.D} {A.B.C.D} creates a static SSM channel table entry by specifying the group and source IP address. The first IP address is an IP multicast address within the SSM range. The second IP address is the source IP address. The source address is an IP host address that sends traffic to the group.

**all**

Enables the SSM map table for all static entries.

**enable**

Enables the static entry.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## Usage Guidelines

Before you disable or delete an ssm-map, always send IGMPv1 or IGMPv2 leave messages from hosts that operate in IGMPv1 or IGMPv2. If you do not perform this action, receiving and processing reports in SSM range on an IGMP interface enabled with IGMPv1 or IGMPv2 can lead to unexpected behavior.

## ip isid-list (for a VRF)

---

Create an I-SID list to use with IS-IS accept policies.

## Syntax

- **ip isid-list WORD<1-32> <0-16777215>**
- **ip isid-list WORD<1-32> list WORD<1-1024>**
- **no ip isid-list WORD<1-32> <0-16777215>**
- **no ip isid-list WORD<1-32> list WORD<1-1024>**

## Command Parameters

**<0-16777215>**

Specifies an I-SID value.

**list WORD<1-1024>**

Specifies a list of I-SID values in one of the following formats (1,3,5,8-10).

**WORD<1-32>**

Specifies a name for the I-SID list.

## Default

None

## Command Mode

VRF Router Configuration

## Usage Guidelines

When creating an I-SID list, you can add I-SID entries until the maximum limit for supported Layer 3 I-SIDs is reached. The system truncates any additional I-SID entries. The maximum limit includes the I-SIDs for locally configured Layer 3 VSNs and the I-SIDs specified for IS-IS accept policy filters.

Use the command **show ip isid-list vrf WORD<1-16>** to view the list of truncated I-SIDs.

When deleting an I-SID list, ensure that the I-SID list is not associated with an IS-IS accept policy. Otherwise the deletion fails. An I-SID list associated with an accept policy cannot be deleted because it must contain at least one constituent I-SID.

## ip mroute resource-usage (for a VRF)

---

Configures the resource usage counters.

## Syntax

- **default ip mroute resource-usage egress-threshold <0-32767>**
- **default ip mroute resource-usage egress-threshold <0-32767> ingress-threshold**
- **default ip mroute resource-usage ingress-threshold <0-32767>**
- **default ip mroute resource-usage log-msg**
- **default ip mroute resource-usage trap-msg**
- **ip mroute resource-usage egress-threshold <0-32767>**
- **ip mroute resource-usage egress-threshold <0-32767> ingress-threshold <0-32767>**
- **ip mroute resource-usage ingress-threshold <0-32767>**
- **ip mroute resource-usage log-msg**
- **ip mroute resource-usage trap-msg**
- **no ip mroute resource-usage egress-threshold <0-32767>**
- **no ip mroute resource-usage egress-threshold <0-32767> ingress-threshold**
- **no ip mroute resource-usage ingress-threshold <0-32767>**
- **no ip mroute resource-usage log-msg**
- **no ip mroute resource-usage trap-msg**

## Command Parameters

### **egress-threshold <0-32767>**

Configures the egress record threshold (S,G). A notification message is sent if this value is exceeded. The default is 0.

### **ingress-threshold <0-32767>**

Configures the ingress record threshold (peps). A notification message is sent if this value is exceeded. The default is 0.

### **log-msg**

Configures the notification method for sending only a log message after the threshold level is exceeded. The default is disabled.

### **log-msg**

Configures the notification method for sending only a log message after the threshold level is exceeded. The default is disabled.

### **trap-msg**

Configures the notification method for sending only a trap message after the threshold level is exceeded. The default is disabled.

### **trap-msg**

Configures the notification method for sending only a trap message after the threshold level is exceeded. The default is disabled.

## Default

None

## Command Mode

VRF Router Configuration

## ip msdp (for a VRF)

---

Create an MSDP instance on a user defined VRF to allow further configuration to take place.

## Syntax

- **ip msdp**

## Default

None

## Command Mode

VRF Router Configuration

---

## ip msdp apply redistribute (for a VRF)

---

Apply MSDP redistribution filters.

### Syntax

- **default ip msdp apply redistribute**
- **ip msdp apply redistribute**
- **no ip msdp apply redistribute**

### Default

None

### Command Mode

VRF Router Configuration

---

## ip msdp connect—retry (for a VRF)

---

Configure the connect-retry period to specify the amount of time, in seconds, between connection attempts for peering sessions.

### Syntax

- **default ip msdp connect—retry {A.B.C.D} <1-65535>**
- **ip msdp connect—retry {A.B.C.D} <1-65535>**
- **no ip msdp connect—retry {A.B.C.D} <1-65535>**

### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

<1-65535>

Specifies the connect-retry interval in seconds. The default is 30 seconds.

### Default

The default is 30 seconds.

### Command Mode

VRF Router Configuration



---

## ip msdp description

---

Configure a peer description to add descriptive text to an MSDP peer for easy identification of a peer.

### Syntax

- **default ip msdp description**
- **ip msdp description {A.B.C.D} WORD<1-255>**
- **no ip msdp description**

### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

WORD<1-255>

Specifies a descriptive text to a MSDP peer in the range of 1-255 characters.

### Default

None

### Command Mode

VRF Router Configuration

---

## ip msdp keepalive (for a VRF)

---

Configure keepalive messages to adjust the interval in seconds at which an MSDP peer sends keep alive messages.

### Syntax

- **default ip msdp keepalive {A.B.C.D} <0-21845> <0-65535>**
- **ip msdp keepalive {A.B.C.D} <0-21845> <0-65535>**
- **no ip msdp keepalive {A.B.C.D} <0-21845> <0-65535>**

### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

<0-21845>

Specifies the keep alive interval in seconds. The default is 60 seconds.

<0-65535>

Specifies the hold time interval in seconds. The default is 75 seconds. 0 seconds means the peer never expires. Values 1 and 2 are not allowed.

## Default

The default is 60 seconds.

## Command Mode

VRF Router Configuration

## ip msdp md5-authentication (for a VRF)

---

Configure Message Digest (MD) 5 authentication to secure control messages on the TCP connection between MSDP peers.

## Syntax

- **default ip msdp md5-authentication**
- **ip msdp md5-authentication**
- **ip msdp md5-authentication {A.B.C.D} [enable]**
- **no ip msdp md5-authentication {A.B.C.D} [enable]**

## Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

**enable**

Enables MD5 authentication.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ip msdp mesh-group (for a VRF)

---

Configure mesh groups to reduce SA flooding. A mesh group does not forward SA messages to other group members.

## Syntax

- **default ip msdp mesh-group WORD<1-64> {A.B.C.D}**

- **ip msdp mesh-group WORD<1-64> {A.B.C.D}**
- **no ip msdp mesh-group WORD<1-64> {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

WORD<1-64>

Specifies the mesh group name.

## Default

None

## Command Mode

VRF Router Configuration

## ip msdp originator-id (for a VRF)

---

Configure the originator ID to set the Rendezvous Point (RP) address inside the Source Active (SA) message.

## Syntax

- **default ip msdp originator-id {A.B.C.D}**
- **ip msdp originator-id {A.B.C.D}**
- **no ip msdp originator-id {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies the MSDP source IP address.

## Default

None

## Command Mode

VRF Router Configuration

## ip msdp password peer (for a VRF)

---

Configure the case sensitive password for MD5 authentication

## Syntax

- **default ip msdp password peer {A.B.C.D}**
- **ip msdp password peer {A.B.C.D} WORD<1-80>**
- **no ip msdp password peer {A.B.C.D} WORD<1-80>**

## Command Parameters

**{A.B.C.D}**

Specifies the MSDP peer IP address.

**WORD<1-80>**

Specifies the MD5 authentication password.

## Default

None

## Command Mode

VRF Router Configuration

---

## ip msdp peer

Configure an MSDP peer to establish a peer relationship between the local MSDP enabled router and a peer in another domain.

## Syntax

- **default ip msdp peer {A.B.C.D}**
- **default ip msdp peer {A.B.C.D} enable**
- **default ip msdp peer {A.B.C.D} remote-as WORD<0-11>**
- **ip msdp peer {A.B.C.D}**
- **ip msdp peer {A.B.C.D} enable**
- **ip msdp peer {A.B.C.D} remote-as WORD<0-11>**
- **no ip msdp peer {A.B.C.D}**
- **no ip msdp peer {A.B.C.D} enable**
- **no ip msdp peer {A.B.C.D} remote-as WORD<0-11>**

## Command Parameters

**{A.B.C.D}**

Specifies the MSDP peer IP address.

**WORD<0-11>**

Specifies the AS number of the MSDP peer, 0-65535 (2-Byte AS) 0-4294967295 (4-Byte AS).

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ip msdp redistribute (for a VRF)

---

Filter SPB routes to filter which (S,G,RP) entries sent out to all MSDP peers.

## Syntax

- **default ip msdp redistribute**
- **ip msdp redistribute**
- **no ip msdp redistribute**

## Default

None

## Command Mode

VRF Router Configuration

## ip msdp redistribute route-policy (for a VRF)

---

Create the route policy name.

## Syntax

- **default ip msdp redistribute route-policy WORD<1-64>**
- **ip msdp redistribute route-policy WORD<1-64>**
- **no ip msdp redistribute route-policy WORD<1-64>**

## Command Parameters

**WORD<1-64>**

Specifies the route policy name.

## Default

None

## Command Mode

VRF Router Configuration

### ip msdp sa-filter in (for a VRF)

---

Create the inbound filter.

#### Syntax

- `default ip msdp sa-filter in {A.B.C.D}`
- `default ip msdp sa-filter in {A.B.C.D} route-policy WORD<1-64>`
- `ip msdp sa-filter in {A.B.C.D}`
- `ip msdp sa-filter in {A.B.C.D} route-policy WORD<1-64>`
- `no ip msdp sa-filter in {A.B.C.D}`
- `no ip msdp sa-filter in {A.B.C.D} route-policy WORD<1-64>`

#### Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

route-policy WORD<1-64>

Specifies the route policy name for an inbound filter.

#### Default

None

## Command Mode

VRF Router Configuration

### ip msdp sa-filter out (for a VRF)

---

Create the outbound filter.

#### Syntax

- `default ip msdp sa-filter out {A.B.C.D}`
- `default ip msdp sa-filter out {A.B.C.D} route-policy WORD<1-64>`
- `ip msdp sa-filter out {A.B.C.D}`
- `ip msdp sa-filter out {A.B.C.D} route-policy WORD<1-64>`
- `ip msdp sa-filter out {A.B.C.D} route-policy WORD<1-64>`
- `no ip msdp sa-filter out {A.B.C.D}`

## Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

route-policy WORD<1-64>

Specifies the route policy name for an outbound filter.

## Default

None

## Command Mode

VRF Router Configuration

## ip msdp sa-limit (for a VRF)

---

Specifies the maximum number of SA messages to keep in SA cache.

## Syntax

- **default ip msdp sa-limit {A.B.C.D} <0-6144>**
- **ip msdp sa-limit {A.B.C.D} <0-6144>**
- **no ip msdp sa-limit {A.B.C.D} <0-6144>**

## Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

<0-6144>

Specifies the maximum number of SA messages to keep in SA cache. The default is 6144 messages.

## Default

The default is 6144.

## Command Mode

VRF Router Configuration

## ip msdp ttl-threshold (for a VRF)

---

Configure the time-to-live (TTL) threshold to limit which multicast data packets the router encapsulated in SA Message forwarded to an MSDP peer.

## Syntax

- **default ip msdp ttl-threshold {A.B.C.D} <1-255>**
- **ip msdp ttl-threshold {A.B.C.D} <1-255>**
- **no ip msdp ttl-threshold {A.B.C.D} <1-255>**

## Command Parameters

{A.B.C.D}

Specifies the MSDP peer IP address.

<1-255>

Specifies the Time-To-Live value. The default is 1.

## Default

The default is 1.

## Command Mode

VRF Router Configuration

---

## ip ospf (for a VRF)

Enables OSPF on the VRF.

## Syntax

- **default ip ospf**
- **ip ospf**
- **no ip ospf**

## Default

The default value is disabled.

## Command Mode

VRF Router Configuration

---

## ip ospf accept adv-rtr

Configures OSPF accept policies for the VRF.



## Syntax

- **default ip ospf accept adv-rtr {A.B.C.D}**
- **default ip ospf accept adv-rtr {A.B.C.D} enable**
- **default ip ospf accept adv-rtr {A.B.C.D} metric-type**
- **default ip ospf accept adv-rtr {A.B.C.D} route-map**
- **ip ospf accept adv-rtr {A.B.C.D}**
- **ip ospf accept adv-rtr {A.B.C.D} enable**
- **ip ospf accept adv-rtr {A.B.C.D} metric-type { type1 | type2 | any }**
- **ip ospf accept adv-rtr {A.B.C.D} route-map WORD<0-64>**
- **no ip ospf accept adv-rtr {A.B.C.D}**
- **no ip ospf accept adv-rtr {A.B.C.D} enable**

## Command Parameters

**{A.B.C.D}**

Specifies the IP address.

**adv-rtr <A.B.C.D>**

Specifies the advertising router IP address.

**enable**

Enables an OSPF accept entry for a specified advertising router.

**metric-type <type1|type2|any>**

OSPF external routes match this entry. any means match all external routes. type1 means match external type 1 only. type2 means match external type 2 only.

**route-map WORD<0-64>**

Specifies the name of the route policy to use for filtering external routes advertised by the specified advertising router before accepting into the routing table.

**vrf WORD<1-16>**

Specifies the configuration for a particular VRF. WORD<1-16> specifies the VRF name.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf admin-state

Shows the administrative status of OSPF for the router. Enabled denotes that the OSPF process is active on at least one interface; disabled disables it for all interfaces.

## Syntax

- `default ip ospf admin-state`
- `ip ospf admin-state`
- `no ip ospf admin-state`

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf area (for a VRF)

---

Configure OSPF parameters on a port to control how OSPF behaves.

## Syntax

- `default ip ospf area {A.B.C.D}`
- `default ip ospf area {A.B.C.D} default-cost`
- `default ip ospf area {A.B.C.D} import`
- `default ip ospf area {A.B.C.D} import-summaries enable`
- `default ip ospf area {A.B.C.D} stub`
- `ip ospf area {A.B.C.D}`
- `ip ospf area {A.B.C.D} default-cost <0-16777215>`
- `ip ospf area {A.B.C.D} import external`
- `ip ospf area {A.B.C.D} import noexternal`
- `ip ospf area {A.B.C.D} import nssa`
- `ip ospf area {A.B.C.D} import-summaries enable`
- `ip ospf area {A.B.C.D} stub`
- `no ip ospf area {A.B.C.D}`
- `no ip ospf area {A.B.C.D} import-summaries enable`

## Command Parameters

`<A.B.C.D>`

Configures the OSPF identification number for the area, typically formatted as an IP address.

`default-cost <0-16777215>`

Stub area default metric for this stub area, which is the cost from 0 to 16 777 215. This is the metric value applied at the indicated type of service.

`import <external|noexternal|nssa>`

Specifies the type of area: external - Stub and NSSA (not so stubby area) are both false.  
noexternal-Configures the area as stub area. nssa - Configures the area as NSSA.

#### import-summaries enable

Configures the area support to import summary advertisements into a stub area. This parameter must be used only if the area is a stub area.

#### stub

Configures the import external option for this area as stub. A stub area has only one exit point (router interface) from the area.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf area range (for a VRF)

Use aggregate area ranges to reduce the number of link-state advertisements that are required within the area. You can also control advertisements.

## Syntax

- **default ip ospf area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-metric**
- **default ip ospf area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-mode**
- **ip ospf area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-metric <0-65535>**
- **ip ospf area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-mode { summarize | suppress | no-summarize }**
- **no ip ospf area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink }**

## Command Parameters

**{A.B.C.D} {A.B.C.D/X}**

<A.B.C.D> identifies an OSPF area and <A.B.C.DX> is the IP address and subnet mask of the range, respectively.

**<summary-link|nssaextlink>**

Specifies the LSA type. If you configure the range as type nssaextlink then you cannot configure the advertise-metric.

**advertise-metric <0-65535>**

Changes the advertised metric cost of the OSPF area range.

**advertise-mode** <summarize|suppress|nosummarize

Changes the advertisement mode of the range.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf area virtual-link (for a VRF)

Enables or disables the automatic creation of virtual links.

## Syntax

- **default ip ospf area virtual-link** {A.B.C.D} {A.B.C.D}
- **default ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **authentication-type**
- **default ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **dead-interval**
- **default ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **hello-interval**
- **default ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **primary-md5-key**
- **default ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **retransmit-interval**
- **default ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **transit-delay**
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D}
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **authentication-key** WORD<0-8>
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **authentication-type** message-digest
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **authentication-type** none
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **authentication-type** simple
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **dead-interval** <0-2147483647>
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **hello-interval** <1-65535>
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **primary-md5-key** <1-255>
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **retransmit-interval** <0-3600>
- **ip ospf area virtual-link** {A.B.C.D} {A.B.C.D} **transit-delay** <0-3600>
- **no ip ospf area virtual-link** {A.B.C.D} {A.B.C.D}

## Command Parameters

**<A.B.C.D> <A.B.C.D>**

Creates a virtual interface area identifier. <A.B.C.D> <A.B.C.D> specify the area ID and the virtual interface ID, respectively.

**authentication-key WORD<0-8>**

Configures the authentication key of up to eight characters.

**authentication-type <none|simple|messagedigest>**

authenticationtype is: none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key. The default is none.

**dead-interval <0-2147483647>**

Configures the dead interval, in seconds, for the virtual interface, the number of seconds that a router Hello packets are not seen before its neighbors declare the router down. This value must be at least four times the Hello interval value. The default is 60.

**hello-interval <1-65535>**

Configures the Hello interval, in seconds, on the virtual interface for the length of time (in seconds) between the Hello packets that the router sends on the interface. The default is 10.

**primary-md5-key <1-255>**

Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the message digest key.

**retransmit-interval <0- 3600>**

Configures the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions. The range is from 0 to 3600.

**transit-delay <0-3600>**

Configures the transit delay for the virtual interface, the estimated number of seconds required to transmit a link-state update over the interface. The range is from 0 to 3600.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf area virtual-link message-digest-key (for a VRF)

---

Configure a Message Digest 5 algorithm (MD5) key for the virtual interface.

## Syntax

- **default ip ospf area virtual-link message-digest-key {A.B.C.D} {A.B.C.D} <1-255>**

- **ip ospf area virtual-link message-digest-key {A.B.C.D} {A.B.C.D} <1-255> md5-key WORD<1-16>**
- **no ip ospf area virtual-link message-digest-key {A.B.C.D} {A.B.C.D} <1-255>**

## Command Parameters

**<1-255> md5-key WORD<1-16>**

<A.B.C.D> is the virtual interface id. <1-255> is the ID for the message digest key. WORD<0-16> is an alphanumeric password in the range of 0 to 16 characters.

**<A.B.C.D> <A.B.C.D>**

Adds a Message Digest 5 algorithm (MD5) key to the interface. At most, you can configure two MD5 keys to an interface. <A.B.C.D> identifies an OSPF area.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf as-boundary-router (for a VRF)

---

Specifies ASBR status, the router is an autonomous system boundary router (ASBR).

## Syntax

- **default ip ospf as-boundary-router**
- **ip ospf as-boundary-router**
- **no ip ospf as-boundary-router**

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf as-boundary-router enable (for a VRF)

---

Configure the router as an autonomous system boundary router (ASBR).

## Syntax

- **default ip ospf as-boundary-router enable**
- **ip ospf as-boundary-router enable**
- **no ip ospf as-boundary-router enable**

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ip ospf auto-vlink (for a VRF)

---

Use automatic virtual links to provide an automatic, dynamic backup link for vital OSPF traffic. Automatic virtual links require more system resources than manually configured virtual links.

## Syntax

- **default ip ospf auto-vlink**
- **ip ospf auto-vlink**
- **no ip ospf auto-vlink**

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf bad-lsa-ignore enable (for a VRF)

---

Configures the switch to accept bad LSAs, for example, with a hole in the mask. If you use the no operator with this command, the switch ignores bad LSAs.

## Syntax

- **default ip ospf bad-lsa-ignore**
- **default ip ospf bad-lsa-ignore enable**
- **ip ospf bad-lsa-ignore enable**
- **no ip ospf bad-lsa-ignore**
- **no ip ospf bad-lsa-ignore enable**

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ip ospf default-cost

---

Configures the default OSPF metrics.



### Note

Not all parameters appear on all hardware platforms.

## Syntax

- `default ip ospf default-cost ethernet`
- `default ip ospf default-cost fast-ethernet`
- `default ip ospf default-cost forty-gig-ethernet`
- `default ip ospf default-cost gig-ethernet`
- `default ip ospf default-cost ten-gig-ethernet`
- `default ip ospf default-cost twentyfive-gig-ethernet`
- `ip ospf default-cost ethernet <1-65535>`
- `ip ospf default-cost fast-ethernet <1-65535>`
- `ip ospf default-cost forty-gig-ethernet <1-65535>`
- `ip ospf default-cost gig-ethernet <1-65535>`
- `ip ospf default-cost ten-gig-ethernet <1-65535>`
- `ip ospf default-cost twentyfive-gig-ethernet <1-65535>`

## Command Parameters

**ethernet <1-65535>**

Configures the OSPF default metrics for 10 Mb/s Ethernet. The default is 100.

**fast-ethernet <1-65535>**

Configures the OSPF default metrics for 100 Mb/s (Fast) Ethernet. The default is 10.

**forty-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 40 Gigabit Ethernet. The default is 1.

**gig-ethernet <1-65535>**

Configures the OSPF default metrics for Gigabit Ethernet. The default is 1.

**hundred-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 100 Gigabit Ethernet. The default is 1.

**ten-gig-ethernet <1-65535>**



Configures the OSPF default metrics for 10 Gigabit Ethernet. The default is 1.

**twentyfive-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 25 Gigabit Ethernet. The default is 1.

**vlan**

Configures the OSPF default metrics for a VLAN. The default is 1.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf host-route {A.B.C.D} (for a VRF)

---

Use host routes when the switch resides in a network that uses routing protocols other than OSPF.

## Syntax

- **default ip ospf host-route {A.B.C.D}**
- **default ip ospf host-route {A.B.C.D} metric**
- **ip ospf host-route {A.B.C.D}**
- **ip ospf host-route {A.B.C.D} metric <0-65535>**
- **no ip ospf host-route {A.B.C.D}**

## Command Parameters

**<A.B.C.D>**

Specifies the IP address of the host router in a.b.c.d format.

**metric <0-65535>**

Configures the metric (cost) for the host route.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf neighbor (for a VRF)

---

Configure NBMA neighbors so that the interface can participate in Designated Router election. All OSPF neighbors that you manually configure are NBMA neighbors.

## Syntax

- **default ip ospf neighbor {A.B.C.D}**
- **ip ospf neighbor {A.B.C.D} priority <0-255>**
- **no ip ospf neighbor {A.B.C.D}**

## Command Parameters

<A.B.C.D>

Identifies an OSPF area in IP address format A.B.C.D.

priority <0-255>

Changes the priority level of the neighbor.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf network (for a VRF)

---

Enable OSPF on a network.

## Syntax

- **default ip ospf network {A.B.C.D}**
- **default ip ospf network {A.B.C.D} {A.B.C.D}**
- **ip ospf network {A.B.C.D}**
- **ip ospf network {A.B.C.D} {A.B.C.D}**
- **ip ospf network {A.B.C.D} area {A.B.C.D}**
- **no ip ospf network {A.B.C.D}**
- **no ip ospf network {A.B.C.D} {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies the IP address of the network.

area {A.B.C.D}

Specifies the OSPF area.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf redistribute

Configure and enable redistribution entries to allow a protocol to announce routes of a certain source type, for example, static, RIP, or direct.

## Syntax

- `default ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr }`
- `default ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } vrf-src WORD<1-16>`
- `default ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } enable`
- `default ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } metric`
- `default ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } metric-type`
- `default ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } route-map`
- `default ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } subnets`
- `default ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } subnets vrf-src WORD<1-16>`
- `ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr }`
- `ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } subnets { allow | suppress }`
- `ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } vrf-src WORD<1-16>`
- `ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } enable`
- `ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } metric <0-65535>`
- `ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } metric-type { type1 | type2 | any }`
- `ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } route-map WORD<0-64>`

- `ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } subnets { allow | suppress } vrf-src WORD<1-16>`
- `no ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr }`
- `no ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } route-policy vrf-src WORD<1-16>`
- `no ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } vrf-src WORD<1-16>`
- `no ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } enable`
- `no ip ospf redistribute { bgp| direct | isis | ospf | rip | static | dvr } route-map`

## Command Parameters

`{ bgp| direct | isis | ospf | rip | static | dvr }`

Specifies the type of routes to redistribute-the protocol source.

`enable`

Enables the route redistribution instance.

`metric <0-65535>`

Configures the metric to apply to redistributed routes.

`metric-type { type1 | type2 | any }`

Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone.

`route-map WORD<0-64>`

Configures the route policy to apply to redistributed routes.

`subnets { allow | suppress }`

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

`vrf WORD <1-16>`

Specifies the VRF instance.

`vrf-src WORD<1-16>`

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

## Default

None

## Command Mode

VRF Router Configuration

### ip ospf rfc1583-compatibility enable (for a VRF)

---

Controls the preference rules used when the router chooses among multiple autonomous system external (ASE) LSAs which advertise the same destination. If enabled, the preference rule is the same as that specified by RFC1583. If disabled, the preference rule is as described in RFC2328, which can prevent routing loops when ASE LSAs for the same destination originate from different areas.

#### Syntax

- **default ip ospf rfc1583-compatibility**
- **default ip ospf rfc1583-compatibility enable**
- **ip ospf rfc1583-compatibility enable**
- **no ip ospf rfc1583-compatibility**
- **no ip ospf rfc1583-compatibility enable**

#### Default

The default is disabled.

## Command Mode

VRF Router Configuration

### ip ospf router-id (for a VRF)

---

Configure OSPF parameters on the switch to control how OSPF behaves on the system. The switch uses global parameters to communicate with other OSPF routers. Globally configure OSPF before you configure OSPF for an interface, port, or VLAN.

#### Syntax

- **default ip ospf router-id**
- **ip ospf router-id {A.B.C.D}**
- **no ip ospf router-id**

#### Command Parameters

**router-id <A.B.C.D>**

Configures the OSPF router ID IP address, where A.B.C.D is the IP address.

## Default

None

## Command Mode

VRF Router Configuration

## ip ospf timers basic holddown (for a VRF)

---

Configures the OSPF hold-down timer value, the length of time (in seconds) that OSPF continues to advertise a network after determining that it is unreachable.

## Syntax

- **default ip ospf timers basic**
- **default ip ospf timers basic holddown**
- **ip ospf timers basic holddown <3-60>**

## Command Parameters

<3-60>

Configures the holddown timer value.

## Default

The default is 120 seconds.

## Command Mode

VRF Router Configuration

## ip ospf trap (For a VRF)

---

Enable OSPF traps.

## Syntax

- **default ip ospf trap**
- **default ip ospf trap enable**
- **ip ospf trap enable**
- **no ip ospf trap**
- **no ip ospf trap enable**

## Command Parameters

**enable**

Enables OSPF traps.

## Default

The default value is disable.

## Command Mode

VRF Router Configuration

## ip prefix-list (for a VRF)

---

Allows or denies specific route updates. A prefix list policy specifies route prefixes to match. When there is a match, the route is used. Configure a prefix list and apply the list to any IP route policy.

## Syntax

- **ip prefix-list WORD<1-64> {A.B.C.D/X}**
- **ip prefix-list WORD<1-64> {A.B.C.D/X} ge <0-32>**
- **ip prefix-list WORD<1-64> {A.B.C.D/X} id <1-2147483647>**
- **ip prefix-list WORD<1-64> {A.B.C.D/X} le <0-32>**
- **ip prefix-list WORD<1-64> name WORD<1-64>**
- **no ip prefix-list WORD<1-64>**
- **no ip prefix-list WORD<1-64> {A.B.C.D/X}**

## Command Parameters

**<A.B.C.D/X> [<ge> <0-32>]**

Adds a prefix entry to the prefix list. A.B.C.D/X is the IP address and mask. <ge> <0-32> Lower bound and higher bound mask lengths together can define a range of networks. Use the no operator to remove a prefix entry from the prefix list: no ip prefix-list WORD<1-64> <A.B.C.D/X>

**name WORD<1-64>**

Renames the specified prefix list. The name length is from 1 to 64 characters.

## Default

None

## Command Mode

VRF Router Configuration

---

## ip rip (for a VRF)

---

Enables RIP on the VRF.

### Syntax

- **ip rip**
- **no ip rip**

### Default

The default is disabled.

### Command Mode

VRF Router Configuration

---

## ip rip default-metric (for a VRF)

---

Configure RIP default import metric. This value is used by RIP announce of OSPF internal routes if the policy does not specify metric. 0 is used for deconfiguration.

### Syntax

- **default ip rip default-metric**
- **ip rip default-metric <0-15>**

### Command Parameters

<0-15>

Configures the value of default import metric to import a route into RIP domain.

### Default

The default value is -1.

### Command Mode

VRF Router Configuration

---

## ip rip domain (for a VRF)

---

Specify the RIP domain.

### Syntax

- **default ip rip domain**



- **ip rip domain <0-39321>**

## Command Parameters

<0-39321>

Specifies the RIP domain.

## Default

The default is 0.

## Command Mode

VRF Router Configuration

## ip rip enable (for a VRF)

---

Enable RIP routing on the interface.

## Syntax

- **default ip rip enable**
- **ip rip enable**
- **no ip rip enable**

## Command Parameters

**enable**

Enables RIP routing on the interface.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ip rip redistribute

---

Configure and enable redistribution entries to allow a protocol to announce routes of a certain source type, for example, static, RIP, or direct.

## Syntax

- `default ip rip redistribute WORD<0-32>`
- `default ip rip redistribute WORD<0-32> enable`
- `default ip rip redistribute WORD<0-32> enable vrf-src WORD<1-16>`
- `default ip rip redistribute WORD<0-32> metric`
- `default ip rip redistribute WORD<0-32> metric vrf-src WORD<1-16>`
- `default ip rip redistribute WORD<0-32> route-map`
- `default ip rip redistribute WORD<0-32> route-map vrf-src WORD<1-16>`
- `default ip rip redistribute WORD<0-32> vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32>`
- `ip rip redistribute WORD<0-32> enable`
- `ip rip redistribute WORD<0-32> enable vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32> metric <0-65535>`
- `ip rip redistribute WORD<0-32> metric <0-65535> vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32> metric <0-65535>`
- `ip rip redistribute WORD<0-32> metric <0-65535> vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32> route-map WORD<0-64>`
- `ip rip redistribute WORD<0-32> route-map WORD<0-64> vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32> vrf-src WORD<1-16>`
- `no ip rip redistribute WORD<0-32>`
- `no ip rip redistribute WORD<0-32> enable`
- `no ip rip redistribute WORD<0-32> enable vrf-src WORD<1-16>`
- `no ip rip redistribute WORD<0-32> route-map`
- `no ip rip redistribute WORD<0-32> route-map vrf-src WORD<1-16>`
- `no ip rip redistribute WORD<0-32> vrf-src WORD<1-16>`

## Command Parameters

### `enable`

Enables the route redistribution instance.

### `metric <0-65535>`

Configures the metric to apply to redistributed routes.

### `route-map WORD<0-64>`

Configures the route map to apply to redistributed routes.

### `vrf WORD <1-16>`

Specifies the VRF instance.

### `vrf-src WORD<1-16>`

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

WORD<0-32>

Specifies the type of routes to redistribute-the protocol source.

## Default

None

## Command Mode

VRF Router Configuration

## ip rip redistribute { direct | isis | ospf | rip | static }

Configure and enable redistribution entries to allow a protocol to announce routes of a certain source type, for example, static, RIP, or direct.

## Syntax

- `default ip rip redistribute { direct | isis | ospf | rip | static }`
- `default ip rip redistribute { direct | isis | ospf | rip | static } enable`
- `default ip rip redistribute { direct | isis | ospf | rip | static } enable vrf-src WORD<1-16>`
- `default ip rip redistribute { direct | isis | ospf | rip | static } metric`
- `default ip rip redistribute { direct | isis | ospf | rip | static } metric vrf-src WORD<1-16>`
- `default ip rip redistribute { direct | isis | ospf | rip | static } route-map`
- `default ip rip redistribute { direct | isis | ospf | rip | static } route-map vrf-src WORD<1-16>`
- `default ip rip redistribute { direct | isis | ospf | rip | static } vrf-src WORD<1-16>`
- `ip rip redistribute { direct | isis | ospf | rip | static }`
- `ip rip redistribute { direct | isis | ospf | rip | static } enable`
- `ip rip redistribute { direct | isis | ospf | rip | static } enable vrf-src WORD<1-16>`
- `ip rip redistribute { direct | isis | ospf | rip | static } metric <0-65535>`
- `ip rip redistribute { direct | isis | ospf | rip | static } metric <0-65535> vrf-src WORD<1-16>`
- `ip rip redistribute { direct | isis | ospf | rip | static } route-map WORD<0-64>`

- `ip rip redistribute { direct | isis | ospf | rip | static } route-map WORD<0-64> vrf-src WORD<1-16>`
- `ip rip redistribute { direct | isis | ospf | rip | static } vrf-src WORD<1-16>`
- `no ip rip redistribute { direct | isis | ospf | rip | static }`
- `no ip rip redistribute { direct | isis | ospf | rip | static } enable`
- `no ip rip redistribute { direct | isis | ospf | rip | static } enable vrf-src WORD<1-16>`
- `no ip rip redistribute { direct | isis | ospf | rip | static } route-map`
- `no ip rip redistribute { direct | isis | ospf | rip | static } route-map vrf-src WORD<1-16>`
- `no ip rip redistribute { direct | isis | ospf | rip | static } vrf-src WORD<1-16>`

## Command Parameters

### `enable`

Enables the route redistribution instance.

### `metric <0-65535>`

Configures the metric to apply to redistributed routes.

### `route-map WORD<0-64>`

Configures the route map to apply to redistributed routes.

### `vrf WORD <1-16>`

Specifies the VRF instance.

### `vrf-src WORD<1-16>`

Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

### `WORD<0-32>`

Specifies the type of routes to redistribute-the protocol source.

## Default

None

## Command Mode

VRF Router Configuration

## ip rip timers basic holddown (for a VRF)

Configures the RIP hold-down timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable.

## Syntax

- `default ip rip timers basic holddown`
- `ip rip timers basic holddown <0-360>`

## Command Parameters

`<0-360>`

Configures the holddown timer value.

## Default

The default is 120 seconds.

## Command Mode

VRF Router Configuration

---

## ip rip timers basic timeout (for a VRF)

Configure the RIP timeout interval.

## Syntax

- `default ip rip timers basic timeout`
- `ip rip timers basic timeout <15-259200>`

## Command Parameters

`<15-259200>`

Configures the value of default import metric to import a route into RIP domain.

## Default

The default is 180.

## Command Mode

VRF Router Configuration

---

## ip rip timers basic update (for a VRF)

Configure the RIP update timer. The update time is the time interval between RIP updates.

## Syntax

- `default ip rip timers basic update`

- `ip rip timers basic update <1-360>`

## Command Parameters

`<1-360>`

Configures the update interval.

## Default

The default is 30 seconds.

## Command Mode

VRF Router Configuration

## ip route (for a VRF)

---

Configure a static route for a VRF. Use this command to:

- Create static routes for data traffic in a specific VRF context for any platform.
- Create static routes for a VRF associated with a Segmented Management Instance CLIP interface.
- Create static routes for management purposes on VSP 8600 Series:
  - Use the mgmtRouter VRF context to configure static routes for the OOB port.

## Syntax

- `default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D}`
- `default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} dynamic`
- `default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable`
- `default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable`
- `default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable next-hop-vrf WORD<1-16>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} name <0-64>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1-255>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1-255> next-hop-vrf WORD<1-16>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> local-next-hop enable`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> name <0-64>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> next-hop-vrf WORD<1-16>`

- **ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> preference <1-255>**
- **no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D}**
- **no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} dynamic**
- **no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} dynamic next-hop-vrf WORD<1-16>**
- **no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable**
- **no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable next-hop-vrf WORD<1-16>**
- **no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable**
- **no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} next-hop-vrf WORD<1-16>**
- **no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference**

## Command Parameters

**{A.B.C.D} {A.B.C.D} {A.B.C.D}**

Specifies the IP address, subnet mask, and next-hop address for the route. The first {A.B.C.D} configures the destination IP address of this route. An entry with a value of 0.0.0.0 is the default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries depends on the network management protocol table access mechanisms. The second {A.B.C.D} configures the route network mask with the destination address before the switch compares the mask to the destination value. The third {A.B.C.D} configures the IP address of the next hop of this route. In the case of a route bound to an interface realized through a broadcast media, the value of this box is the agent IP address on that interface.

**<1-255>**

Indicates the route preference of this entry. If you can use more than one route to forward IP traffic, the switch uses the route with the highest preference. The higher the number, the higher the preference.

**<1-65535>**

Specifies the static route cost.



### Note

Do not configure a static interface subnet route with a weight of 1.

**WORD<0-16>**

Specifies the VRF ID in inter-VRF static-route configuration.

**name WORD<0-64>**

Specifies the name associated with the static route.

This command does not apply to all hardware platforms.

## Default

None

## Command Mode

VRF Router Configuration

## Usage Guidelines

The *name* parameter is not supported on VSP 8600 Series.

VSP 8600 Series uses the routing stack to create static routes for data traffic as well as management purposes. For all other platforms, static routes for the management OOB and management VLAN, if supported, must use the Segmented Management Instance. For more information, see [VOSS User Guide](#). The management CLIP can use the Segmented Management Instance or routes in the associated VRF routing table manager (RTM).

## ip route preference protocol (for a VRF)

---

Specifies the route preference within a specific VRF context.

### Syntax

- **default ip route preference protocol <static | ospf-intra | ospf-inter | ebgp | ibgp | rip | ospf-extern1 | ospf-extern2 | spbm-level1>**
- **ip route preference protocol <static | ospf-intra | ospf-inter | ebgp | ibgp | rip | ospf-extern1 | ospf-extern2 | spbm-level1> <0-255>**

### Command Parameters

{static | ospf-intra | ospf-inter | ebgp | ibgp | rip | ospf-extern1 | ospf-extern2 | spbm-level1}

Specifies the Protocol type.

<0-255>

Preference value (0 is reserved for Local routes).

### Default

None

### Command Mode

VRF Router Configuration

## ip source-route (for VRF)

---

Enables IPv4 source routing on the specified VRF.

### Syntax

- **default ip source-route**



- **ip source-route**
- **no ip source-route**

## Default

Disabled

## Command Mode

VRF Router Configuration

## ip spb-pim-gw foreign-source (for a VRF)

---

Configures a static foreign source.

## Syntax

- **default ip spb-pim-gw foreign-source {A.B.C.D} group {A.B.C.D}**
- **ip spb-pim-gw foreign-source {A.B.C.D} group {A.B.C.D}**
- **no ip spb-pim-gw foreign-source {A.B.C.D} group {A.B.C.D}**

## Command Parameters

{A.B.C.D}

Specifies the multicast foreign source IP address.

group {A.B.C.D}

Specifies the group IP address.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 alternative-route (for VRF)

---

Enable IPv6 alternative route.

## Syntax

- **default ipv6 alternative-route**
- **ipv6 alternative-route**
- **no ipv6 alternative-route**

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

## ipv6 dhcp-relay (for VRF)

---

Configure Dynamic Host Configuration Protocol (DHCP) Relay.

## Syntax

- **default ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255>**
- **ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> enable**
- **no ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> enable**

## Command Parameters

**enable**

Enables dhcp-relay forwarding path.

**fwd-path**

Creates a forwarding path.

**WORD<0-255>**

Specifies Agent IPv6 address.

**WORD<0-255>**

Specifies Server IPv6 address.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 ecmp (for VRF)

---

IPv6 ECMP configuration.

## Syntax

- **default ipv6 ecmp enable**
- **default ipv6 ecmp max-path**

- **ipv6 ecmp enable**
- **ipv6 ecmp max-path <ECMP-Paths>**
- **no ipv6 ecmp enable**

## Command Parameters

### **enable**

Enables IPv6 ECMP globally.

### **max-path <ECMP-Paths>**

Specifies the maximum number of ECMP paths. Different hardware platforms can support a different number of ECMP paths. For more information on the maximum number of ECMP paths supported on the switch, see the scaling information in [VSP 8600 Release Notes](#).

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ipv6 forwarding (for VRF)

---

Configures IPv6 router with respect to the forwarding of datagrams received by, but not addressed to, this entity. Enable forwarding to act as a router.

## Syntax

- **default ipv6 forwarding**
- **ipv6 forwarding**
- **no ipv6 forwarding**

## Default

By default, forwarding is enabled on an interface. You must enable it globally before the interface configuration takes effect.

## Command Mode

VRF Router Configuration

## ipv6 hop-limit (for VRF)

---

Insert a value into the hop-limit field of the IPv6 header.

## Syntax

- **default ipv6 hop-limit <0-255>**
- **ipv6 hop-limit <0-255>**

## Command Parameters

<0-255>

Inserts a value into the hop-limit field of IPv6 header in the range of 0 to 255.

## Default

The default hop limit is 64.

## Command Mode

VRF Router Configuration

## ipv6 icmp drop-fragments (for a VRF)

---

Enable Internet Control Message Protocol (ICMP) redirect and unreachable messages on the VRF instance. The system inspects each incoming IPv6 ICMP packet to determine if it should drop or forward it.

## Syntax

- **default ipv6 icmp drop-fragments**
- **ipv6 icmp drop-fragments**
- **no ipv6 icmp drop-fragments**

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## ipv6 icmp echo multicast-request (for VRF)

---

Enables or disables the processing of IPv6 ICMP messages sent to a multicast address globally.

## Syntax

- **default ipv6 icmp echo multicast-request**
- **ipv6 icmp echo multicast-request**
- **no ipv6 icmp echo multicast-request**

## Command Parameters

### echo multicast-request

Enables or disables the processing of IPv6 ICMP messages sent to a multicast address globally. The default value is enabled.

## Default

The default is enabled.

## Command Mode

VRF Router Configuration

---

## ipv6 icmp drop-fragments (for a VRF)

---

Enable Internet Control Message Protocol (ICMP) redirect and unreachable messages on the VRF instance. The system inspects each incoming IPv6 ICMP packet to determine if it should drop or forward it.

## Syntax

- **default ipv6 icmp drop-fragments**
- **ipv6 icmp drop-fragments**
- **no ipv6 icmp drop-fragments**

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

---

## ipv6 icmp error-interval (for VRF)

---

Configure the interval (in milliseconds) for sending ICMPv6 error messages.

### Syntax

- **default ipv6 icmp error-interval**
- **ipv6 icmp error-interval <0-2147483647>**

### Command Parameters

**<1-2147483647>**

Configures the interval (in milliseconds) for sending ICMPv6 error messages. An entry of 0 seconds results in no sent ICMPv6 error messages.

### Default

The default error interval is 1000.

### Command Mode

VRF Router Configuration

---

## ipv6 icmp error-quota (for VRF)

---

Configure the number of Internet Control Message Protocol (ICMP) error messages that can be sent during the ICMP error interval.

### Syntax

- **default ipv6 icmp error-quota**
- **ipv6 icmp error-quota <0-2000000>**

### Command Parameters

**<0-2000000>**

Configures the number of internet Control Message Protocol (ICMP) error messages that the system can send during the ICMP error interval. A value of zero instructs the system not to send any ICMP error messages.

### Default

The default error quota is 50.

## Command Mode

VRF Router Configuration

### ipv6 icmp unreachable-msg (for VRF)

---

Enable Internet Control Message Protocol (ICMP) network unreachable messages.

#### Syntax

- **default ipv6 icmp unreachable-msg**
- **ipv6 icmp unreachable-msg**
- **no ipv6 icmp unreachable-msg**

#### Default

By default ICMP network unreachable messages are disabled.

## Command Mode

VRF Router Configuration

### ipv6 ipvpn (for VRF)

---

Enable IPv6 IP VPN configurations.

#### Syntax

- **default ipv6 ipvpn enable**
- **ipv6 ipvpn enable**
- **no ipv6 ipvpn enable**

#### Command Parameters

**enable**

Enables IPv6 IP VPN.

#### Default

None

## Command Mode

VRF Router Configuration

---

## ipv6 isis (for VRF)

---

Enable IPv6 isis accept and redistribute commands.

### Syntax

- **default ipv6 isis redistribute direct enable**
- **default ipv6 isis redistribute static enable**
- **ipv6 isis redistribute direct enable**
- **ipv6 isis redistribute static enable**
- **no ipv6 isis redistribute direct enable**
- **no ipv6 isis redistribute static enable**

### Command Parameters

#### direct

Configures IPv6 isis redistribute direct command.

#### enable

Enable isis redistribute direct command.

#### redistribute

Configures IPv6 isis redistribute.

#### static

Configures IPv6 isis redistribute static command.

### Default

None

### Command Mode

VRF Router Configuration

---

## ipv6 isis accept (for a VRF)

---

Configure an IPv6 Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all IPv6 routes from all Backbone Edge Bridges (BEBs) for a Virtual Routing and Forwarding (VRF) instance.

### Syntax

- **ipv6 isis accept i-sid <0-16777215>**
- **ipv6 isis accept i-sid <0-16777215> enable**
- **ipv6 isis accept i-sid <0-16777215> route-map WORD<1-64>**
- **ipv6 isis accept isid-list WORD<1-32>**



- **ipv6 isis accept isid-list WORD<1-32> enable**
- **ipv6 isis accept isid-list WORD<1-32> route-map WORD<1-64>**
- **ipv6 isis accept route-map WORD<1-64>**
- **no ipv6 isis accept i-sid <0-16777215>**
- **no ipv6 isis accept i-sid <0-16777215> enable**
- **no ipv6 isis accept i-sid <0-16777215> route-map**
- **no ipv6 isis accept isid-list WORD<1-32>**
- **no ipv6 isis accept isid-list WORD<1-32> enable**
- **no ipv6 isis accept isid-list WORD<1-32> route-map**
- **no ipv6 isis accept route-map**

## Command Parameters

### enable

Enables the IPv6 IS-IS accept policy.

### i-sid <0-16777215>

Specifies a service instance identifier (I-SID) number representing a local or remote IPv6 Layer 3 VSN. The number 0 represents the GRT.

### isid-list WORD <1-32>

Specifies a list of I-SID numbers representing local or remote IPv6 Layer 3 VSNs.

### route-map WORD<1-64>

Specifies an IPv6 IS-IS route policy.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ipv6 isis accept adv-rtr (for a VRF)

---

Configure an IPv6 Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all IPv6 routes for a specific Backbone Edge Bridge (BEB) for a Virtual Routing and Forwarding (VRF) instance.

## Syntax

- **ipv6 isis accept adv-rtr <x.xx.xx>**
- **ipv6 isis accept adv-rtr <x.xx.xx> enable**
- **ipv6 isis accept adv-rtr <x.xx.xx> i-sid <0-16777215>**
- **ipv6 isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> enable**

- `ipv6 isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> route-map WORD<1-64>`
- `ipv6 isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `ipv6 isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `ipv6 isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map WORD<1-64>`
- `ipv6 isis accept adv-rtr <x.xx.xx> route-map WORD<1-64>`
- `no ipv6 isis accept adv-rtr <x.xx.xx>`
- `no ipv6 isis accept adv-rtr <x.xx.xx> enable`
- `no ipv6 isis accept adv-rtr <x.xx.xx> i-sid <0-16777215>`
- `no ipv6 isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> enable`
- `no ipv6 isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> route-map`
- `no ipv6 isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `no ipv6 isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `no ipv6 isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map`
- `no ipv6 isis accept adv-rtr <x.xx.xx> route-map`

## Command Parameters

### `adv-rtr <x.xx.xx>`

Specifies a specific advertising BEB for the IPv6 IS-IS accept policy. The x.xx.xx variable specifies an SPBM nickname.

### `enable`

Enables the IPv6 IS-IS accept policy.

### `i-sid <0-16777215>`

Configures the service instance identifier (I-SID) to which the IPv6 IS-IS accept policy applies. The number 0 represents the GRT.

### `isid-list WORD <1-32>`

Configures a list of I-SIDs to which the IPv6 IS-IS accept policy applies.

### `route-map WORD<1-64>`

Specifies an IPv6 IS-IS route policy.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## ipv6 isis redistribute bgp

---

Identify IPv6 routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

### Syntax

- **default ipv6 isis redistribute bgp enable**
- **default ipv6 isis redistribute bgp metric**
- **default ipv6 isis redistribute bgp metric-type**
- **default ipv6 isis redistribute bgp route-map**
- **ipv6 isis redistribute bgp**
- **ipv6 isis redistribute bgp enable**
- **ipv6 isis redistribute bgp metric <0-65535>**
- **ipv6 isis redistribute bgp metric-type external**
- **ipv6 isis redistribute bgp metric-type internal**
- **ipv6 isis redistribute bgp route-map WORD<0-64>**
- **no ipv6 isis redistribute bgp**
- **no ipv6 isis redistribute bgp enable**
- **no ipv6 isis redistribute bgp metric**
- **no ipv6 isis redistribute bgp metric-type**
- **no ipv6 isis redistribute bgp route-map**

### Command Parameters

#### **enable**

Enables Border Gateway Protocol (BGP) route redistribution.

#### **metric <0-65535>**

Specifies the metric for the redistributed route. Use a value that is consistent with the destination protocol. The default is 1.

#### **metrictype external**

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

#### **metrictype internal**

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

### Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

## ipv6 isis redistribute direct

Identify IPv6 routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

### Syntax

- **default ipv6 isis redistribute direct enable**
- **default ipv6 isis redistribute direct metric**
- **default ipv6 isis redistribute direct metric-type**
- **default ipv6 isis redistribute direct route-map**
- **ipv6 isis redistribute direct**
- **ipv6 isis redistribute direct enable**
- **ipv6 isis redistribute direct metric <0-65535>**
- **ipv6 isis redistribute direct metric-type external**
- **ipv6 isis redistribute direct metric-type internal**
- **ipv6 isis redistribute direct route-map WORD<0-64>**
- **no ipv6 isis redistribute direct**
- **no ipv6 isis redistribute direct enable**
- **no ipv6 isis redistribute direct metric**
- **no ipv6 isis redistribute direct metric-type**
- **no ipv6 isis redistribute direct route-map**

### Command Parameters

#### **enable**

Enables direct route redistribution.

#### **metric <0-65535>**

Specifies the metric for the redistributed route. Use a value that is consistent with the destination protocol. The default is 1.

#### **metric-type external**

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

#### **metric-type internal**

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

## Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

## ipv6 isis redistribute ospf

---

Identify IPv6 routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

## Syntax

- **default ipv6 isis redistribute ospf enable**
- **default ipv6 isis redistribute ospf metric**
- **default ipv6 isis redistribute ospf metric-type**
- **default ipv6 isis redistribute ospf route-map**
- **ipv6 isis redistribute ospf**
- **ipv6 isis redistribute ospf enable**
- **ipv6 isis redistribute ospf metric <0-65535>**
- **ipv6 isis redistribute ospf metric-type external**
- **ipv6 isis redistribute ospf metric-type internal**
- **ipv6 isis redistribute ospf route-map WORD<0-64>**
- **no ipv6 isis redistribute ospf**
- **no ipv6 isis redistribute ospf enable**
- **no ipv6 isis redistribute ospf metric**
- **no ipv6 isis redistribute ospf metric-type**
- **no ipv6 isis redistribute ospf route-map**

## Command Parameters

### enable

Enables Open Shortest Path First (OSPF) route redistribution.

### metric <0-65535>

Specifies the metric for the redistributed route. Use a value that is consistent with the destination protocol. The default is 1.

### metrictype external

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

### metrictype internal

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

## Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

## ipv6 isis redistribute static

---

Identify IPv6 routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

## Syntax

- **default ipv6 isis redistribute static enable**
- **default ipv6 isis redistribute static metric**
- **default ipv6 isis redistribute static metric-type**
- **default ipv6 isis redistribute static route-map**
- **ipv6 isis redistribute static**
- **ipv6 isis redistribute static enable**
- **ipv6 isis redistribute static metric <0-65535>**
- **ipv6 isis redistribute static metric-type external**
- **ipv6 isis redistribute static metric-type internal**
- **ipv6 isis redistribute static route-map WORD<0-64>**
- **no ipv6 isis redistribute static**
- **no ipv6 isis redistribute static enable**
- **no ipv6 isis redistribute static metric**
- **no ipv6 isis redistribute static metric-type**
- **no ipv6 isis redistribute static route-map**

## Command Parameters

**enable**

Enables static route redistribution.

**metric <0-65535>**

Specifies the metric for the redistributed route. Use a value that is consistent with the destination protocol. The default is 1.

**metrictype external**

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

#### **metrictype internal**

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

## Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

## ipv6 neighbor (for VRF)

---

Commands to configure IPv6 neighbors globally.

## Syntax

- **ipv6 neighbor WORD<0-128> port {slot/port[sub-port]} mac 0x00:0x00:0x00:0x00:0x00:0x00 vlan <1-4059>**
- **no ipv6 neighbor WORD<0-128> port {slot/port[sub-port]}**
- **no ipv6 neighbor WORD<0-128> vlan <1-4059>**

## Command Parameters

**mac 0x00:0x00:0x00:0x00:0x00:0x00**

Specifies the MAC address.

**port {slot/port[sub-port]}**

Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the subport in the format slot/port/sub-port.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 0 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the *vrf-scaling* and *spbm-config-mode* boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**WORD<0-128>**

Ipv6 address in hex colon format.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 ospf (for a VRF)

---

Configure IPv6 OSPF parameters for a VRF.

### Syntax

- **default ipv6 ospf**
- **ipv6 ospf**
- **no ipv6 ospf**

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 ospf area (for a VRF)

---

Configure OSPF parameters on a VRF to control how OSPF behaves.

### Syntax

- **default ipv6 ospf area {A.B.C.D}**
- **default ipv6 ospf area {A.B.C.D} default-cost**
- **default ipv6 ospf area {A.B.C.D} import**
- **default ipv6 ospf area {A.B.C.D} import-summaries enable**
- **ipv6 ospf area {A.B.C.D}**
- **ipv6 ospf area {A.B.C.D} default-cost <0-16777215>**
- **ipv6 ospf area {A.B.C.D} import external**
- **ipv6 ospf area {A.B.C.D} import noexternal**
- **ipv6 ospf area {A.B.C.D} import nssa**
- **ipv6 ospf area {A.B.C.D} import-summaries enable**
- **no ipv6 ospf area {A.B.C.D}**
- **no ipv6 ospf area {A.B.C.D} import-summaries enable**



## Command Parameters

**{A.B.C.D}**

Specifies the area address.

**default-cost <0-16777215>**

Stub area default metric for this stub area, which is the cost from 0 to 16 777 215. This is the metric value applied at the indicated type of service.

**import <external|noexternal|nssa>**

Specifies the type of area: external - Stub and NSSA (not so stubby area) are both false. noexternal-Configures the area as stub area. nssa - Configures the area as NSSA.

**import-summaries enable**

Configures the area support to import summary advertisements into a stub area. This parameter must be used only if the area is a stub area.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 ospf area range (for a VRF)

Configure OSPF parameters on a VRF to control how OSPF behaves.

## Syntax

- **default ipv6 ospf area range {A.B.C.D} WORD<0-255> inter-area-prefix-link [advertise-metric]**
- **default ipv6 ospf area range {A.B.C.D} WORD<0-255> nssa-extlink [advertise-metric]**
- **ipv6 ospf area range {A.B.C.D} WORD<0-255> advertise-mode advertise**
- **ipv6 ospf area range {A.B.C.D} WORD<0-255> advertise-mode not-advertise**
- **ipv6 ospf area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-metric <0-65535>**
- **ipv6 ospf area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-mode advertise**
- **ipv6 ospf area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-mode not-advertise**
- **ipv6 ospf area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-metric <0-65535>**
- **ipv6 ospf area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-mode advertise**

- **ipv6 ospf area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-mode not-advertise**
- **no ipv6 ospf area range {A.B.C.D} WORD<0-255> inter-area-prefix-link**
- **no ipv6 ospf area range {A.B.C.D} WORD<0-255> nssa-extlink**

## Command Parameters

**{A.B.C.D}**

Specifies the area address.

**advertise-metric <0-65535>**

Specifies the advertise metric value and LSA type. The default advertise-metric is 0.

**advertise-mode <advertise|not-advertise>**

Configures if the area advertises into other OSPF areas. The default advertise-mode is advertise.

**inter-area-prefix-link**

Configures the area to use this LSA type.

**nssa-extlink**

Configures the area to use this LSA type.

**WORD<0-255>**

Specifies the IPv6 address and prefix.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 ospf area virtual-link (for a VRF)

Configure OSPF parameters on a VRF to control how OSPF behaves.

## Syntax

- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D}**
- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} dead-interval**
- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} hello-interval**
- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval**
- **default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} transit-delay**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D}**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} dead-interval <1-65535>**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} hello-interval <1-65535>**

- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval <1-1800>**
- **ipv6 area virtual-link {A.B.C.D} {A.B.C.D} transit-delay <1-1800>**
- **no ipv6 area virtual-link {A.B.C.D} {A.B.C.D}**

## Command Parameters

**{A.B.C.D} {A.B.C.D}**

Specifies the area address and the virtual link address.

**dead-interval <1-65535>**

Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default dead-interval is 60.

**hello-interval <1-65535>**

Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default hello interval is 10.

**retransmit-interval <1-1800>**

Specifies the retransmit interval, in seconds, for link-state advertisements. The default retransmit-interval is 5.

**transit-delay <1-1800>**

Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default transit-delay is 1.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 ospf as-boundary-router

---

Specify ASBR status, the router is an autonomous system boundary router (ASBR).

## Syntax

- **default ipv6 ospf as-boundary-router**
- **ipv6 ospf as-boundary-router**
- **no ipv6 ip ospf as-boundary-router**

## Default

None

## Command Mode

VRF Router Configuration

### ipv6 ospf default-cost

---

Configures the default OSPF metrics.



#### Note

Not all parameters appear on all hardware platforms.

## Syntax

- **default ipv6 ospf default-cost ethernet**
- **default ipv6 ospf default-cost fast-ethernet**
- **default ipv6 ospf default-cost forty-gig-ethernet**
- **default ipv6 ospf default-cost gig-ethernet**
- **default ipv6 ospf default-cost ten-gig-ethernet**
- **default ipv6 ospf default-cost twentyfive-gig-ethernet**
- **ipv6 ospf default-cost ethernet <1-65535>**
- **ipv6 ospf default-cost fast-ethernet <1-65535>**
- **ipv6 ospf default-cost forty-gig-ethernet <1-65535>**
- **ipv6 ospf default-cost gig-ethernet <1-65535>**
- **ipv6 ospf default-cost ten-gig-ethernet <1-65535>**
- **ipv6 ospf default-cost twentyfive-gig-ethernet <1-65535>**
- **ipv6 ospf default-cost vlan**

## Command Parameters

**ethernet <1-65535>**

Configures the OSPF default metrics for 10 Mb/s Ethernet. The default is 100.

**fast-ethernet <1-65535>**

Configures the OSPF default metrics for 100 Mb/s (Fast) Ethernet. The default is 10.

**forty-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 40 Gigabit Ethernet. The default is 1.

**gig-ethernet <1-65535>**

Configures the OSPF default metrics for Gigabit Ethernet. The default is 1.

**hundred-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 100 Gigabit Ethernet. The default is 1.

**ten-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 10 Gigabit Ethernet. The default is 1.

**twentyfive-gig-ethernet <1-65535>**

Configures the OSPF default metrics for 25 Gigabit Ethernet. The default is 1.

#### vlan

Configures the OSPF default metrics for a VLAN. The default is 1.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 ospf helper-mode-disable

---

Disable helper mode for OSPF on a VRF.

## Syntax

- **default ipv6 ospf helper-mode-disable**
- **ipv6 ospf helper-mode-disable**
- **no ipv6 ospf helper-mode-disable**

## Default

The default is enabled when OSPF is configured.

## Command Mode

VRF Router Configuration

## ipv6 ospf redistribute

---

Configure a redistribute entry to announce certain routes into the OSPFv3 domain.

## Syntax

- **default ipv6 ospf redistribute { bgp| direct | isis | static }**
- **default ipv6 ospf redistribute { bgp| direct | isis | static } enable**
- **default ipv6 ospf redistribute { bgp| direct | isis | static } metric**
- **default ipv6 ospf redistribute { bgp| direct | isis | static } metric-type**
- **default ipv6 ospf redistribute { bgp| direct | isis | static } route-map**
- **ipv6 ospf redistribute { bgp| direct | isis | static }**
- **ipv6 ospf redistribute { bgp| direct | isis | static } enable**

- **ipv6 ospf redistribute { bgp | direct | isis | static } metric <0-65535>**
- **ipv6 ospf redistribute { bgp | direct | isis | static } metric-type { type1 | type2 }**
- **ipv6 ospf redistribute { bgp | direct | isis | static } route-map WORD<0-64>**
- **no ipv6 ospf redistribute { bgp | direct | isis | static }**
- **no ipv6 ospf redistribute { bgp | direct | isis | static } enable**
- **no ipv6 ospf redistribute { bgp | direct | isis | static } route-map**

## Command Parameters

**{bgp | direct | isis | static}**

Specifies the type of routes to redistribute—the protocol source.

**enable**

Enables the route redistribution instance.

**metric <0-65535>**

Configures the metric to apply to redistributed routes.

**metric-type { type1 | type2 }**

Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 ospf router-id

---

Configure the OSPF router ID for a VRF.

## Syntax

- **default ipv6 ospf router-id**
- **ipv6 ospf router-id {A.B.C.D}**
- **no ipv6 ospf router-id**

## Command Parameters

**router-id <A.B.C.D>**

Configures the OSPF router ID IP address, where A.B.C.D is the IP address.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 prefix-list

---

Use prefix lists to allow or deny specific route updates. A prefix list policy specifies route prefixes to match. When there is a match, the route is used. Configure a prefix list and apply the list to a route policy.

## Syntax

- **ipv6 prefix-list WORD<1-64> name WORD<1-64>**
- **ipv6 prefix-list WORD<1-64> WORD<1-256> ge <0- 128>**
- **ipv6 prefix-list WORD<1-64> WORD<1-256> id <1-2147483647>**
- **ipv6 prefix-list WORD<1-64> WORD<1-256> le <0-128>**
- **no ipv6 prefix-list WORD<1-64> [WORD<1-256>]**

## Command Parameters

**ge <0-128>**

Specifies the minimum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

**id <1-2147483647>**

Specifies the prefix list ID.

**le <0-128>**

Specifies the maximum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

**name WORD<1-64>**

Renames the specified prefix list. The name length is from 1 to 64 characters.

**WORD<1-256>**

Specifies the IPv6 address and length.

**WORD<1-64>**

Adds a prefix entry to the prefix list. WORD<1-64> is the prefix-list name. WORD<1-256> is the IPv6 address and length. <ge|le><0- 128> is the minimum and maximum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

## Default

None

## Command Mode

VRF Router Configuration

## ipv6 route (for VRF)

Configure a static route to destination IPv6 address prefixes. Use this command to:

- Create static routes for data traffic in a specific VRF context for any platform.
- Create static routes for a VRF associated with a Segmented Management Instance CLIP interface.
- Create static routes for management purposes on VSP 8600 Series:
  - Use the mgmtRouter VRF context to configure static routes for the OOB port.

## Syntax

- **default ipv6 route WORD<0-46>**
- **default ipv6 route WORD<0-46> enable next-hop WORD<0-46>**
- **default ipv6 route WORD<0-46> enable port {slot/port[/sub-port]}**
- **default ipv6 route WORD<0-46> enable vlan <1-4059>**
- **default ipv6 route WORD<0-46> preference**
- **default ipv6 route WORD<0-46> preference next-hop WORD<0-46>**
- **default ipv6 route WORD<0-46> preference port {slot/port[/sub-port]}**
- **default ipv6 route WORD<0-46> preference vlan <1-4059>**
- **ipv6 route WORD<0-46> cost <1-65535>**
- **ipv6 route WORD<0-46> cost <1-65535> next-hop WORD<0-46>**
- **ipv6 route WORD<0-46> cost <1-65535> port {slot/port[/sub-port]}**
- **ipv6 route WORD<0-46> cost <1-65535> preference <1-255>**
- **ipv6 route WORD<0-46> cost <1-65535> vlan <1-4059>**
- **ipv6 route WORD<0-46> enable**
- **ipv6 route WORD<0-46> enable next-hop WORD<0-46>**
- **ipv6 route WORD<0-46> enable port {slot/port[/sub-port]}**
- **ipv6 route WORD<0-46> enable vlan <1-4059>**
- **ipv6 route WORD<0-46> preference <1-255>**
- **ipv6 route WORD<0-46> preference <1-255> next-hop WORD<0-46>**
- **ipv6 route WORD<0-46> preference <1-255> port {slot/port[/sub-port]}**



- **ipv6 route WORD<0-46> preference <1-255> vlan <1-4059>**
- **no ipv6 route WORD<0-46>**
- **no ipv6 route WORD<0-46> enable**
- **no ipv6 route WORD<0-46> enable next-hop WORD<0-46>**
- **no ipv6 route WORD<0-46> enable port {slot/port[/sub-port]}**
- **no ipv6 route WORD<0-46> enable vlan <1-4059>**
- **no ipv6 route WORD<0-46> next-hop WORD<0-46>**
- **no ipv6 route WORD<0-46> port {slot/port[/sub-port]}**
- **no ipv6 route WORD<0-46> vlan <1-4059>**

## Command Parameters

**cost <1-65535>**

Specifies the cost or distance ratio to reach the destination for this node. The default cost is 1.

**enable**

Enables the static route on the port. The default state for a new static route is enable.

**next-hop WORD<0-46>**

Specifies the IPv6 address of the next hop on this route. You do not need to specify the next hop if the devices directly connect to one another. Configure the next hop if the two nodes do not share the same network prefix but reside on the same link.

**port {slot/port[/sub-port]}**

Specifies the port to which this entry applies. You must specify the port if the next hop is a link-local address.

**preference <1-255>**

Specifies the routing preference of the destination IPv6 address. The default preference is 5.

**vlan <1-4059>**

Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

**WORD<0-46>**

Specifies the IPv6 destination network address.

## Default

The default state for a new static route is enable.

## Command Mode

VRF Router Configuration

## Usage Guidelines

The *name* parameter is not supported on VSP 8600 Series.

VSP 8600 Series uses the routing stack to create static routes for data traffic as well as management purposes. For all other platforms, static routes for the management OOB and management VLAN, if supported, must use the Segmented Management Instance. For more information, see [VOSS User Guide](#). The management CLIP can use the Segmented Management Instance or routes in the associated VRF routing table manager (RTM).

## ipv6 source-route (for VRF)

---

Enables IPv6 source routing globally.

### Syntax

- **default ipv6 source-route**
- **ipv6 source-route**
- **no ipv6 source-route**

### Default

Disabled

### Command Mode

VRF Router Configuration

## ipvpn

---

Create an IP Virtual Private Network (VPN) instance on the Virtual Routing and Forwarding (VRF).

### Syntax

- **default ipvpn**
- **ipvpn**
- **ipvpn enable**
- **no ipvpn**

### Command Parameters

**enable**

Enable IP Virtual Private Network (VPN) on the Virtual Routing and Forwarding (VRF).

### Default

The default is disabled.

## Command Mode

VRF Router Configuration

### ipvpn enable

---

Enable IP Virtual Private Network (VPN) on the Virtual Routing and Forwarding (VRF).

#### Syntax

- **default ipvpn enable**
- **ipvpn enable**
- **no ipvpn enable**

#### Default

The default is disabled.

## Command Mode

VRF Router Configuration

### i-sid (for a VRF)

---

Assign an service instance identifier (I-SID) to the VRF.

#### Syntax

- **default i-sid**
- **i-sid <0-16777215>**
- **no i-sid**
- **i-sid name <0-16777215> WORD<0-64>**
- **no i-sid name <0-16777215>**

#### Command Parameters

**<0-16777215>**

Specifies the service instance identifier (I-SID).

**name WORD<0-64>**

Specifies the name service instance identifier (I-SID).

#### Default

The default is disabled.

## Command Mode

VRF Router Configuration

## Usage Guidelines

The *name* parameter is not supported on VSP 8600 Series or XA1400 Series.

## isis accept (for a VRF)

---

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all routes from all Backbone Edge Bridges (BEBs) for a Virtual Routing and Forwarding (VRF) instance.

## Syntax

- **isis accept i-sid <0-16777215>**
- **isis accept i-sid <0-16777215> enable**
- **isis accept i-sid <0-16777215> route-map WORD<1-64>**
- **isis accept isid-list WORD<1-32>**
- **isis accept isid-list WORD<1-32> enable**
- **isis accept isid-list WORD<1-32> route-map WORD<1-64>**
- **isis accept route-map WORD<1-64>**
- **no isis accept i-sid <0-16777215>**
- **no isis accept i-sid <0-16777215> enable**
- **no isis accept i-sid <0-16777215> route-map**
- **no isis accept isid-list WORD<1-32>**
- **no isis accept isid-list WORD<1-32> enable**
- **no isis accept isid-list WORD<1-32> route-map**
- **no isis accept route-map**

## Command Parameters

### enable

Enables the IS-IS accept policy.

### i-sid <0-16777215>

Specifies a service instance identifier (I-SID) number representing a local or remote Layer 3 VSN. The number 0 represents the GRT.

### isid-list WORD <1-32>

Specifies a list of I-SID numbers representing local or remote Layer 3 VSNs.

### route-map WORD<1-64>

Specifies an IS-IS route policy.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## isis accept adv-rtr (for a VRF)

---

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all routes for a specific Backbone Edge Bridge (BEB) for a Virtual Routing and Forwarding (VRF) instance.

## Syntax

- `isis accept adv-rtr <x.xx.xx>`
- `isis accept adv-rtr <x.xx.xx> enable`
- `isis accept adv-rtr <x.xx.xx> i-sid <0-16777215>`
- `isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> enable`
- `isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> route-map WORD<1-64>`
- `isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map WORD<1-64>`
- `isis accept adv-rtr <x.xx.xx> route-map WORD<1-64>`
- `no isis accept adv-rtr <x.xx.xx>`
- `no isis accept adv-rtr <x.xx.xx> enable`
- `no isis accept adv-rtr <x.xx.xx> i-sid <0-16777215>`
- `no isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> enable`
- `no isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> route-map`
- `no isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `no isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `no isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map`
- `no isis accept adv-rtr <x.xx.xx> route-map`

## Command Parameters

`adv-rtr <x.xx.xx>`

Specifies a specific advertising BEB for the IS-IS accept policy. The x.xx.xx variable specifies an SPBM nickname.

`enable`

Enables the IS-IS accept policy.

`i-sid <0-16777215>`

Configures the service instance identifier (I-SID) to which the IS-IS accept policy applies. The number 0 represents the GRT.

**isis-list WORD <1-32>**

Configures a list of I-SIDs to which the IS-IS accept policy applies.

**route-map WORD<1-64>**

Specifies an IS-IS route policy.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## isis multi-area ip redistribute routed-multicast

Enables IS-IS Multi-area SPB IPv4 routed multicast redistribution for the specific Virtual Router Forwarding (VRF) instance on the switch.

## Syntax

- **default isis multi-area ip redistribute routed-multicast**
- **default isis multi-area ip redistribute routed-multicast [enable]**
- **default isis multi-area ip redistribute routed-multicast [home-to-remote]**
- **default isis multi-area ip redistribute routed-multicast [home-to-remote] [enable]**
- **default isis multi-area ip redistribute routed-multicast [home-to-remote] [route-map]**
- **default isis multi-area ip redistribute routed-multicast [remote-to-home]**
- **default isis multi-area ip redistribute routed-multicast [remote-to-home] [enable]**
- **default isis multi-area ip redistribute routed-multicast [remote-to-home] [route-map]**
- **default isis multi-area ip redistribute routed-multicast [route-map]**
- **isis multi-area ip redistribute routed-multicast**
- **isis multi-area ip redistribute routed-multicast [enable]**
- **isis multi-area ip redistribute routed-multicast [home-to-remote]**
- **isis multi-area ip redistribute routed-multicast [home-to-remote] [enable]**
- **isis multi-area ip redistribute routed-multicast [home-to-remote] [route-map WORD<1-64>]**

- `isis multi-area ip redistribute routed-multicast [remote-to-home]`
- `isis multi-area ip redistribute routed-multicast [remote-to-home] [enable]`
- `isis multi-area ip redistribute routed-multicast [remote-to-home] [route-map WORD<1-64>]`
- `isis multi-area ip redistribute routed-multicast [route-map WORD<1-64>]`
- `no isis multi-area ip redistribute routed-multicast`
- `no isis multi-area ip redistribute routed-multicast [enable]`
- `no isis multi-area ip redistribute routed-multicast [home-to-remote]`
- `no isis multi-area ip redistribute routed-multicast [home-to-remote] [enable]`
- `no isis multi-area ip redistribute routed-multicast [home-to-remote] [route-map]`
- `no isis multi-area ip redistribute routed-multicast [remote-to-home]`
- `no isis multi-area ip redistribute routed-multicast [remote-to-home] [enable]`
- `no isis multi-area ip redistribute routed-multicast [remote-to-home] [route-map]`
- `no isis multi-area ip redistribute routed-multicast [route-map]`

## Command Parameters

### enable

Enables the IS-IS Multi-area SPB IPv4 routed multicast redistribution.

### home-to-remote

Specifies the redistribution configuration for home to remote direction.

### remote-to-home

Specifies the redistribution configuration for remote to home direction.

### route-map

Specifies the Multi-area SPB IPv4 redistribution route policy.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis multi-area ip redistribute unicast

Enables IS-IS Multi-area SPB IPv4 unicast redistribution for the specific Virtual Router Forwarding (VRF) instance on the switch.

## Syntax

- `default isis multi-area ip redistribute unicast`
- `default isis multi-area ip redistribute unicast [enable]`
- `default isis multi-area ip redistribute unicast [home-to-remote]`
- `default isis multi-area ip redistribute unicast [home-to-remote] [enable]`
- `default isis multi-area ip redistribute unicast [home-to-remote] [route-map]`
- `default isis multi-area ip redistribute unicast [remote-to-home]`
- `default isis multi-area ip redistribute unicast [remote-to-home] [enable]`
- `default isis multi-area ip redistribute unicast [remote-to-home] [route-map]`
- `default isis multi-area ip redistribute unicast [route-map]`
- `isis multi-area ip redistribute unicast`
- `isis multi-area ip redistribute unicast [enable]`
- `isis multi-area ip redistribute unicast [home-to-remote]`
- `isis multi-area ip redistribute unicast [home-to-remote] [enable]`
- `isis multi-area ip redistribute unicast [home-to-remote] [route-map WORD<1-64>]`
- `isis multi-area ip redistribute unicast [remote-to-home]`
- `isis multi-area ip redistribute unicast [remote-to-home] [enable]`
- `isis multi-area ip redistribute unicast [remote-to-home] [route-map WORD<1-64>]`
- `isis multi-area ip redistribute unicast [route-map WORD<1-64>]`
- `no isis multi-area ip redistribute unicast`
- `no isis multi-area ip redistribute unicast [enable]`
- `no isis multi-area ip redistribute unicast [home-to-remote]`
- `no isis multi-area ip redistribute unicast [home-to-remote] [enable]`
- `no isis multi-area ip redistribute unicast [home-to-remote] [route-map]`
- `no isis multi-area ip redistribute unicast [remote-to-home]`



- `no isis multi-area ip redistribute unicast [remote-to-home] [enable]`
- `no isis multi-area ip redistribute unicast [remote-to-home] [route-map]`
- `no isis multi-area ip redistribute unicast [route-map]`

## Command Parameters

### enable

Enables the IS-IS Multi-area SPB IPv4 unicast redistribution.

### home-to-remote

Specifies the redistribution configuration for home to remote direction.

### remote-to-home

Specifies the redistribution configuration for remote to home direction.

### route-map

Specifies the Multi-area SPB IPv4 redistribution route policy.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis multi-area ipv6 redistribute unicast

---

Enables IS-IS Multi-area SPB IPv6 unicast redistribution for the specific Virtual Router Forwarding (VRF) instance on the switch.

## Syntax

- `default isis multi-area ipv6 redistribute unicast`
- `default isis multi-area ipv6 redistribute unicast [enable]`
- `default isis multi-area ipv6 redistribute unicast [home-to-remote]`
- `default isis multi-area ipv6 redistribute unicast [home-to-remote] [enable]`
- `default isis multi-area ipv6 redistribute unicast [home-to-remote] [route-map]`
- `default isis multi-area ipv6 redistribute unicast [remote-to-home]`

- `default isis multi-area ipv6 redistribute unicast [remote-to-home] [enable]`
- `default isis multi-area ipv6 redistribute unicast [remote-to-home] [route-map]`
- `default isis multi-area ipv6 redistribute unicast [route-map]`
- `isis multi-area ipv6 redistribute unicast`
- `isis multi-area ipv6 redistribute unicast [enable]`
- `isis multi-area ipv6 redistribute unicast [home-to-remote]`
- `isis multi-area ipv6 redistribute unicast [home-to-remote] [enable]`
- `isis multi-area ipv6 redistribute unicast [home-to-remote] [route-map WORD<1-64>]`
- `isis multi-area ipv6 redistribute unicast [remote-to-home]`
- `isis multi-area ipv6 redistribute unicast [remote-to-home] [enable]`
- `isis multi-area ipv6 redistribute unicast [remote-to-home] [route-map WORD<1-64>]`
- `isis multi-area ipv6 redistribute unicast [route-map WORD<1-64>]`
- `no isis multi-area ipv6 redistribute unicast`
- `no isis multi-area ipv6 redistribute unicast [enable]`
- `no isis multi-area ipv6 redistribute unicast [home-to-remote]`
- `no isis multi-area ipv6 redistribute unicast [home-to-remote] [enable]`
- `no isis multi-area ipv6 redistribute unicast [home-to-remote] [route-map]`
- `no isis multi-area ipv6 redistribute unicast [remote-to-home]`
- `no isis multi-area ipv6 redistribute unicast [remote-to-home] [enable]`
- `no isis multi-area ipv6 redistribute unicast [remote-to-home] [route-map]`
- `no isis multi-area ipv6 redistribute unicast [route-map]`

## Command Parameters

### enable

Enables the IS-IS Multi-area SPB IPv6 unicast redistribution.

### home-to-remote

Specifies the redistribution configuration for home to remote direction.

### remote-to-home

Specifies the redistribution configuration for remote to home direction.

### route-map

Specifies the Multi-area SPB IPv6 redistribution route policy.

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## Usage Guidelines

This command does not apply to all hardware platforms. For more information about feature support, see [VOSS Feature Support Matrix](#).

## isis redistribute bgp

---

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

## Syntax

- `default isis redistribute bgp enable`
- `default isis redistribute bgp metric`
- `default isis redistribute bgp metric-type`
- `default isis redistribute bgp route-map`
- `default isis redistribute bgp subnets`
- `isis redistribute bgp`
- `isis redistribute bgp enable`
- `isis redistribute bgp metric <0-65535>`
- `isis redistribute bgp metric-type external`
- `isis redistribute bgp metric-type internal`
- `isis redistribute bgp route-map WORD<0-64>`
- `isis redistribute bgp subnets allow`
- `isis redistribute bgp subnets suppress`
- `no isis redistribute bgp`
- `no isis redistribute bgp enable`
- `no isis redistribute bgp metric`
- `no isis redistribute bgp metric-type`
- `no isis redistribute bgp route-map`
- `no isis redistribute bgp subnets`

## Command Parameters

enable

Enables Border Gateway Protocol (BGP) route redistribution.

**metric <0-65535>**

Specifies the metric for the redistributed route. Use a value that is consistent with the destination protocol. The default is 1.

**metric-type external**

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

**metric-type internal**

Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes. Specifies a name.

**subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

## Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

## isis redistribute direct

---

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

## Syntax

- **default isis redistribute direct enable**
- **default isis redistribute direct metric**
- **default isis redistribute direct metric-type**
- **default isis redistribute direct route-map**
- **default isis redistribute direct subnets**
- **isis redistribute direct**

- **isis redistribute direct enable**
- **isis redistribute direct metric <0-65535>**
- **isis redistribute direct metric-type external**
- **isis redistribute direct metric-type internal**
- **isis redistribute direct route-map WORD<0-64>**
- **isis redistribute direct subnets allow**
- **isis redistribute direct subnets suppress**
- **no isis redistribute direct**
- **no isis redistribute direct enable**
- **no isis redistribute direct metric**
- **no isis redistribute direct metric-type**
- **no isis redistribute direct route-map**
- **no isis redistribute direct subnets**

## Command Parameters

### **enable**

Enables route redistribution.

### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type internal**

Configures the type of route to import into the protocol. The default is internal.

### **route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes. Specifies a name.

### **subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

### **subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

## Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

---

## isis redistribute ospf

---

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

### Syntax

- `default isis redistribute ospf enable`
- `default isis redistribute ospf metric`
- `default isis redistribute ospf metric-type`
- `default isis redistribute ospf route-map`
- `default isis redistribute ospf subnets`
- `isis redistribute ospf`
- `isis redistribute ospf enable`
- `isis redistribute ospf metric <0-65535>`
- `isis redistribute ospf metric-type external`
- `isis redistribute ospf metric-type internal`
- `isis redistribute ospf route-map WORD<0-64>`
- `isis redistribute ospf subnets allow`
- `isis redistribute ospf subnets suppress`
- `no isis redistribute ospf`
- `no isis redistribute ospf enable`
- `no isis redistribute ospf metric`
- `no isis redistribute ospf metric-type`
- `no isis redistribute ospf route-map`
- `no isis redistribute ospf subnets`

### Command Parameters

#### `enable`

Enables route redistribution.

#### `metric <0-65535>`

Configures the metric (cost) to apply to redistributed routes. The default is 1.

#### `metrictype external`

Configures the type of route to import into the protocol. The default is internal.

#### `metrictype internal`

Configures the type of route to import into the protocol. The default is internal.

#### `route-map WORD<0-64>`

Configures the route policy to apply to redistributed routes. Specifies a name.

#### `subnets allow`

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

## Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

## isis redistribute rip

---

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

## Syntax

- **default isis redistribute rip enable**
- **default isis redistribute rip metric**
- **default isis redistribute rip metric-type**
- **default isis redistribute rip route-map**
- **default isis redistribute rip subnets**
- **isis redistribute rip**
- **isis redistribute rip enable**

- **isis redistribute rip metric <0-65535>**
- **isis redistribute rip metric-type external**
- **isis redistribute rip metric-type internal**
- **isis redistribute rip route-map WORD<0-64>**
- **isis redistribute rip subnets allow**
- **isis redistribute rip subnets suppress**
- **no isis redistribute rip**
- **no isis redistribute rip enable**
- **no isis redistribute rip metric**
- **no isis redistribute rip metric-type**
- **no isis redistribute rip route-map**
- **no isis redistribute rip subnets**

## Command Parameters

### **enable**

Enables route redistribution.

### **enable**

Enables route redistribution.

### **enable**

Enables route redistribution.

### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### **metric <0-65535>**

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type external**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type internal**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type internal**

Configures the type of route to import into the protocol. The default is internal.

### **metric-type internal**

Configures the type of route to import into the protocol. The default is internal.



**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes. Specifies a name.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes. Specifies a name.

**route-map WORD<0-64>**

Configures the route policy to apply to redistributed routes. Specifies a name.

**subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets allow**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

**subnets suppress**

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

## Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

## isis redistribute static

---

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

## Syntax

- `default isis redistribute static enable`
- `default isis redistribute static metric`
- `default isis redistribute static metric-type`
- `default isis redistribute static route-map`
- `default isis redistribute static subnets`
- `isis redistribute static`
- `isis redistribute static enable`
- `isis redistribute static metric <0-65535>`
- `isis redistribute static metric-type external`
- `isis redistribute static metric-type internal`
- `isis redistribute static route-map WORD<0-64>`
- `isis redistribute static subnets allow`
- `isis redistribute static subnets suppress`
- `no isis redistribute static`
- `no isis redistribute static enable`
- `no isis redistribute static metric`
- `no isis redistribute static metric-type`
- `no isis redistribute static route-map`
- `no isis redistribute static subnets`

## Command Parameters

### `enable`

Enables route redistribution.

### `metric <0-65535>`

Configures the metric (cost) to apply to redistributed routes. The default is 1.

### `metric-type external`

Configures the type of route to import into the protocol. The default is internal.

### `metric-type internal`

Configures the type of route to import into the protocol. The default is internal.

### `route-map WORD<0-64>`

Configures the route policy to apply to redistributed routes. Specifies a name.

### `subnets allow`

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose `allow` to advertise the subnets individually with the learned or configured mask of the subnet. The default is `allow`.

### `subnets suppress`

Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

## Default

By default, redistribution is disabled.

## Command Mode

VRF Router Configuration

## mvpn enable

---

Enables Layer 3 VSN IP multicast over Fabric Connect for a specific VRF.

## Syntax

- **default mvpn enable**
- **mvpn enable**
- **no mvpn enable**

## Default

The default is disabled.

## Command Mode

VRF Router Configuration

## mvpn fwd-cache-timeout <10-86400>

---

Configures the timeout value on the VRF.

## Syntax

- **default mvpn fwd-cache-timeout**
- **mvpn fwd-cache-timeout <10-86400>**
- **no mvpn fwd-cache-timeout**

## Command Parameters

<10-86400>

Specifies the timeout value. The default is 210 seconds.

## Default

The default is 210 seconds.

## Command Mode

VRF Router Configuration



# VRRP Router Configuration

---

The following topics document commands available in VRRP Router Configuration mode of the command line interface (CLI).

## ipv6 send-trap enable

---

Configure Virtual Router Redundancy Protocol (VRRP) notification control.

### Syntax

- **default ipv6 send-trap enable**
- **ipv6 send-trap enable**
- **no ipv6 send-trap enable**

### Default

Generation of SNMP traps for VRRP events is enabled.

### Command Mode

VRRP Router Configuration

## ping-virtual-address

---

Ping a virtual address to test the connection.

### Syntax

- **default ping-virtual-address**
- **default ping-virtual-address enable**
- **default ping-virtual-address enable vrf WORD<1-16>**
- **no ping-virtual-address**
- **no ping-virtual-address enable**
- **no ping-virtual-address enable vrf WORD<1-16>**
- **ping-virtual-address**
- **ping-virtual-address enable**
- **ping-virtual-address enable vrf WORD<1-16>**

## Command Parameters

**enable**

Enables the virtual address ping.

**vrf WORD <1-16>**

Specifies the virtual routing and forwarding (VRF) name from 1-16 characters.

## Default

None

## Command Mode

VRRP Router Configuration

---

## send-trap

Configure Virtual Router Redundancy Protocol (VRRP) notification control.

## Syntax

- **default send-trap**
- **default send-trap enable**
- **default send-trap enable vrf WORD<1-16>**
- **no send-trap**
- **no send-trap enable**
- **no send-trap enable vrf WORD<1-16>**
- **send-trap**
- **send-trap enable**
- **send-trap enable vrf WORD<1-16>**

## Command Parameters

**enable**

Enable a trap for VRRP events.

**vrf WORD<1-16>**

Specifies the VRF name.

## Default

Generation of SNMP traps for VRRP events is enabled.

## Command Mode

VRRP Router Configuration



# VXLAN Configuration

---

The following topics document commands available in VXLAN Configuration mode of the command line interface (CLI).

## c-vid (for a VXLAN Gateway mlt)

---

Associate VLANs in an MLT list to the specified VNID instance.

### Syntax

- **c-vid <1-4094> mlt <1-4094>**
- **no c-vid <1-4094> mlt <1-4094>**

### Command Parameters

**<1-4094> mlt <1-4094>**

Specifies a value that uniquely identifies the customer VLAN ID and MLTs of this ELAN end point.

### Default

None

### Command Mode

VXLAN Configuration

## c-vid (for a VXLAN Gateway port)

---

Associate VLANs in a port list to the specified VNID instance.

### Syntax

- **c-vid <1-4094> port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**
- **no c-vid <1-4094> port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}**



## Command Parameters

**<1-4094> port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

Specifies a value that uniquely identifies the customer VLAN ID and ports of this ELAN end point.

## Default

None

## Command Mode

VXLAN Configuration

---

## untagged-traffic (for a VXLAN Gateway mlt)

Specify the MLT in this VNID instance that will support untagged traffic.

## Syntax

- **no untagged-traffic mlt <1-4094>**
- **untagged-traffic mlt <1-4094>**

## Command Parameters

**mlt <1-4094>**

Specifies the MLTs that support untagged traffic.

## Default

None

## Command Mode

VXLAN Configuration

---

## untagged-traffic (for a VXLAN Gateway port)

Specify the ports in this VNID instance that will support untagged traffic.

## Syntax

- **no untagged-traffic port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}
- **untagged-traffic port** {*slot/port[/sub-port]* [-*slot/port[/sub-port]*] [,...]}

## Command Parameters

**port** {*slot/port[/sub-port]* [*-slot/port[/sub-port]*] [,...]}

Specifies the ports that support untagged traffic.

## Default

None

## Command Mode

VXLAN Configuration

## vtep (association)

---

Associate VTEPs to the specified VNID instance.

## Syntax

- **no vtep** <1-255>
- **vtep** <1-255>

## Command Parameters

<1-255>

Lists the remote VTEP destinations to associate with the specified VNID.

## Default

None

## Command Mode

VXLAN Configuration