COMMAND REFERENCE GUIDE

Extreme SLX-OS Command Reference, 18x.1.00a

Supporting the ExtremeSwitching SLX 9030 Switches

9035671-01
March 2019

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, please see: 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: www.extremenetworks.com/support/policies/software-licensing

Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Conventions

This section discusses the conventions used in this guide.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.

Format	Description
`Courier font`	Identifies CLI output. Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/open-source-declaration/.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

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

- GTAC (Global Technical Assistance Center) for Immediate Support
  - **Phone:** 1-800-998-2408 (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
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- Extreme Portal — Search the GTAC 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.

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

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) 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

Subscribing to Service Notifications

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

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

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

4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.

- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please 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.

About This Document

Supported hardware and software

The following platforms are supported by this release:

- ExtremeSwitching SLX 9030 Series

What's new in this document

There are new and changed commands in this release.

New commands

The following commands are new:

- **endpoint-tracking timeout reauth-period**

Modified commands

The following commands are modified:

- **endpoint-tracking enable**
- **show mac-address-table endpoint-tracking**
- **show vlan brief**
- **show vlan detail**

Regarding Ethernet interfaces and chassis devices

Many features can apply to either single-slot (1 RU) or multi-slot (chassis) devices.

The Ethernet interface configuration and output examples in this document may appear as either 0/*X* or *N*/*X* assignments, where *N* is an integer greater than 0.

Be aware of the interface configuration options of your particular device.

In addition, some legacy show outputs may reflect output from a variety of devices, including chassis devices.

Regarding CLI History tables

This document contains legacy commands from previous SLX-OS releases. However, the History tables indicate that these legacy commands are introduced in this release.

Using the SLX-OS CLI

User accounts

A user account specifies that user's level of access to the device CLI.

The SLX-OS software uses role-based access control (RBAC) as the authorization mechanism. A *role* is a container for rules, which specify which commands can be executed and with which permissions. When you create a user account you need to specify a role for that account. In general, *user* (as opposed to *user-level*) refers to any account—to which any role can be assigned—user, admin, or a non-default role.

The software ships with two default accounts—admin and user—and two corresponding default roles:

- **admin**—Accounts with admin permissions can execute all commands supported on the device. (For the initial admin login, refer to the relevant *Hardware Installation Guide*.)
- **user**—Accounts with user-level permissions can execute all **show** commands supported on the device. User-level accounts can also execute the following operational commands: **cfm**, **execute-script**, **exit**, **mtrace**, **no**, **ping**, **rasman**, **ssh**, **sysmon**, **telnet**, **timestamp**, **trace-l2**, and **traceroute**.

For more information on user accounts and roles, refer to the *Extreme SLX-OS Security Configuration Guide*.

Accessing the CLI

After an IP address is assigned to the device, you can access the CLI through a serial console connection to the active management module or a Telnet or SSH session using the chassis management IP address. For more information on a serial console connection, refer to the relevant *SLX-OS Hardware Installation Guide*. For information on a session connection, refer to the *Extreme SLX-OS Management Configuration Guide*.

The procedure to access the CLI is the same through either the console interface or through a Telnet or SSH session; both access methods bring you to the login prompt. The following example shows the admin role logging into the device:

```
device login: admin
Password:**********
device#
```

NOTE

Multiple users can open sessions on the device and issue commands. The device supports a maximum of 32 CLI sessions.

Command modes

The SLX-OS CLI uses an industry-standard hierarchical shell familiar to Ethernet/IP networking administrators. You can use one of three major command modes to enter commands and access sub-configuration modes on the device.

Privileged EXEC mode

Privileged EXEC mode supports all clear, show, and debug commands. In addition, you can enter some configuration commands that do not make changes to the system configuration. The following example shows the privileged EXEC prompt. At this prompt, you issue the **configure terminal** command to enter global configuration mode.

```
device# configure terminal
device(config)#
```

Global configuration mode

Global configuration mode supports commands that can change the device configuration. For any changes to be persistent, you must save the system configuration before rebooting the device. The global configuration mode provides access to sub-configuration modes for individual interfaces, VLANs, routing protocols, and other configuration areas. The following example shows how you access the interface sub-configuration mode by issuing the **interface** command with a specified interface.

```
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)#
```

Using the do command as a shortcut

You can use the **do** command to save time when you are working in any configuration mode and you want to run a command in privileged EXEC mode.

For example, if you are configuring an Ethernet interface and you want to execute a privileged EXEC mode command, such as the **dir** command, you would first have to exit the Interface configuration mode. By using the **do** command with the **dir** command, you can ignore the need to change configuration modes, as shown in the following example.

```
device(config-if-eth-0/2)# do dir
total 32
drwxrwxr-x 3 21487 1011  4096 Mar 26 17:58 .
drwxrwxr-x 3 21487 1011  4096 Mar 13 06:45 ..
-rw-r--r-- 1 root  sys    495 Mar 16 15:41 defaultconfig.cluster
-rw-r--r-- 1 root  sys    210 Mar 16 15:41 defaultconfig.standalone
drwxrwxr-x 5 root  sys   4096 Mar 26 17:57 flex-cli
-rw-r--r-- 1 root  root 11093 Mar 26 18:04 startup-config

16908197888 bytes total (8438681600  bytes free)
```

Using the top command as a shortcut

You can use the **top** command to save time when you want to add or remove a top-level configuration while staying at the same command level.

```
device# configure terminal
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# top ip access-list extended acl_01
2018/06/03-07:44:41, [SSMD-1400], 30282, DCE, INFO, SLX, IPv4 access list acl_01 is created.
```

Displaying CLI commands and command syntax

You can display commands and syntax information in any mode and from any point in the command hierarchy.

Enter a question mark (?) in any command mode to display the list of commands available in that mode.

```
device# configure terminal
device(config)# hardware
C-78(config-hardware)# ?
Possible completions:
  connector     Configure a connector
  describe      Display transparent command information
  do            Run an operational-mode command
  exit          Exit from current mode
  help          Provide help information
  no            Negate a command or set its defaults
  port-group    Configure a port-group
  profile       Configure Hardware Profile on a Switch
  pwd           Display current mode path
  system-mode   Set system mode
  top           Exit to top level and optionally run command
```

To display a list of commands that start with the same characters, type the characters followed by a question mark (**?**).

```
device# e?
Possible completions:
  end             Terminate configuration session
  event-handler   Event Handler Commands
  evpn            EVPN configuration.
  exit            Exit from current mode
```

To display the keywords and arguments associated with a command, enter the keyword followed by a space a then a question mark (?).

```
device# terminal ?
Possible completions:
 length    Sets Terminal Length for this session
 monitor   Enables terminal monitoring for this session
 no        Sets Terminal Length for this session to default :24.
 timeout   Sets the interval that the EXEC command interpreter wait for user input.
```

If the question mark (?) is typed within an incomplete keyword, but the keyword matches several keywords, the CLI displays help for all the matching keywords.

```
device# show l
Possible completions:
  lacp                  LACP commands
  license               Display license keys installed on the switch.
  linecard              Show linecard
  link-fault-signaling  Show Link Fault Signalling configs
  lldp                  Link Layer Discovery Protocol(LLDP).
  logging               Show logging
```

The CLI accepts abbreviations for commands. This example is the abbreviation for the **show qos interface all** command.

```
device# sh q i a
```

If the device does not recognize a command after you press **Enter**, an error message displays.

```
device# hookup
                ^
syntax error: unknown argument.
```

If you enter an incomplete command, an error message displays.

```
device# show
                    ^
syntax error: unknown argument.
```

Completing CLI commands

To complete the spelling of commands or keywords automatically, begin typing the command or keyword and then press **Tab**. For example, at the CLI command prompt, type `te` and press **Tab**:

```
device# te
```

The CLI displays the following command.

```
device# terminal
```

If there is more than one command or keyword associated with the characters typed, the CLI displays all choices. For example, at the CLI command prompt, type `show l` and press **Tab**.

```
device# show l

device# show l
Possible completions:
  lacp                  LACP commands
  license               Display license keys installed on the switch.
  linecard              Show linecard
  link-fault-signaling  Show Link Fault Signalling configs
  lldp                  Link Layer Discovery Protocol(LLDP).
  logging               Show logging
```

CLI keyboard shortcuts

The following table lists CLI keyboard shortcuts.

TABLE 1 SLX-OS CLI keyboard shortcuts

Keystroke	Description
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+B (or the left arrow key)	Moves the cursor back one character.
Ctrl+C	Escapes and terminates command prompts and ongoing tasks (such as lengthy displays), and displays a fresh command prompt.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+F (or the right arrow key)	Moves the cursor forward one character.
Ctrl+N (or the down arrow key)	Displays commands in the history buffer with the most recent command displayed last.
Ctrl+P (or the up arrow key)	Displays commands in the history buffer with the most recent command displayed first.
Ctrl+U or **Ctrl+X**	Deletes all characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word you typed.
Ctrl+Z	Returns to privileged EXEC mode. Using Ctrl+Z in privileged EXEC mode executes partial commands.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.

NOTE

In privileged EXEC mode, use the **show history** command to list the commands most recently entered. The device retains the history of the last 1000 commands entered for the current session.

Using CLI command output modifiers

You can filter the output of the CLI **show** commands by using the output modifiers described below.

TABLE 2 CLI command output modifiers

Output modifier	Description
append	Appends the output to a file.
redirect	Redirects the command output to the specified file.
include	Displays the command output that includes the specified expression.
exclude	Displays the command output that excludes the specified expression.
begin	Displays the command output that begins with the specified expression.
last	Displays only the last few lines of the command output.
tee	Redirects the command output to the specified file. Notice that this modifier also displays the command output.
until *string*	Ends the output when the output text matches the string.
count	Counts the number of lines in the output.
linnum	Enumerates the lines in the output.
more	Paginates the output.
nomore	Suppresses the pagination of the output.
FLASH	Redirects the output to flash memory.

Debug and system diagnostic commands

Debug and system diagnostic commands, such as "debug" and "show system internal" commands, are developed and intended for specialized troubleshooting.

Extreme Networks recommends that you work closely with Extreme technical support in executing such commands and interpreting their results.

NOTE
Not all diagnostic commands are documented.

Command shortcuts (aliases)

Aliases are command shortcuts that you can define globally or for individual user accounts.

Configuring global aliases

Global aliases (command shortcuts) are accessible to any logged-in user.

1. In privileged EXEC mode, enter the **configure terminal** command.

```
device# configure terminal
```

2. Enter the **alias-config** command to access alias configuration mode.

```
device(config)# alias-config
```

3. Enter the **alias** command, specifying the alias and its corresponding command.

```
device(config-alias-config)# alias ck "show clock"
```

4. Verify the alias.

```
device(config-alias-config)# exit
device(config)#  exit
device# ck
device#  show clock
2016-06-14 13:03:55 Etc/GMT
```

Configuring user-level aliases

User-level command aliases (command shortcuts) are defined for an individual user account.

1. In privileged EXEC mode, enter the **configure terminal** command.

```
device# configure terminal
```

2. Enter the **alias-config** command to access alias configuration mode.

```
device(config)# alias-config
```

3. Enter the **user** command to access user-alias configuration mode.

```
device(config-alias-config)# user jdoe
```

4. Enter the **alias** command, specifying the alias and its corresponding command.

```
device(config-user-jdoe)# alias int2 "interface ethernet 0/2"
```

5. Verify the alias.

NOTE

The following verification example assumes that the user jdoe defined the user-level alias "int2". If an admin defined the alias for this user, the example would show the admin logging out of the CLI and jdoe logging into the CLI.

```
device(config-alias-config)# exit
device(config-user-jdoe)# exit
device(config-alias-config)# exit
device(config)# int2

<Displayed automatically:>
device(config)#interface ethernet 0/2
device(conf-if-eth-0/2)#
```

Commands A - B

aaa accounting

Enables accounting for command or login information; information is forwarded to the accounting server.

Syntax

aaa accounting { **commands** | **exec** } **default start-stop** [**none** | **radius** | **tacacs+**]

no aaa accounting { **commands** | **exec** } **default start-stop** [**none** | **radius** | **tacacs+**]

Command Default

Accounting is disabled.

Parameters

commands
Causes command accounting.

exec
Causes login accounting.

default
Causes the sending of logged information to the default server.

start-stop
Causes the sending of a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.

none
Disables accounting services.

radius
Specifies using the RADIUS server for accounting.

tacacs+
Specifies using the TACACS+ server for accounting.

Modes

Global configuration mode

Usage Guidelines

Before enabling login (EXEC) or command accounting for RADIUS, at least one RADIUS server must be configured on the device.

In RADIUS command accounting:

- All command accounting packets are sent to the initial RADIUS server configured (rather than any RADIUS server used for authentication). When the initial server fails, packets are sent to the next configured server in round-robin fashion.
- Commands with a partial timestamp are not accounted.

The following configuration commands are not accounted:

- **abort**
- **end**
- **exit**
- **help**
- **no vlan**
- **service**
- **top**

The following operational commands are not accounted:

- **cipherset**
- **copy**
- **delete**
- **dir**
- **dot1x**
- **exit**
- **help**
- **history**
- **logout**
- **oscmd**
- **ping**
- **rename**
- **reload**
- **resequence**
- **send**
- **show cipherset**
- **show cli**
- **show file**
- **show history**
- **show netconf-state**
- **show parser dump**
- **show startup-config**
- **ssh**
- **telnet**
- **traceroute**

- **quit**
- **help**

The **no** form of the command disables accounting. You can also disable accounting by using the **aaa accounting** command specifying the **none** option.

Examples

The following example configures command accounting, with the CLI information being forwarded to the TACACS+ server.

```
device(config)# aaa accounting commands default start-stop tacacs+
```

The following example configures command accounting, with the CLI information being forwarded to the RADIUS server.

```
device(config)# aaa accounting commands default start-stop radius
```

The following example disables login accounting by specifying the **none** option; command accounting (when also configured) remains active.

```
device(config)# aaa accounting exec default start-stop none
```

The following example disables login accounting by using the **no aaa accounting** command; command accounting (when also configured) remains active.

```
device(config)# no aaa accounting exec default start-stop
```

History

Release version	Command history
18x.1.00	This command was introduced.

aaa authentication

Configures the AAA login sequence.

Syntax

aaa authentication login { **default** | **ldap** | **local** }

aaa authentication login { **radius** | **tacacs+** } { **local** | **local-auth-failback** }

no aaa authentication login

Command Default

The default server is Local.

Parameters

login

Specifies the type of server that will be used for authentication, authorization, and accounting (AAA) on the device. The local server is the default. Specify one of the following options:

default

Specifies the default mode (local server). Authenticates the user against the local database only. If the password does not match or the user is not defined, the login fails.

ldap

Specifies the Lightweight Directory Access Protocol (LDAP) servers.

local

Specifies to use the local device database if prior authentication methods are inactive.

radius

Specifies the RADIUS servers.

tacacs+

Specifies the TACACS+ servers.

local

Specifies to use the local device database if prior authentication methods are inactive.

local-auth-failback

Specifies to use the local device database if prior authentication methods are not active or if authentication fails.

Modes

Global configuration mode

Usage Guidelines

This command selects the order of authentication sources to be used for user authentication during the login process. Two sources are supported: primary and secondary. The secondary source of authentication is optional and will be used if the primary source fails or is not available.

The authentication mode can only be set and cannot be added or deleted. For example, to change a configuration from "radius local" to radius only, execute the **no aaa authentication login** command to resets the configuration to the default mode, and then reconfigure the AAA mode with the desired setting.

In a configuration with primary and secondary sources of authentication, the primary mode cannot be modified alone. For example, you cannot change from “radius local" or "radius local-auth-fallback” to “tacacs+ local" or "tacacs+ local-auth-fallback” respectively. First remove the existing configuration and then configure it to the required configuration.

Examples

To change the AAA server to TACACS+ using the local device database as a secondary source of authentication:

```
device(config)# aaa authentication login tacacs+ local
Broadcast message from root (pts/0) Tue Apr  5 16:34:12 2011...
```

To change the AAA server from TACACS+ and local to TACACS+ only (no secondary source):

```
device(config)# no aaa authentication login tacacs+ local
device(config)# aaa authentication login tacacs+
device(config)# do show running-config aaa
aaa authentication login tacacs+
```

History

Release version	Command history
18x.1.00	This command was introduced.

aaa command authorization

Allows a designated user to execute commands normally restricted to the administrator role.

Syntax

aaa command authorization { **none** | **tacacs+** [**local**]}

Command Default

AAA command authorization is disabled.

Parameters

none

Disables command authorization.

tacacs+

Enables command authorization for the user role.

local

Authorizes the command even if the TACACS+ server is offline or returns an error.

Modes

Global configuration mode

Usage Guidelines

At least one TACACS+ server must be configured on the device using the **tacacs-server host** command.

You must configure a server-side user role on the TACACS+ server. The following example assigns the user "Agnes" a single password for all types of login authentication.

```
user = tacuser {
        default service = permit
        chap = cleartext "password"
        service = exec {
            brcd-role = admin
        }
        cmd = show {
         deny vrf
         permit .*
        }
 }
```

Command authorization can be enabled only if at least one TACACS+ server is configured. Similarly, if command authorization is enabled, then the last TACACS+ server cannot be removed if it is the only server in the list.

Whenever a command is executed, an authorization request is sent to the configured TACACS+ server in a round-robin fashion. The TACACS+ server responds with an accept or reject based on the configuration. If server responds with a reject, the authorization fails and the command is not executed.

If the 'local' option is not selected and if all the configured TACACS+ servers are unreachable, or TACACS+ server responds with an error, then the command is not executed.

If the 'local' option is selected and if all the configured TACACS+ servers are unreachable, or TACACS+ server responds with an error, then the command is executed, but is based on the local role. However, the command fails if the TACACS+ server responds with a reject.

Use the **aaa authorization commands none** command to disable command authorization.

Limitations:

- Certificate Revocation List (CRL) is not supported.
- HA sync is not supported.

Examples

Example of activating authorization commands.

```
device# configure terminal
device(config)# aaa command authorization tacacs+
```

Example of deactivating authorization commands.

```
device# configure terminal
device(config)# aaa command authorization none
```

Example of activating authorization commands with the local option.

```
device# configure terminal
device(config)# aaa command authorization tacacs+ local
```

History

Release version	Command history
18x.1.00	This command was introduced.

acl-mirror

Defines a destination port or port-channel for ACL-based mirroring of a physical interface.

Syntax

acl-mirror source ethernet *slot* **/** *port* **destination** { **ethernet** *slot* **/** *port* | **port-channel** *index* }

no acl-mirror source ethernet *slot* **/** *port* **destination** { **ethernet** *slot* **/** *port* | **port-channel** *index* }

Command Default

No ACL mirror is defined.

Parameters

source
Specifies the interface for which you are defining a mirror.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

destination
Specifes the physical interface or port-channel mirror.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *index*
Specifies a port-channel interface.

Modes

Global configuration mode

Usage Guidelines

ACL mirroring applies to extended-ACL rules that include the **mirror** keyword.

ACL mirroring is supported only for ACLs applied to incoming traffic.

Only one destination port is supported.

To cancel an ACL mirroring destination, use the **no** form of this command.

Examples

The following example defines a physical port as mirror.

```
device# configure
device(config)# acl-mirror source ethernet 0/1 destination ethernet 0/2
```

The following example defines a port-channel as mirror.

```
device# configure
device(config)# acl-mirror source ethernet 0/1 destination port-channel 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

acl-policy

Accesses the ACL policy configuration mode, from which you can change the default settings regarding conflicting and duplicate ACL rules.

Syntax

acl-policy

Modes

Global configuration mode

Usage Guidelines

To return to global configuration mode, enter the **exit** command.

Examples

The following example accesses the ACL policy configuration mode and then disables the default restriction on duplicate rules within ACLs.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# allow-duplicate-rules
```

History

Release version	Command history
18x.1.00	This command was introduced.

action event-stream

Activates the event-stream action within the event-stream configuration mode.

Syntax

action event-stream

no action event-stream

Command Default

The action is not active.

Modes

Event-stream configuration mode.

Usage Guidelines

Use the **no action event-stream** command to halt the event stream action.

If an action oes not exist in the database, a new action is created validated. If the event-stream is already activated on the device, then adding or updating an event action also takes immediate effect.

Examples

Example for activating the event stream.

```
device# configure terminal
device(config)# telemetry profile event-stream profile1
device(config-event-stream-profile1)# action event-stream
```

Example for deactivating the event stream.

```
device# configure terminal
device(config)# telemetry profile event-stream profile1
device(config-event-stream-profile1)# no action event-stream
```

History

Release version	Command history
18x.1.00	This command was introduced.

action python-script

Specifies a Python file that runs when a trigger condition occurs.

Syntax

action python-script *file-name*

no action python-script *file-name*

Parameters

file-name

Specifies a Python script file name. Valid values range from 4 through 32 characters (including the **.py** extension). The first character must be alphabetic.

Modes

Event-handler configuration mode

Usage Guidelines

You can assign only one action to a given event-handler profile.

You can also specify the Python file as part of the **event-handler** command.

To change the file assigned to a profile, you do not need to enter the **no** form of this command. You only need to enter **action python-script** *file-name*, specifying the new file name.

Running this command copies the Python script file from the `flash://` directory to the database. After specifying a file for all relevant event-handler profiles, you can delete it from the `flash://` directory.

If the event-handler for which you are modifying this command is active on the device, the changes take effect with no need to de-activate and re-activate the event-handler.

A Python event-handler script runs only if all of the following occur:

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.
- In configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.
  - Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

If an event-handler profile is not activated, the **no** form of this command deletes its action.

Examples

The following example specifies Python files for two event-handler profiles.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)# action python-script example.py
device(config-event-handler-eventHandler1)# event-handler eventHandler2
device(config-event-handler-eventHandler2)# action python-script example2.py
```

History

Release version	Command history
18x.1.00	This command was introduced.

action-profile

Creates an action profile.

Syntax

action-profile *action-profile-name*

no action-profile

Parameters:

action-profile-name

Specifies the action profile name. An action profile can be up to 32 characters.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the corresponding configured action profile also its association with source and remote MEP pair.

Examples

This example shows how to create an action profile.

```
device# configure terminal
device (config-cfm)# y1731
device(config-cfm-y1731)# action-profile a1
device(config-cfm-y1731-action-profile-a1)# event ccm-up actions all
```

History

Release version	Command history
18x.1.00	This command was introduced.

action-timeout

Specifies the maximum number of minutes to wait for an action-script to complete execution.

Syntax

action-timeout *minutes*

no action-timeout

Command Default

No action timeout is defined.

Parameters

minutes

Specifies the number of minutes to wait for an action-script to complete execution. If you specify "0", no timeout is set. Valid timeout values are any positive integer.

Modes

Event-handler activation mode

Usage Guidelines

If the action-timeout expires, then script execution ends.

To restore the default setting of no timeout, enter the **no** form of this command.

Examples

The following example specifies an action timeout of 30 minutes.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# action-timeout 30
```

History

Release version	Command history
18x.1.00	This command was introduced.

activate (Telemetry collector)

Activates the Telemetry data stream to the collector.

Syntax

activate

no activate

Command Default

The collector is deactivated.

Modes

Telemetry streaming mode

Usage Guidelines

Activates the collector, which in turn begins streaming related telemetry information to the collector server.

Use the **no activate** command to disable streaming to the collector server.

Examples

Typical command execution.

```
device# configure terminal
device(config)# telemetry collector collector1
device(config-collector-collector1)# ip 10.24.12.87 port 8080
device(config-collector-collector1)# encoding json
device(config-collector-collector1)# profile system-profile default_system_utilization_statistics
device(config-collector-collector1)# activate
```

History

Release version	Command history
18x.1.00	This command was introduced.

activate (Telemetry server)

Activates the Telemetry server.

Syntax

activate

no activate

Command Default

The Telemetry server is deactivated.

Modes

Telemetry configuration mode

Usage Guidelines

Use the **no activate** command to disable the server.

This command activates the Telemetry server so that the data stream is collected.

Examples

Typical command execution.

```
device# configure terminal
device(config)# telemetry server
device(config-server-mgmt-vrf)# activate
device(config-server-mgmt-vrf)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

activate (VXLAN overlay gateway)

Activates a VXLAN overlay gateway instance.

Syntax

activate

no activate

Command Default

By default, a gateway is not activated during initial configuration.

Modes

Overlay gateway configuration mode

Usage Guidelines

It is recommended that you configure all gateway parameters before activating the gateway. This operation enables all tunnels that are associated with this gateway.

The following conditions that must be in place before you can execute the **activate** command:

- Loopback interfaces must be configured on all gateways. Refer to the **interface loopback** command,
- The IP address of the VXLAN gateway must be configured. Refer to the **ip interface** command.

Use the **no activate** command in VXLAN overlay gateway configuration mode to deactivate the gateway. All associated tunnels are also deactivated.

Examples

The following example activates a VXLAN gateway named gateway1. The gateway was previously configured by means of the **overlay-gateway** command:

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# activate
```

History

Release version	Command history
18x.1.00	This command was introduced.

additional-paths

Enables an additional-paths capability for all peers in a Border Gateway Protocol (BGP) address family.

Syntax

additional-paths { **receive** [**send**] | **send** }

no additional-paths receive

no additional-paths send

Command Default

Peer devices configured under a BGP address family are not capable of receiving or sending additional-paths.

Parameters

receive
Enables all peer devices configured under a BGP address family to receive additional-paths.

send
Enables all peer devices configured under a BGP address family to send additional-paths.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

NOTE
Changes to the additional-paths capability for peers in a BGP address family take effect only after the BGP session is restarted.

Peers exchange and negotiate additional-path capability during session establishment.

Additional-paths can be enabled as receive only, send only, or both receive and send.

The **no** form of the command disables the specified (receive or send) additional-paths capability.

To remove the configuration when both the **receive** and **send** options have been set, you should enter both the **no additional-paths** command, specifying the **receive** option to disable the receive additional-paths capability, and the **no additional-paths** command, specifying the **send** option to disable the send additional-paths capability.

Examples

The following example shows how to enable peers configured under the IPv4 unicast address family to both receive and send additional-paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# additional-paths receive send
```

The following example shows how to disable the capability to receive additional-paths for all peers in the IPv4 unicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# no additional-paths receive
```

History

Release version	Command history
18x.1.00	This command was introduced.

additional-paths select

Configures routes that are eligible for selection as additional-paths by peers configured under a Border Gateway Protocol (BGP) address family.

Syntax

additional-paths select { **all** [**best** *num*] [**group-best**] | **best** *num* | **group-best** }

no additional-paths select all

no additional-paths select best *num*

no additional-paths select group-best

Parameters

all

Causes all routes to be eligible for selection as additional-paths. A maximum of 16 routes is allowed.

best *num*

Specifies the number of best paths allowed for selection as additonal-paths. The number ranges from 2 through 16.

group-best

Causes all group-best paths to be eligible for selection as additional-paths. Only routes with a rank less than or equal to 16 are allowed. Even when it is the group best, a route with a rank greater than 16 is not eligible for selection as an additional path.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **all**, **best**, and **group-best** options are not mutually exclusive. When you perform a combination of these commands, the combined configuration is applied to the BGP address family.

The **no** form of the command removes the specified configuration.

When more than one option is configured, it is recommended that you disable each configured option separately; for example, disable the **all** configuration by using the **no additional-paths select** command specifying the **all** option, and so on.

Examples

The following example shows how to configure all (up to a maximum of 16) routes to be eligible for selection as additional-paths by all peers in the IPv4 unicast address family.

```
device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-router-ipv4u)# additional-paths select all
```

The following example shows how to restore the default configuration when the **all**, **best**, and **group-best** options were previously configured for the IPv4 unicast address family. It is recommended that you disable each configuration option separately.

```
device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-router-ipv4u)# no additional-paths select all
device(config-bgp-router-ipv4u)# no additional-paths select best 2
device(config-bgp-router-ipv4u)# no additional-paths select group-best
```

History

Release version	Command history
18x.1.00	This command was introduced.

address-family unicast (BGP)

Enables the IPv4 or IPv6 address family configuration mode to configure a variety of BGP unicast routing options.

Syntax

address-family { **ipv4** | **ipv6** } **unicast** [**vrf** *vrf-name*]

no address-family { **ipv4** | **ipv6** } **unicast** [**vrf** *vrf-name*]

Command Default

Disabled.

Parameters

ipv4
Specifies an IPv4 address family.

ipv6
Specifies an IPv6 address family.

vrf *vrf-name*
Specifies a VRF instance.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove IPv4 or IPv6 address family configurations from the device.

Examples

The following example enables BGP IPv4 address-family configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)#
```

The following example enables BGP IPv6 address-family configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)#
```

The following example enables BGP IPv4 address-family configuration mode for VRF "green".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf green
device(config-bgp-ipv4u-vrf)#
```

This example enables BGP IPv6 address-family configuration mode for VRF "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

advertise dot1-tlv

Advertises globally to any attached device IEEE 802.1 organizationally specific Type, Length, Values (TLV) values, or for a specific LLDP profile.

Syntax

advertise dot1-tlv

no advertise dot1-tlv

Command Default

Advertisement is disabled.

Modes

Protocol LLDP and profile configuration modes

Usage Guidelines

Enter **no advertise dot1-tlv** to return to the default setting.

Examples

The following example advertises TLV configuration for IEEE 802.1

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# advertise dot1-tlv
device(conf-lldp)#
```

The following example advertises TLV configuration for IEEE 802.1 for a specific LLDP profile.

```
device(conf-lldp)# profile test1
device(config-profile-test1)# advertise dot1-tlv
device(conf-profile-test1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

advertise dot3-tlv

Advertises to any attached device IEEE 802.3 organizationally specific Type, Length, Values (TLV) values, or for a specific LLDP profile.

Syntax

advertise dot3-tlv

no advertise dot3-tlv

Command Default

Advertisement is disabled.

Modes

Protocol LLDP and profile configuration modes.

Usage Guidelines

Enter **no advertise dot3-tlv** to return to the default setting.

Examples

The following example advertises TLV configuration for IEEE 802.3.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# advertise dot3-tlv
device(conf-lldp)#
```

The following example advertises TLV configuration for IEEE 802.3 for a specific LLDP profile.

```
device(conf-lldp)# profile test1
device(config-profile-test1)# advertise dot3-tlv
device(conf-profile-test1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

advertise optional-tlv

Advertises the optional Type, Length, and Values (TLV) values, or for a specific LLDP profile.

Syntax

advertise optional-tlv { **management-address** | **port-description** | **system-capabilities** | **system-description** | **system-name** }

no advertise optional-tlv

Command Default

Advertisement is disabled.

Parameters

management-address
Advertises the management address of the system.

port-description
Advertises the user-configured port.

system-capabilities
Advertises the capabilities of the system.

system-description
Advertises the system firmware version and the current image running on the system.

system-name
Advertises the name of the system.

Modes

Protocol LLDP and profile configuration modes

Usage Guidelines

Enter **no advertise optional-tlv** to return to the default setting.

Examples

The following example advertises the management address of the system and the user-configured port.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# advertise optional-tlv ?
Possible completions:
  management-address    Management Address TLV
  port-description      Port-Description TLV
  system-capabilities   System Capabilities TLV
  system-description    System Description
  system-name           System Name TLV
device(conf-lldp)# advertise optional-tlv management-address ?
Possible completions:
  port-description      Port-Description TLV
  system-capabilities   System Capabilities TLV
  system-description    System Description
  system-name           System Name TLV
device(conf-lldp)# advertise optional-tlv management-address port-description
device(conf-lldp)#
```

The following example advertises the management address of the system for a specific LLDP profile.

```
device(conf-lldp)# profile test1
device(config-profile-test1)# advertise optional-tlv ?
Possible completions:
  management-address    Management Address TLV
  port-description      Port-Description TLV
  system-capabilities   System Capabilities TLV
  system-description    System Description
  system-name           System Name TLV
device(conf-profile-test1)# advertise optional-tlv management-address
device(conf-profile-test1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

advertise-backup

Enables a backup VRRP router to send advertisement frames to the master VRRP router.

Syntax

advertise-backup

no advertise-backup

Command Default

Advertisement is disabled.

Modes

Virtual-router-group configuration mode

Usage Guidelines

If a backup router is enabled to send advertisement frames, the frames are sent every 60 seconds.

This command can be used for VRRP-E, but not for VRRP.

Enter **no advertise backup** to return to the default setting (no periodic transmission).

Examples

To enable the backup VRRP routers to send advertisement frames to the master VRRP router:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 1
device(config-vrrp-extended-group-1)# advertise-backup
```

History

Release version	Command history
18x.1.00	This command was introduced.

advertise-best-external

Stores and advertises the best external route for a Border Gateway Protocol (BGP) address family.

Syntax

advertise-best-external

no advertise-best-external

Command Default

The best external route for a BGP address family is not stored or advertised.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default configuration.

The **advertise-best-external** command enables storing and advertising of the best external route under an address family; the best external route is advertised in addition to the best route.

Examples

The following example shows how to store and advertise the best external route under the IPv4 address family in unicast mode.

```
device# configure terminal
device(bgp)# address-family ipv4 unicast
device(config-bgp)# advertise-best-external
```

History

Release version	Command history
18x.1.00	This command was introduced.

advertisement-interval (VRRP)

Configures the interval at which the master VRRP router advertises its existence to the backup routers.

Syntax

advertisement-interval *range*

Command Default

1 second for version 2, 1000 milliseconds for version 3.

Parameters

range

Interval at which the master VRRP router advertises its existence to the backup routers. Valid values range from 1 through 255 seconds for VRRPv2 and from 100 through 40900 milliseconds for VRRPv3.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This interval is the length of time, in seconds, between each advertisement sent from the master to its backup VRRP routers. The advertisement notifies the backup routers that the master is still active. If the backup routers do not receive an advertisement from the master in a designated amount of time, the backup with the highest priority can assume the role of master.

This command can be used for either VRRP or VRRP-E and for VRRPv3 and VRRP-Ev3.

Examples

To set the advertisement interval to 30 seconds for VRRP-E group 10:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 10
device(config-vrrp-extended-group-10)# advertisement-interval 30
```

To set the advertisement interval to 3000 milliseconds for VRRP-Ev3 group 19:

```
device# configure terminal
device(config)# interface ve 2019
device(config-ve-2019)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-19)# advertisement-interval 3000
```

History

Release version	Command history
18x.1.00	This command was introduced.

advertisement-interval-scale

Configures subsecond intervals at which the master VRRP-Ev3 device advertises its existence to the backup routers.

Syntax

advertisement-interval-scale *scale*

Command Default

The default advertisement interval scale is 1.

Parameters

scale

Number representing the scale of the division of a configured interval at which the master VRRP-Ev3 device advertises its existence to the backup devices. Valid values are 1, 2, 5 and 10.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This command scales the advertisement interval of the master VRRP-Ev3 device as configured by the **advertisement-interval** command. A value of 1, 2, 5, or 10 can be set and the existing advertisement interval value is divided by the scaling value, for example, if the advertisement interval is set to 1 second and the scaling value is set to 10, the new advertisement interval is 100 milliseconds. When all the advertisement intervals in a VRRP-Ev3 session are scaled, subsecond VRRP-Ev3 convergence is possible if a master fails. The advertisement notifies the backup devices that the master is still active. If the backup devices do not receive an advertisement from the master in a designated amount of time, the backup device with the highest priority can assume the role of master. Using subsecond advertising intervals, subsecond device redundancy can be achieved.

This command is only supported by VRRP-Ev3.

Examples

To set the scaling of the advertisement interval to 500 milliseconds for VRRP-Ev3 group 19:

```
device# configure terminal
device(config)# interface ve 2019
device(config-ve-25)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-10)# advertisement-interval 1
device(config-vrrp-extended-group-10)# advertisement-interval-scale 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

aggregate-address (BGP)

Configures the device to aggregate routes from a range of networks into a single network prefix.

Syntax

aggregate-address { *ip-addr ip-mask* | *ipv6-addr ipv6-mask* } [**advertise-map** *map-name* | **as-set** | **attribute-map** *map-name* | **summary-only** | **suppress-map** *map-name*]

no aggregate-address { *ip-addr ip-mask* | *ipv6-addr ipv6-mask* } [**advertise-map** *map-name* | **as-set** | **attribute-map** *map-name* | **summary-only** | **suppress-map** *map-name*]

Command Default

The address aggregation feature is disabled. By default, the device advertises individual routes for all networks.

Parameters

ip-addr
IPv4 address.

ip-mask
IPv4 mask.

ipv6-addr
IPv6 address.

ipv6-mask
IPv6 mask.

advertise-map
Causes the device to advertise the more-specific routes in the specified route map.

map-name
Specifies a route map to be consulted. Range is from 1 through 63 ASCII characters.

as-set
Causes the device to aggregate AS-path information for all routes in the aggregate routes from a range of networks into a single network prefix.

attribute-map
Causes the device to set attributes for the aggregate routes according to the specified route map.

map-name
Specifies a route map to be consulted.

summary-only
Prevents the device from advertising more-specific routes contained within the aggregate route.

suppress-map
Prevents the more-specific routes contained in the specified route map from being advertised.

map-name
Specifies a route map to be consulted.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to restore the defaults.

Examples

The following example aggregates routes from a range of networks into a single network prefix under the IPv6 address family and advertises the paths for this route as AS_SET.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# aggregate-address 2001:db8::/32 as-set
```

History

Release version	Command history
18x.1.00	This command was introduced.

alias

Configures global or user-level aliases for device commands.

Syntax

alias *alias-name expansion*

no alias *alias-name*

Parameters

alias-name

Specifies the alias name. The number of characters can be from 1 through 255.

expansion

Specifies the CLI command to be triggered when the alias is entered. If the command is more than one word, type double quotes (") around the command. The number of characters can be from 1 through 1023.

Modes

Alias configuration mode

User-alias configuration mode

Usage Guidelines

Global aliases are available to all users.

User-level aliases are available only for a specified user.

In the alias configuration mode, to delete a global alias use the **no** form of his command.

In the user-alias configuration mode, to delete a user alias use the **no** form of his command.

Examples

The following example defines `ck` as a global alias that enters the **show clock** command.

```
device# configure terminal
device(config)# alias-config
device(config-alias-config)# alias ck "show clock"
```

For the user jdoe, the following example defines `sv` as a user-level alias that enters the **show version** command.

```
device# configure terminal
device(config)# alias-config
device(config-alias-config)# user jdoe
device(config-user-jdoe)# alias sv "show version"
```

History

Release version	Command history
18x.1.00	This command was introduced.

alias-config

Launches the alias configuration mode, enabling you to define aliases.

Syntax

alias-config

no alias-config [**alias** | **user** *username*]

Parameters

alias
(For the **no** option) Deletes all global aliases.

user *username*
(For the **no** option) Deletes all aliases defined for the specified user.

Modes

Global configuration mode

Usage Guidelines

From the alias configuration mode—which you access by entering this command—you can manage global aliases. From that mode, you can also access the user-alias configuration mode for a specified user, from which you can manage aliases for that user.

To delete all global aliases, use the **no alias-config alias** form of this command.

To delete all aliases defined for a specified user, use the **no alias-config user** form of this command.

Examples

The following example accesses the alias configuration mode. It then defines `ck` as a global alias for the **show clock** command.

```
device# configure terminal
device(config)# alias-config
device(config-alias-config)# alias ck "show clock"
```

The following example deletes all aliases defined for the user jdoe.

```
device# configure terminal
device(config)# no alias-config user jdoe
```

History

Release version	Command history
18x.1.00	This command was introduced.

allow-conflicting-rules

Towards editing ACLs, disables the default restriction on conflicting rules within an ACL. You can then create a conflicting rule before deleting the previous version.

Syntax

allow-conflicting-rules

no allow-conflicting-rules

Command Default

Conflicting rules are not allowed within an ACL.

Modes

ACL policy mode

Usage Guidelines

If the only difference between two rules is that one is a **deny** and the other a **hard-drop**, they are not considered conflicting. However, they are considered duplicates; refer to the **allow-duplicate-rules** topic.

Towards modifying ACL rules, you do not need to first remove ACLs from interfaces. Changes are implemented "on the fly," with no gap in protection.

We recommend that after ACL-editing sessions towards which you enabled **allow-conflicting-rules**, restore the default setting—by entering the **no allow-conflicting-rules** command.

Entering **no allow-conflicting-rules** launches a check of all ACLs for conflicting rules. If you did not immediately restore the default setting, and created ACLs with conflicting rules, you will need to delete conflicting rules before the software accepts **no allow-conflicting-rules**.

Examples

When modifying ACLs by changing a rule from **permit** to **deny** or **hard-drop**—or vice versa—the following flow is typical.

1. Enter the **show running-config** command to display the rules in the ACL that you need to modify.

```
device# show running-config mac access-list extended mac1
mac access-list extended mac1
 seq 10 permit host 0001.0001.0001 any
 seq 20 deny host 0001.0001.0002 any count
 seq 30 hard-drop host 0001.0001.0003 any mirror
```

2. Enter the **allow-conflicting-rules** command.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# allow-conflicting-rules
```

3. In the ACL that you need to modify, create the new rule and then delete the old rule.

```
device(config-acl-policy)# exit
device(config)# mac access-list mac1
device(conf-macl-ext)# seq 21 permit host 0001.0001.0002 any count
device(conf-macl-ext)# no seq 20
```

4. Enter the **no allow-conflicting-rules** command to restore the default setting.

```
device(conf-macl-ext)# exit
device(config)# acl-policy
device(config-acl-policy)# no allow-conflicting-rules
```

History

Release version	Command history
18x.1.00	This command was introduced.

allow-duplicate-rules

Towards editing ACLs, disables the default restriction on duplicate rules within an ACL. You can then create a duplicate rule at a new sequence before deleting the previous version.

Syntax

allow-duplicate-rules

no allow-duplicate-rules

Command Default

Duplicate rules are not allowed within an ACL.

Modes

ACL policy mode

Usage Guidelines

If the only difference between two rules is that one is a **deny** and the other a **hard-drop**, they are considered duplicates.

Towards modifying ACL rules, you do not need to first remove ACLs from interfaces. Changes are implemented "on the fly," with no gap in protection.

We recommend that after ACL-editing sessions towards which you enabled **allow-duplicate-rules**, restore the default setting—by entering the **no allow-duplicate-rules** command.

Entering **no allow-duplicate-rules** launches a check of all ACLs for duplicate rules. If you did not immediately restore the default setting, and created ACLs with duplicate rules, you will need to delete duplicates before the software accepts **no allow-duplicate-rules**.

Examples

When editing ACLs by duplicating a rule into a new sequence and then deleting the original rule, the following flow is typical.

1. Enter the **show running-config** command to display the rules in the ACL that you need to modify.

```
device# show running-config mac access-list extended mac1
mac access-list extended mac1
 seq 10 permit host 0001.0001.0001 any
 seq 20 deny host 0001.0001.0002 any count
 seq 30 hard-drop host 0001.0001.0003 any mirror
```

2. Enter the **allow-duplicate-rules** command.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# allow-duplicate-rules
```

3. In the ACL that you need to modify, create the duplicate rule—specifying the new sequence number—and then delete the old rule.

```
device(config-acl-policy)# exit
device(config)# mac access-list mac1
device(conf-macl-ext)# seq 11 hard-drop host 0001.0001.0003 any mirror
device(conf-macl-ext)# no seq 30
```

4. Enter the **no allow-duplicate-rules** command to restore the default setting.

```
device(conf-macl-ext)# exit
device(config)# acl-policy
device(config-acl-policy)# no allow-duplicate-rules
```

History

Release version	Command history
18x.1.00	This command was introduced.

always-compare-med

Configures the device always to compare the Multi-Exit Discriminators (MEDs), regardless of the autonomous system (AS) information in the paths.

Syntax

always-compare-med

no always-compare-med

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command disallows the comparison of the MEDs for paths from neighbors in different autonomous systems.

Examples

The following example configures the device always to compare the MEDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# always-compare-med
```

History

Release version	Command history
18x.1.00	This command was introduced.

always-propagate

Enables the device to advertise BGP routes even though they are not installed in the RIB Manager.

Syntax

always-propagate

no always-propagate

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

This example configures the device to advertise routes that are not installed in the RIB manager.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# always-propagate
```

This example configures the device to reflect advertise that are not installed in the RIB manager in IPv6 address-family unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# always-propagate
```

This example configures the device to advertise routes that are not installed in the RIB manager in a nondefault VRF instance.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# always-propagate
```

History

Release version	Command history
18x.1.00	This command was introduced.

anycast-rp

Configures PIM anycast rendezvous points (RPs) in IPv4 and IPv6 multicast domains.

Syntax

anycast-rp *rp-address*

no anycast-rp *rp-address*

Command Default

PIM anycast RPs are not configured.

Parameters

rp-address

Specifies a shared RP address used among multiple PIM routers.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command removes the anycast RP configuration.

PIM Anycast RP is a method of providing load balancing and fast convergence to PIM RPs in an IPv4 multicast domain. The RP address of the Anycast RP is a shared address used among multiple PIM routers, known as PIM RP. The PIM RP routers create an Anycast RP set. Each router in the Anycast RP set is configured using two IP addresses; a shared RP address in their loopback address and a separate, unique ip address. The loopback address must be reachable by all PIM routers in the multicast domain. The separate, unique IP address is configured to establish static peering with other PIM routers and communication with the peers.

When the source is activated in a PIM Anycast RP domain, the PIM First Hop (FH) will register the source to the closet PIM RP. The PIM RP follows the same MSDP Anycast RP operation by decapsulating the packet and creating the (s,g) state. If there are external peers in the Anycast RP set, the router will re-encapsulate the packet with the local peering address as the source address of the encapsulation. The router will unicast the packet to all Anycast RP peers. The re-encapsulation of the data register packet to Anycast RP peers ensures source state distribution to all RPs in a multicast domain.

Examples

The following example shows how to configure PIM anycast RP.

```
device(config-pim-router)# anycast-rp101.101.101.101 my-anycast-rps
device(config-pim-router)# exit
device(config)# ip prefix-list my-anycast-rpspermit 1.1.1.1/32
device(config)# ip prefix-list my-anycast-rpspermit 2.2.2.2/32
device(config)# interface loopback 1
device(config-Loopback-1)# ip address 1.1.1.1/32
device(config-Loopback-1)# ip pim-sparse
device(config)#interface loopback 2
device(config-Loopback-2)# ip address 2.2.2.2/32
device(config-Loopback-2)# ip pim-sparse
device(config-Loopback-11)# ip address 101.101.101.101/32
device(config-Loopback-11# ip pim-sparse
```

History

Release version	Command history
18x.1.00	This command was introduced.

area authentication (OSPFv3)

Enables authentication for an OSPF Version 3 (OSPFv3) area.

Syntax

area { *A.B.C.D* | *decimal* } **authentication spi** *value* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** *key*

no area { *A.B.C.D* | *decimal* } **authentication spi** *value*

Command Default

Authentication is not enabled on an area.

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format.

spi
Specifies the Security Policy Index (SPI).

value
Specifies the Security Policy Index (SPI) value. Valid values range from decimal numbers 512 through 4294967295

ah
Specifies authentication header (ah) as the protocol to provide packet-level security.

esp
Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null
Specifies that the ESP payload is not encrypted.

hmac-md5
Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPF area.

hmac-sha1
Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPF area.

key
Number used in the calculation of the message digest.

key
The 40 hexadecimal character key.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Enter **no area authentication spi** to remove an authentication specification for an area from the configuration.

Examples

The following example enables ah and MD5 authentication for an OSPF area, setting a SPI value of 750.

```
device# configure termnial
device(config)# ip router-id 10.1.2.3
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 0 authentication spi 750 ah hmac-md5 key
abcef12345678901234fedcba098765432109876
```

The following example enables esp and SHA-1 authentication for an OSPF area, setting a SPI value of 900.

```
device# configure terminal
device(config)# ip router-id 10.1.2.3
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 0 authentication spi 900 esp null hmac-md5 sha1
abcef12345678901234fedcba098765432109876
```

History

Release version	Command history
18x.1.00	This command was introduced.

area nssa (OSPFv2)

Creates a not-so-stubby area (NSSA) or modifies its parameters.

Syntax

area { *ip-addr* | *decimal* } **nssa** { *metric* [**no-summary**] | **default-information-originate** }

no area nssa

Command Default

No areas are created.

Parameters

ip-addr
Area address in IP address format.

decimal
Area address In decimal format.

metric
Additional cost for using a route to or from this area.

no-summary
When configured on the NSSA area border router (ABR), this parameter prevents any Type 3 and Type 4 summary link-state advertisement (LSA) from being injected into the area. The only exception is that a default route is injected into the NSSA by the ABR, and strictly as a Type 3 LSA (not a Type 7, because that could cause intra-AS traffic to get routed out the AS). This makes the NSSA an NSSA totally stubby area, which can only have Type 1, 2 and 7 LSAs.
Note: This parameter is disabled by default, which means the default route must use a Type 7 LSA.

default-information-originate
When configured on the ABR, this parameter injects a Type 7 default route into the NSSA area. As a result, the other NSSA routers install the default route through the advertising NSSA ABR. By default the NSSA ABR does not originate a default route to the NSSA.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

NSSAs are typically needed when one-way transmission of Type-5 LSAs (out of the area) is desired but injection of the same LSAs into the area is not acceptable.

Once created, the type of the area cannot be changed. The only exception to this rule is that an NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

The **no** form of the command deletes a NSSA.

Examples

The following example sets an additional cost of 5 on an NSSA identified as 2, includes the no-summary parameter, and prevents the device from importing type 3 and type 4 summary LSAs into the NSSA area.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 2 nssa 5 no-summary
```

History

Release version	Command history
18x.1.00	This command was introduced.

area nssa (OSPFv3)

Creates a not-so-stubby area (NSSA) or modifies its parameters.

Syntax

area { *ip-addr* | *decimal* } **nssa** [*metric*] [**default-information-originate** [**metric** *num*] [**metric-type** { **type1** | **type2** }]] [**no-redsitribution**] [**no-summary**] [**translator-always**] [**translator-interval** *interval*]

no area nssa

Command Default

No areas are created.

Parameters

ip-addr
Area address in IP address format.

decimal
Area address in decimal format.

metric
Additional cost for using a route to or from this area. Valid values range from 1 through 1048575.

default-information-originate
When configured on the ABR, this parameter injects a Type 7 default route into the NSSA area. As a result, the other NSSA routers install the default route through the advertising NSSA ABR. By default the NSSA ABR does not originate a default route to the NSSA.

metric-type
Specifies how the cost of a neighbor metric is determined.

type1
The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.

type2
The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

no-redistribution
The no-redistribution parameter prevents an NSSA ABR from generating external (type-7) LSA into a NSSA area. This is used in the case where an ASBR should generate type-5 LSA into normal areas and should not generate type-7 LSA into a NSSA area. By default, redistribution is enabled in a NSSA.

no-summary
When configured on the NSSA area border router (ABR), this parameter prevents any Type 3 and Type 4 summary link-state advertisement (LSA) from being injected into the area. The only exception is that a default route is injected into the NSSA by the ABR, and strictly as a Type 3 LSA (not a Type 7, because that could cause intra-AS traffic to get routed out the AS). This makes the NSSA a NSSA totally stubby area, which can only have Type 1, 2 and 7 LSAs.
Note: This parameter is disabled by default, which means the default route must use a Type 7 LSA.

translator-always

Configures the translator-role. When configured on an ABR, this causes the router to unconditionally assume the role of a NSSA translator. By default, translator-always is not set, the translator role by default is candidate.

translator-interval *interval*

Configures the time interval for which an elected NSSA translator continues to perform its duties even after its NSSA translator role has been disposed by another router. Valid values range from 10 through 60 seconds. By default the stability-interval is 40 seconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

NSSAs are typically needed when one-way transmission of Type-5 LSAs (out of the area) is desired but injection of the same LSAs into the area is not acceptable.

Once created, the type of the area cannot be changed. The only exception to this rule is that a NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

The **no** form of the command deletes a NSSA.

Examples

The following example sets an additional cost of 4 on a NSSA identified as 8 (in decimal format), and prevents any Type 3 or Type 4 summary LSAs from being injected into the area.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 8 nssa 4 no-summary
```

History

Release version	Command history
18x.1.00	This command was introduced.

area prefix-list (OSPFv2)

Filters prefixes advertised in type 3 link-state advertisements (LSAs) between OSPFv2 areas of an area border router (ABR).

Syntax

area { *ip-addr* | *decimal* } **prefix-list** *name* { **in** | **out** }

no area { *ip-addr* | *decimal* } **prefix-list** *name* { **in** | **out** }

Parameters

ip-addr
Area address in IP address format.

decimal
Area address in decimal format.

prefix-list *name*
Specifies a prefix-list between 1 and 32 characters.

in
Specifies that the prefix list is applied to prefixes advertised to the specified area from other areas.

out
Specifies that the prefix list is applied to prefixes advertised out of the specified area to other areas.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

This command is only applicable to ABRs. The **no** form of the command changes or cancels the configured filter and advertises all type 3 LSAs.

Examples

The following example applies a prefix list to type 3 LSAs advertised out of an area with the area-id 10.1.1.1.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 10.1.1.1 prefix-list myprefixlist out
```

The following example applies a prefix list to type 3 LSAs advertised in to an area with the area-id 10.1.1.1.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 10.1.1.1 prefix-list myprefixlist in
```

History

Release version	Command history
18x.1.00	This command was introduced.

area range (OSPFv2)

Specifies area range parameters on an area border router (ABR).

Syntax

area { *A.B.C.D* | *decimal* } **range** *E.F.G.H I.J.K.L* **advertise** [**cost** *cost_value*]

area { *A.B.C.D* | *decimal* } **range** *E.F.G.H I.J.K.L* **not-advertise** [**cost** *cost_value*]

area { *A.B.C.D* | *decimal* } **range** *E.F.G.H I.J.K.L* **cost** *cost_value*

no area range

Parameters

A.B.C.D
: Area address in IP address format.

decimal
: Area address in decimal format.

E.F.G.H I.J.K.L
: Specifies the IP address and mask portion of the range. All network addresses that match this network are summarized in a single route and advertised by the ABR.

advertise
: Sets the address range status to *advertise* and generates a Type 3 summary LSA.

cost *cost_value*
: Sets the cost value for the area range. This value is used as the generated summary LSA cost. The range for *cost_value* is 1 to 6777214. If this value is not specified, the cost value is the default range metric calculation for the generated summary LSA cost.

not-advertise
: Sets the address range status to DoNotAdvertise; the Type 3 LSA is suppressed, and the component networks remain hidden from other networks. This setting is used to temporarily pause route summarization from the area.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Use this command only on ABRs to specify route summarization for an existing area. The result is that a single summary route is advertised to other areas by the ABR, in the form of a Type 3 LSA. Routing information is condensed at area boundaries and external to the area, and only a single route is advertised for each address range.

An example of when you might want to use this command is if you have many small networks advertised from area 0 to any other area, or from any non-backbone area into the backbone. This command gives you a summary route instead of many

smaller routes. In an area, the OSPF database on each router must be an exact copy of the databases of the other routers. This means that no summarization is allowed within the area.

The **no** form of the command disables the specification of range parameters on an ABR.

Examples

The following example advertises to Area 3 all the addresses on the network 10.1.1.0 10.255.255.0 in the ABR you are signed into.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 3 range 10.1.1.0 10.255.255.0 advertise
```

History

Release version	Command history
18x.1.00	This command was introduced.

area range (OSPFv3)

Specifies area range parameters on an area border router (ABR).

Syntax

area { *ip-addr* | *decimal* } **range** *ipv6 address/mask* [**advertise** | **not-advertise**] [**cost** *cost_value*]

no area range

Parameters

ip-addr
Area address in IP address format.

decimal
Area address in decimal format.

ipv6 address/mask
Specifies the IPv6 address in dotted-decimal notation and the IPv6 mask in CIDR notation. All network addresses that match this network are summarized in a single route and advertised by the ABR.

advertise
Sets the address range status to *advertise* and generates a Type 3 summary LSA.

cost *cost_value*
Sets the cost value for the area range. This value is used as the generated summary LSA cost. The range for *cost_value* is 1 to 6777214. If this value is not specified, the cost value is the default range metric calculation for the generated summary LSA cost.

not-advertise
Sets the address range status to DoNotAdvertise; the Type 3 LSA is suppressed, and the component networks remain hidden from other networks. This setting is used to temporarily pause route summarization from the area.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Use this command only on ABRs to specify route summarization for an existing area. The result is that a single summary route is advertised to other areas by the ABR, in the form of a Type 3 LSA. Routing information is condensed at area boundaries and external to the area, and only a single route is advertised for each address range.

An example of when you might want to use this command is if you have many small networks advertised from area 0 to any other area, or from any non-backbone area into the backbone. This command gives you a summary route instead of many smaller routes. In an area, the OSPF database on each router must be an exact copy of the databases of the other routers. This means that no summarization is allowed within the area.

The **no** form of the command disables the specification of range parameters on an ABR.

Examples

The following example advertises to Area 3 all the addresses on the network 2001:db8:8::/45 in the ABR you are signed into.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 3 range 2001:db8:8::/45 advertise
```

History

Release version	Command history
18x.1.00	This command was introduced.

area stub (OSPFv2)

Creates or deletes a stub area or modifies its parameters.

Syntax

area { *ip-addr* | *decimal* } **stub** *metric* [**no-summary**]

no area stub

Command Default

No areas are created.

Parameters

A.B.C.D

Area address in IP address format.

decimal

Area address In decimal format.

metric

Additional cost for using a route to or from this area. Valid values range from 1 through 6777215.

no-summary

When configured on the ABR, this parameter prevents any Type 3 and Type 4 summary LSAs from being injected into the area. The only exception is that a default route is injected into the stub/totally stubby area by the ABR as a Type 3 LSA. Enabling this parameter makes the area a so-called totally stubby area, which can only have Types 1 and 2. This parameter is disabled by default.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Once created, the type of the area cannot be changed. The only exception to this rule is that a NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

The **no** form of the command deletes a stub area.

Examples

The following example sets an additional cost of 5 on a stub area called 2.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 2 stub 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

area stub (OSPFv3)

Creates or deletes a stub area or modifies its parameters.

Syntax

area { *ip-addr* | *decimal* } **stub** *metric*

area { *ip-addr* | *decimal* } **stub no-summary** *metric*

no area stub

Command Default

No areas are created.

Parameters

ip-addr
Area address in IP address format.

decimal
Area address In decimal format.

metric
Additional cost for using a route to or from this area. Valid values range from 3 through 1048575.

no-summary
When configured on the ABR, this parameter prevents any Type 3 and Type 4 summary LSAs from being injected into the area. The only exception is that a default route is injected into the stub/totally stubby area by the ABR as a Type 3 LSA. Enabling this parameter makes the area a so-called totally stubby area, which can only have Types 1 and 2. This parameter is disabled by default.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Once created, the type of the area cannot be changed. The only exception to this rule is that a NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

The **no** form of the command deletes a stub area.

Examples

The following example sets an additional cost of 5 on a stub area called 2.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 2 stub 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

area virtual-link (OSPFv2)

Creates or modifies virtual links for an area.

Syntax

area { *ip-addr* | *decimal* } **virtual-link** *E.F.G.H* [**authentication-key** *password*] [**dead-interval** *time*] [**hello-interval** *time*] [**md5-authentication** { **key-activation-wait-time** *time* | **key-id** *num key* }] [**retransmit-interval** *time*] [**transmit-delay** *time*]

no area virtual-link

Command Default

No virtual links are created.

Parameters

ip-addr
Area address in IP address format.

decimal
Area address in decimal format.

E.F.G.H
ID of the OSPF router at the remote end of the virtual link.

authentication-key *password*
Sets the password and encryption method. Only one encryption method can be active on an interface at a time. All OSPF packets transmitted on the interface contain this password. All OSPF packets received on the interface are checked for this password. If the password is not present, then the packet is dropped.

dead-interval *time*
How long a neighbor router waits for a hello packet from the current router before declaring the router down. This value must be the same for all routers and access servers that are attached to a common network. Valid values range from 3 through 65535 seconds. The default is 40 seconds.

hello-interval *time*
Time between hello packets that the router sends on an interface. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 through 65535 seconds. The default is 10 seconds.

md5-authentication
Sets either MD5 key-activation wait time or key identifier.

key-activation-wait-time *time*
Time before a newly configured MD5 authentication key is valid. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends will use the newly configured MD5 Key. OSPF packets that contain the old MD5 key are accepted for up to five minutes (300 seconds) after the new MD5 key is in operation. Valid values range from 0 through 14400 seconds. The default is 300 seconds.

key-id *num key*

The *num* is a number between 1 and 255 which identifies the MD5 key being used. This parameter is required to differentiate among multiple keys defined on a device. When MD5 is enabled, the key is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPF packet transmitted. You must enter a password in this field when the system is configured to operate with either simple or MD5 authentication. By default, the MD5 authentication key is encrypted.

retransmit-interval *time*

Time between Link State Advertisement (LSA) retransmissions for adjacencies belonging to the interface. Set this interval to a value larger than the expected round-trip delay between any two routers on the attached network. Valid values range from 0 through 3600 seconds. The default is 5 seconds.

transmit-delay *time*

Estimated time required to send an LSA on the interface. This value must be an integer greater than zero. The age of each LSA in the update packet is incremented by the value of this parameter before transmission occurs. Valid values range from 0 through 3600 seconds. The default is 1 second.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

The **no** form of the command removes a virtual link.

Examples

The following example creates a virtual link for an area whose decimal address is 1, and where the ID of the OSPFv2 device at the remote end of the virtual link is 10.1.2.3.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 1 virtual-link 10.1.2.3
```

History

Release version	Command history
18x.1.00	This command was introduced.

area virtual-link (OSPFv3)

Creates or modifies virtual links for an area.

Syntax

area { *ip-addr* | *decimal* } **virtual-link** *A.B.C.D* [**dead-interval** *time* | **hello-interval** *time* | **hello-jitter** *interval* | **retransmit-interval** *time* | **transmit-delay** *time*] [**authentication key-chain** *name*]

no area virtual-link

Command Default

No virtual links are created.

Parameters

ip-addr
Area address in IP address format.

decimal
Area address in decimal format.

A.B.C.D
ID of the OSPFv3 device at the remote end of the virtual link.

dead-interval *time*
How long a neighbor device waits for a hello packet from the current device before declaring the device down. This value must be the same for all devices and access servers that are attached to a common network. Valid values range from 3 through 65535 seconds. The default is 40 seconds.

hello-interval *time*
Time between hello packets that the device sends on an interface. The value must be the same for all devices and access servers that are attached to a common network. Valid values range from 1 through 65535 seconds. The default is 10 seconds.

hello-jitter *interval*
Sets the allowed jitter between hello packets. Valid values range from 1 through 50 percent (%). The default value is 10%.

retransmit-interval *time*
Time between Link State Advertisement (LSA) retransmissions for adjacencies belonging to the interface. Set this interval to a value larger than the expected round-trip delay between any two devices on the attached network. Valid values range from 1 through 3600 seconds. The default is 5 seconds.

transmit-delay *time*
Estimated time required to send an LSA on the interface. This value must be an integer greater than zero. The age of each LSA in the update packet is incremented by the value of this parameter before transmission occurs. Valid values range from 0 through 3600 seconds. The default is 1 second.

authentication key-chain *name*
The name of the authentication key-chain.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The values of the **dead-interval** and **hello-interval** parameters must be the same at both ends of a virtual link. Therefore, if you modify the values of these parameters at one end of a virtual link, you must make the same modifications on the other end of the link. The values of the other virtual link parameters do not require synchronization.

The **no** form of the command removes a virtual link.

Examples

The following example creates a virtual link for an area whose decimal address is 1, and where the ID of the OSPFv3 device at the remote end of the virtual link is 209.157.22.1.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 1 virtual-link 209.157.22.1
```

History

Release version	Command history
18x.1.00	This command was introduced.

area virtual-link authentication (OSPFv3)

Enables authentication for virtual links in an OSPFv3 area.

Syntax

area { *ip-addr* | *decimal* } **virtual-link** *E.F.G.H* **authentication spi** *spi-value* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** *key*

no area { *A.B.C.D* | *decimal* } **virtual-link** *E.F.G.H* **authentication spi** *spi*

Command Default

Authentication is not enabled on a virtual-link.

Parameters

ip-addr
Area address in IP address format.

decimal
Area address in decimal format.

E.F.G.H
ID of the OSPFv3 device at the remote end of the virtual link.

spi *spi-value*
Specifies the security policy index (SPI) value. Valid values range from decimal numbers 512 through 4294967295

ah
Specifies authentication header (ah) as the protocol to provide packet-level security.

esp
Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null
Specifies that the ESP payload is not encrypted.

hmac-md5
Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPF area.

hmac-sha1
Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPF area.

key *key*
Number used in the calculation of the message digest. 40 hexadecimal character key. The 40 hexadecimal character key is encrypted by default.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Enter **no area** { *A.B.C.D* | *decimal* } **virtual-link** *E.F.G.H* **authentication spi** *spi* to remove authentication from the virtual-links in the area.

Examples

The following example configures IPsec on a virtual link in an OSPFv3 area.

```
device# configure terminal
device(config)# ip router-id 10.1.2.2
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 2 virtual-link 10.1.2.2 authentication spi 600 ah
hmac-sha1 key 1134567890223456789012345678901234567890
```

History

Release version	Command history
18x.1.00	This command was introduced.

arp

Creates a static Address Resolution Protocol (ARP) entry.

Syntax

arp *A.B.C.D mac-address* **interface** { **ethernet** *slot* **/** *port* | **ve** *ve-id* }

no arp *A.B.C.D*

Parameters

A.B.C.D
Specifies a valid IP address.

mac-address
Specifies a valid MAC address.

interface
Specifies an interface type.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

ve *ve-id*
Specifies a virtual Ethernet (VE) interface.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of the command deletes a static ARP entry.

Examples

The following example creates a static ARP entry that associates an IP address, a MAC address, and a physical port.

```
device# configure terminal
device(config)# arp 10.53.4.2 1245.7654.2348 interface ethernet 0/1
```

The following example configures a static ARP within a user-defined VRF.

```
device# configure terminal
device(config)# vrf test
device(config-vrf-test)# address-family ipv4 unicast
device(vrf-test-ipv4-unicast)# arp 10.6.6.7 0001.0001.0001 interface ethernet 0/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

arp access-list

Creates an Address Resolution Protocol (ARP) access control list (ACL), which is one of the steps implementing Dynamic ARP Inspection (DAI) on a VLAN.

Syntax

arp access-list *acl-name*

no arp access-list *acl-name*

Command Default

No ARP ACLs are defined.

Parameters

acl-name

Specifies the name of the ARP ACL. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore (_) and hyphen (-).

Modes

Global configuration mode

Usage Guidelines

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

You can also append the **permit ip host** command to the **arp access-list** command.

The **no** form of the command deletes the ARP ACL if the ACL is not applied on any VLAN or port.

Examples

The following example implements DAI:

1. Creates an ARP ACL named "arp_acl_1".
2. Defines **permit ip host** rules in that ACL.
3. Applies the ACL to VLAN 200.
4. Enables dynamic ARP inspection (DAI) on VLAN 200.

```
device# configure terminal
device(config)# arp access-list arp_acl_1
device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222
device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223
device(config-arp-acl)# exit

device(config)# vlan 200
device(config-vlan-200)# ip arp inspection filter arp_acl_1
device(conf-vlan-200)# ip arp inspection
```

History

Release version	Command history
18x.1.00	This command was introduced.

as-path-ignore

Disables the comparison of the autonomous system (AS) path lengths of otherwise equal paths.

Syntax

as-path-ignore

no as-path-ignore

Command Default

The comparison of the AS path lengths of otherwise equal paths is enabled.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command restores default behavior.

Examples

The following example configures the device to always disable the comparison of AS path lengths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# as-path-ignore
```

History

Release version	Command history
18x.1.00	This command was introduced.

auth-port

Configures a user datagram protocol (UDP) port for Remote Authentication Dial-In User Service (RADIUS) server authentication.

Syntax

auth-port *portnum*

no auth-port

Command Default

By default, port 1812 is used for RADIUS server authentication.

Parameters

portnum

Specifies the UDP port to use for RADIUS server authentication. The valid range is 0 through 65535. The default port is 1812.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure port 1234 as the port used for connection to the RADIUS server for authentication.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# auth-port 1234
```

History

Release version	Command history
18x.1.00	This command was introduced.

auto-cost reference-bandwidth (OSPFv2)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth { *value* | **use-active-ports** }

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

value

Reference bandwidth in Mbps. Valid values range from 1 through 4294967.

use-active-ports

Specifies that any dynamic change in bandwidth immediately affects the cost of OSPF routes. This parameter enables cost calculation for currently active ports only.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Use this command to configure the cost of an interface that a device advertises to it's OSPF neighbors. OSPF calculates the cost of a route as the ratio of the reference bandwidth to the bandwidth of the egress interface. An increase in the reference bandwidth results in an increased cost. If the resulting cost is less than 1, the software rounds the cost up to 1.

The bandwidth for interfaces that consist of more than one physical port is calculated as follows:

- LAG group — The combined bandwidth of all the ports.
- Virtual interface — The lowest individual bandwidth of all the ports that carry the VLAN for the associated VE.

If a change to the reference bandwidth results in a cost change to an interface, the device sends a link-state update to update the costs of interfaces advertised by the device.

NOTE

If you specify the cost for an individual interface (by using the **ip ospf cost** command), the cost you specify overrides the cost calculated by the software.

The **no** form of the command disables bandwidth configuration.

Examples

The following example configures a reference bandwidth of 500.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# auto-cost reference-bandwidth 500
```

The reference bandwidth specified in this example results in the following costs:

- 10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.

The costs for 10 Mbps and 100 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

History

Release version	Command history
18x.1.00	This command was introduced.

auto-cost reference-bandwidth (OSPFv3)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth *value*

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

value

Reference bandwidth in Mbps. Valid values range from 1 through 4294967. The default is 100 Mbps.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Use this command to configure the cost of an interface that a device advertises to it's OSPF neighbors. OSPFv3 calculates the cost of a route as the ratio of the reference bandwidth to the bandwidth of the egress interface. An increase in the reference bandwidth results in an increased cost. If the resulting cost is less than 1, the software rounds the cost up to 1.

The bandwidth for interfaces that consist of more than one physical port is calculated as follows:

- LAG group — The combined bandwidth of all the ports.
- Virtual interface — The lowest individual bandwidth of all the ports that carry the VLAN for the associated VE.

If a change to the reference bandwidth results in a cost change to an interface, the device sends a link-state update to update the costs of interfaces advertised by the device.

NOTE

If you specify the cost for an individual interface using the **ipv6 ospf cost** command, the cost you specify overrides the cost calculated by the software.

The **no** form of the command restores the reference bandwidth to its default value and, thus, restores the default costs of the interfaces to their default values.

Examples

The following example configures a reference bandwidth of 500.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# auto-cost reference-bandwidth 500
```

The reference bandwidth specified in this example results in the following costs:

- 10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.
- 155 Mbps port cost = 500/155 = 3.23, which is rounded up to 4
- 622 Mbps port cost = 500/622 = 0.80, which is rounded up to 1
- 2488 Mbps port cost = 500/2488 = 0.20, which is rounded up to 1

The costs for 10 Mbps, 100 Mbps, and 155 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

History

Release version	Command history
18x.1.00	This command was introduced.

auto-shutdown-new-neighbors

Disables the establishment of BGP connections with a remote peer when the peer is first configured.

Syntax

auto-shutdown-new-neighbors

no auto-shutdown-new-neighbors

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

The **auto-shutdown-new-neighbors** command applies to all neighbors configured under each VRF. When the **auto-shutdown-new-neighbors** command is used, any new neighbor configured will have the shutdown flag enabled for them by default. Once all the neighbor parameters are configured and it is ready to start the establishment of BGP session with the remote peer, the BGP neighbor's shutdown parameter has to disabled by removing the shutdown command for the neighbor.

The **no** form of the command restores the default.

Examples

The following example enables auto shutdown of BGP neighbors on initial configuration.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# auto-shutdown-new-neighbors
```

The following example disables the peer shutdown state and begins the BGP4 session establishment process.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65520
device(config-bgp-router)# no neighbor 10.1.1.1 shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

backup-advertisement-interval

Configures the interval at which backup VRRP routers advertise their existence to the master router.

Syntax

backup-advertisement-interval *interval*

Command Default

The default backup advertisement-interval is 60 seconds.

Parameters

interval

Interval at which a backup VRRP router advertises its existence to the master router. Valid values range from 60 through 3600 seconds.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The interval is the length of time, in seconds, between each advertisement sent from the backup routers to the master router. The advertisement notifies the master router that the backup is still active. If the master router does not receive an advertisement from the backup in a designated amount of time, the backup with the highest priority can assume the role of master.

This command can be used for either VRRP or VRRP-E.

Examples

To set the backup advertisement interval to 120 seconds for VRRP-E group 10:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 10
device(config-vrrp-extended-group-10)# backup-advertisement-interval 120
```

History

Release version	Command history
18x.1.00	This command was introduced.

banner

Defines an incoming, login, or message of the day banner.

Syntax

banner { **incoming** | **login** | **motd** } *string*

no banner incoming | **login** | **motd**

Parameters

incoming
Sets the incoming terminal line banner that is displayed on the console when a user establishes a Telnet session.

login
Sets the login banner that is displayed on the user terminal when the user logs into the device.

motd
Sets the message of the day (MOTD) that is displayed on the user terminal when a Telnet CLI session is established.

string
Specifies a text string from 1 through 2048 characters in length including spaces.

Modes

Global configuration mode.

Usage Guidelines

Use the **no** form of the command to delete the banner.

The banner can appear on multiple lines if you enter multiline mode by using **Esc-M** and exit by using **CTRL-D**.

Examples

To create a login banner with a single line:

```
device(config)# banner login "Please do not disturb the setup on this switch"
```

History

Release version	Command history
18x.1.00	This command was introduced.

beacon enable

Configures Beacon LED based on chassis or based on interface/port-channel.

Syntax

beacon enable chassis [**lenght** *lenght* | **start** *start-time*]

beacon enable interface { **ethernet** {*slot/port* [**lenght** *length* **start** *start-time*] } | { **port-channel** *port-channel id* }}

Parameters

length
Specifies the duration in minutes. The range can be an integer in the range 1 to 1440.

start-time
Specifies the start time in the format (CCYY-MM-DD**T**HH:MM:SS). Date and time are separated by a delimiter T.

port-channel
Specifies the port channel ID.

Modes

Privileged EXEC mode

Usage Guidelines

For the configuration based on chassis, all the interfaces on all the line cards of the chassis will blink at rate of 1 blink /second. For the configuration based on interface or port-channel, only the specific ethernet interface or the port-channel blinks at rate of 1 blink/second. RASLOG messages are displayed for both chassis beacon enable and disable.

Examples

The following example configures the Beacon LED based on chassis.

```
device# beacon enable chassis ?
Possible completions:
  length   Duration in minutes
  start    Start time
  |        Output modifiers
  <cr>

device# beacon enable chassis length ?
Possible completions:
  <Enter a valid integer, 1 .. 1440>
device# beacon enable chassis length 1 ?
Possible completions:
  start   Start time
  |       Output modifiers
  <cr>

device# beacon enable chassis length 1 start ?
Possible completions:
  <dateTime (CCYY-MM-DDTHH:MM:SS)>
 Please note the delimiter T which is used to separate date and time
```

The following example configures the Beacon LED based on interface/port-channel. .

```
device# beacon enable interface ?
Possible completions:
  ethernet       Ethernet interface
  port-channel   Port-channel interface

device# beacon enable interface ethernet 0/1 ?
Possible completions:
  length   Duration in minutes
  start    Start time
  |        Output modifiers
<cr>

device# beacon enable interface port-channel ?
Possible completions:
  <port channel id>
```

The following example shows RASLOG messages for chassis beacon enable and disable.

```
device# 2017/01/09-19:32:00, [NSM-2071], 7549, DCE, INFO, SLX9540, Chassis beaconing is enabled
device# 2017/01/09-19:33:00, [NSM-2072], 7550, DCE, INFO, SLX9540, Chassis beaconing is disabled
```

History

Release version	Command history
18x.1.00	This command was introduced.

bfd

Enables Bidirectional Forwarding Detection (BFD).

Syntax

bfd

no bfd

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Use the **bfd** command in OSPF router configuration mode to enable BFD sessions on all OSPFv2 interfaces on which BFD has been configured using the **ip ospf bfd** command. Use the **bfd** command in OSPFv3 router configuration mode to enable BFD sessions on all OSPFv3 interfaces on which BFD has been configured using the **ipv6 ospf bfd** command.

The **no** form of the command disables BFD globally.

Examples

The following example enables BFD globally in OSPF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# bfd
```

The following example disables BFD globally in OSPFv3 router configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# no bfd
```

History

Release version	Command history
18x.1.00	This command was introduced.

bfd holdover-interval

Sets the time interval for which Open Shortest Path First (OSPF), Intermediate System to Border Gateway Protocol (BGP) routes are withdrawn after a Bidirectional Forwarding Detection (BFD) session is declared down.

Syntax

bfd holdover-interval *time*

no bfd holdover-interval *time*

Command Default

The BFD holdover interval is set to 0 by default.

Parameters

time

Specifies the BFD holdover interval in seconds. In BGP configuration mode, valid values range from 0 through 30 and the default is 0. In OSPF router VRF and OSPFv3 router VRF configuration mode, valid values range from 0 through 20 and the default is 0.

Modes

BGP configuration mode

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The BFD holdover interval is supported for both single-hop and multihop sessions.

In BGP configuration mode, use this command to set the BFD holdover interval globally for BGP. In OSPF router configuration mode or OSPF router VRF configuration mode, use this command to set the BFD holdover interval globally for OSPFv2. In OSPFv3 router or OSPFv3 router VRF configuration mode, use this command to set the BFD holdover interval globally for OSPFv3.

The **no** form of the command removes the configured BFD holdover interval from the configuration, and reverts to the default value of 0.

Examples

The following example sets the BFD holdover interval globally to 15 in BGP configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# bfd holdover-interval 15
```

The following example sets the BFD holdover interval globally to 12 in OSPF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# bfd holdover-interval 12
```

The following example sets the BFD holdover interval globally to 20 in OSPFv3 router configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# bfd holdover-interval 20
```

The following example sets the BFD holdover interval globally to12 in IS-IS router configuration mode.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# bfd holdover-interval 12
```

History

Release version	Command history
18x.1.00	This command was introduced.

bgp-redistribute-internal

Causes the device to allow the redistribution of IBGP routes from BGP into OSPF for non-default VRF instances.

Syntax

bgp-redistribute-internal

no bgp-redistribute-internal

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

By default, with default VRF instances, the device does not allow the redistribution of IBGP routes from BGP4 and BGP4+ into OSPF. This helps to eliminate routing loops. In non-default VRF instances, use this command to allow the redistribution of IBGP routes from BGP into OSPF. This command is enabled only if a non-default VRF instance has been specified.

Examples

This example enables BGP4 route redistribution.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# bgp-redistribute-internal
```

This example enables BGP4+ route redistribution for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# bgp-redistribute-internal
```

History

Release version	Command history
18x.1.00	This command was introduced.

bpdu-drop-enable

Enables dropping Layer 2 (L2) bridge protocol data units (BPDUs) on endpoints in a bridge domain.

Syntax

bpdu-drop-enable

no bpdu-drop-enable

Command Default

Dropping of L2 BPDUs is disabled. L2 BPDUs are allowed on endpoints in the bridge domain.

Modes

Bridge-domain configuration mode.

Usage Guidelines

The **no** form of the command disables dropping of Layer 2 (L2) bridge protocol data units (BPDUs) in a bridge domain.

Examples

The following example shows how to enable dropping of L2 BPDUs in bridge domain 3.

```
device# configure terminal
device(config)# bridge-domain 3
device(config-bridge-domain-3)# bpdu-drop-enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

breakout mode 4x10g

Configures any 40G port on the SLX 9850 36X100G line card (LC) as four 10G ports.

Syntax

breakout mode 4x10g

no breakout mode 4x10g

Modes

Hardware connector configuration mode

Usage Guidelines

Use the **no** form of the command to reset the port on the 36X100G LC to a 40G port.

You must power off the line card before using this command.

After using this command, save the running-config file to the startup-config file, and power on the line card or reload the device for the changes to take effect.

When you power on the line card, the SFP interfaces come up under the new mode with default configurations. Unaffected interfaces retain the configurations they had before the line card was powered off.

Examples

The following example shows the configuration of a 40G port on the 36X100G LC into four 10G ports.

```
device# power-off linecard 4
device# configure terminal
device(config)# hardware
device(config-hardware)# connector 4/2
device(config-connector-4/2)# breakout mode 4x10g
%Warning: Sfp Breakout is a disruptive command.
Please save the running-config to startup-config and use reload command on the device or power-cycle
linecard on Chassis system for the changes to take effect.
device(config-port-group-4/2)# Ctrl-z
device# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
device# power-on linecard 4
```

History

Release version	Command history
18x.1.00	This command was introduced.

bridge-domain

Creates a bridge domain. A bridge domain represents a switching or inter-connection domain for a wide range of service end-point types.

Syntax

bridge-domain { *id* } [**p2mp** | **p2p**]

no bridge-domain { *id* } [**p2mp** | **p2p**]

Command Default

No bridge domain is configured.

Parameters

id

Specifies a unique numeric bridge-domain identifier. The range is from 1 through 4096.

p2mp

Specifies a multipoint service type. This is the default service type.

p2p

Specifies a point-to-point cross-connect service type.

Modes

Global configuration mode.

Usage Guidelines

Use the bridge-domain to specify the related configuration for both VPLS and VLL.

The **no** version of the command removes the bridge-domain configuration.

Examples

The following example shows how to configure bridge domain 1 and specifies a point-to-point cross-connect service for the domain.

```
device# configure terminal
device(config)# bridge-domain 1 p2p
```

The following example shows the error message that is displayed when the specified bridge-domain ID is out of range.

```
device# configure terminal
device(config)# bridge-domain 10000000
Error: syntax error: "10000000" is out of range.
```

The following example shows the error message that is displayed when the bridge-domain creation is not successful in the back-end.

```
device# configure terminal
device(config)# bridge-domain 110
Error: bridge-domain: connection instance creation failed.
```

History

Release version	Command history
18x.1.00	This command was introduced.

bridge-domain (EVPN)

Specifies a bridge domain (BD), or adds or removes a range VLANs from the BD, for an Ethernet Virtual Private Network (EVPN) instance.

Syntax

bridge-domain *BD-ID*

no bridge-domain *BD-ID*

bridge-domain { **add** | **remove** } {*VLAN-range* }

Command Default

Disabled

Parameters

BD-ID
Specifies a BD.

add
Adds a range of VLANs to the BD for default EVPN instance.

remove
Removes a range of VLANs from the BD for the default EVPN instance.

VLAN-range
Specifies a hyphen-delimited VLAN range to be added to or removed from BD for the EVPN instance.

Modes

EVPN configuration mode

Usage Guidelines

Each VLAN/BD added to an EVPN configuration is considered as an EVPN instance and is assigned a unique EVPN instance ID (EVI) internally. The EVI is calculated as shown in the following table.

When adding a bridge domain, use the **clear bgp evpn neighbor all soft in** command for the change to take effect.

TABLE 3 Calculating EVI values from VLAN/BD values

VLAN/BD	EVI value
VLAN: 1–4096	VLAN ID
BD: 1–4096	BD ID + 4096

ATTENTION
To interoperate with third-party vendors, the RTs across the interoperating devices must be the same. If third-party devices do not support automatic RT assigment, or the EVIs are not calculated as shown in the above table, the VLAN/BD instances must be configured manually to ensure that RTs across the devices are compatible.

Examples

To specify a BD and enter EVPN BD configuration mode:

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain 100
device(evpn-bridge-domain-100)#
```

To add BDs 100 through 200 to the default EVPN instance:

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain add 100-200
device(config-evpn-default)#
```

To remove BDs 150 through 180 from the default EVPN instance:

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain remove 150-180
device(config-evpn-default)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

bridge-priority

Specifies the bridge priority for the common instance.

Syntax

bridge-priority *priority*

no bridge-priority

Command Default

The default priority is 32768.

Parameters

priority

Specifies the bridge priority. Valid values range from 0 through 61440 in increments of 4096.

Modes

Protocol Spanning Tree mode

Usage Guidelines

The priority values can be set only in increments of 4096.

Using a lower priority value indicates that the bridge might become root.

Enter **no bridge-priority** to return to the default priority.

Examples

To specify the bridge priority:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# bridge-priority 8192

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# bridge-priority 8192

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# bridge-priority 8192
```

History

Release version	Command history
18x.1.00	This command was introduced.

bsr-candidate

Configures a bootstrap router (BSR) as a candidate to distribute rendezvous point (RP) information to the other PIM Sparse devices within a PIM Sparse domain.

Syntax

bsr-candidate interface [*ethernet* | *loopback* | *port-channel*| *ve*]

no bsr-candidate

Command Default

The PIM router does not participate in BSR election.

Parameters

loopback *num*
Specifies the loopback interface for the candidate BSR.

ve *num*
Specifies the virtual interface for the candidate BSR.

port-channel *num*
Specifies the port-channel number for the candidate BSR.

Modes

PIM Router configuration mode

Usage Guidelines

The **no** form of this command makes the PIM router cease to act as a candidate BSR.

Each PIM Sparse domain has one active BSR. For redundancy, you can configure ports on multiple devices as candidate BSRs. The PIM Sparse protocol uses an election process to select one of the candidate BSRs as the BSR for the domain. The BSR with the highest BSR priority is elected. If the priorities result in a tie, the candidate BSR interface with the highest IP address is elected.

Although you can configure the device as only a candidate BSR or an RP, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

Examples

The following example uses a physical interface to configure a device as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate ethernet 2/2 30 255
```

The following example uses a loopback interface to configure a device as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate interface loopback 11 mask 32
```

The following example uses a virtual interface to configure a device as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate ve 120 30 250
```

History

Release version	Command history
18x.1.00	This command was introduced.

Commands C - D

capability as4-enable

Enables 4-byte autonomous system number (ASN) capability at the BGP global level.

Syntax

capability as4-enable

no capability

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to disable this functionality.

Examples

The following example enables 4-byte ASN capability.

```
device#configure terminal
device(config)# router bgp
device(config-bgp-router)# capability as4-enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

ccm-interval

Sets the time interval between two successive Continuity Check Messages (CCMs) that are sent by Maintenance End Points (MEP) in the specified Maintenance Association (MA).

Syntax

ccm-interval [1-second | 10-second | 3.3-ms | 10-ms | 100-ms]

Parameters

1-second
Sets the time interval between two successive CCM packets to 1 second.

10-second
Sets the time interval between two successive CCM packets to 10 seconds.

3.3-ms
Ssets the time interval between two successive CCM packets to 3.3 milliseconds.

10-ms
Sets the time interval between two successive CCM packets to 10 milliseconds.

100-ms
Sets the time interval between two successive CCM packets to 100 milliseconds.

Modes

CFM protocol configuration mode

Usage Guidelines

The default value is 10 seconds.

Examples

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 4
device(config-cfm-md-ma-ma1)#ccm-interval 10-second
```

History

Release version	Command history
18x.1.00	This command was introduced.

certutil import sshkey

Imports an SSH public key for a local SSH user from a remote host using the login credentials and path name.

Syntax

certutil import sshkey directory *ssh_public_key_path* **file** *file-name* **host** *remote_ip_address* **login** *login_id* **password** *password* **user** *user_acct*

Parameters

directory *path*
Specifies the path to the certificate on the remote host.

file *filename*
Specifies the SSH public key with a .pub extension.

host *remote_ip*
Specifies the IP address of the remote host.

login *login_id*
Specifies the login name in the remote host.

password *password*
Specifies the password to access the remote host.

user *user_acct*
Specifies a local user name.

Modes

Privileged EXEC mode

Usage Guidelines

When using the **password** parameter with special characters (such as #$@`) use single or double-quotes around the password. Alternatively, preceed the special characters by a backslash (\) character.

To delete a public key for a specific user, use to the **no cerutil sshkey** command.

Examples

The following example shows how to import an SSH public key for an SSH user named admin from a remote host (10.70.4.106). The command specifies the SSH public key directory on the remote host as well as login credentials to the remote host.

```
device# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/bmeenaks/.ssh file
id_rsa.pub login fvt password pass1
```

The following example demonstrates the use of special characters in a password.

```
device# certutil import ssh host 192.168.10.10 dir /home/brcd1/.ssh file id_rsa.pub user admin login
brcd1 pass Abcde\! login brcd1 pass "Abcde!"
```

History

Release version	Command history
18x.1.00	This command was introduced.

certutil sshkey

Enters an SSH public key for a specific user by using the command line interface (CLI).

Syntax

certutil sshkey user *user_acct* **pubkey** *public_key*

no certutil sshkey user *user_acct*

Parameters

user *user_acct*
Specifies a user name. The user must be a pre-existing user on the device. By default there are two users: “admin” and “user”.

pubkey *public_key*
Specifies a public key.

Modes

Privileged EXEC mode

Usage Guidelines

NOTE
After an SSH public key is configured, the SSH server restarts on all VRF instances and all existing SSH connections are disconnected.

The user for whom a public key is to be configured by using the **certutil sshkey** command, must already be configured on the device. By default, two users (admin and user) are configured on the device. Additional users are configured by using the **username** command in global configuration mode.

The public key must be entered within double quotes (" ").

To generate a public key, run the **ssh-keygen -t rsa** command on any server from which you want to start an SSH session to the device. Once you run this command, and have not entered any other path while generating the key, the public key is generated at /root/.ssh/id_rsa.pub by default. Open this file and copy all its contents after the **pubkey** option in the CLI.

The **no** form of the command removes the public key configuration for the specified user.

Examples

The following example shows how to enter an SSH public key directly into the CLI under the username admin.

```
device# certutil sshkey user admin pubkey “ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDnim+Ofjx/
id3z2jDxXu9DcMuQqVq/NKi2Lms+q7dA5Dqww8jlrOGawG8tMySOvnB1ZEvJt1kqNneRi4l6Ot4/7hfd99rIOPGBP/
NJs6xTLUrQhDgxB78ddTg+6euBtkYLTAaTC7kbXGXcO8VVB9+4xrH+0bkvjU9RRvGJguUfdiFKEfIGVOyt0atdHi1dmgQ9BE0cO65nc/
i9MjMJedBe174/QT4TxeGeEgaQ57c2AL5It2V4CzrZBDtnixdnHUO5w2vmBR61LZIDVT1fuX/xYxDAm9H8SDpDX8pZlfFpQBy/
wrkIYPZ/p4OLrUApB/XAJGujrlNlZLEu9U9MPVM/ root@ldap.hc-fusion.in”
```

History

Release version	Command history
18x.1.00	This command was introduced.

cfm linktrace

Transmits a linktrace message to a Maintenance End Point (MEP) in the domain

Syntax

cfm linktrace { **domain** *name* | **ma** *ma-name* | **src-mep** *mep-id* { **target-mip** *HH:HH:HH:HH:HH:HH* | **target-mep** *mep-id* }| **timeout** *time* | **ttl** *ttl-value*

Parameters

domain *name*
Specifies the maintenance domain to be used for a linktrace message. The name attribute is case-sensitive.

ma *ma-name*
Specifies the maintenance association to be used for a linktrace message. The ma-name attribute is case-sensitive.

src-mep *mep-id*
Specifies the Source ID. The range of valid values is from 1 through 8192.

target-mip *HH:HH:HH:HH:HH:HH*
Specifies the MAC address of the MIP linktrace destination.

target-mep *mep-id*
Specifies the destination ID. The range of valid values is from 1 through 8192.

ttl *ttl-value*
specifies the initial TTL field value. The range of valid values is from 1 through 64.

timeout *time*
Specifies the timeout used to wait for linktrace reply in seconds.

Modes

Privileged EXEC mode .

Usage Guidelines

The **cfm linktrace** command sends a trace message to a specified MEP in the domain to diagnose the path of the MEP link.

Examples

The following example transmits a successful trace from MEP 21 to MEP 1.

```
device# cfm linktrace domain md1 ma ma1 src-mep 21 target-mep 1 timeout 10

Linktrace to 000c.dbfb.5378 on Domain md1, level 4: timeout 10ms, 4 hops
------------------------------------------------------------------
Hops            MAC         Ingress     Ingress Action     Relay Action
Forwarded         Egress     Egress Action     Nexthop
------------------------------------------------------------------
1         000c.dbe2.6ea0                          RLY_FDB
Forwarded         5/4         EgrOK
2         000c.dbfb.5378     7/2         IgrOK         RLY_HIT
Not Forwarded
Destination 000c.dbfb.5378 reached
```

History

Release version	Command history
18x.1.00	This command was introduced.

cfm loopback

Transmits a loopback message to a specific Maintenance End Point (MEP) or Maintenance Intermediate Point (MIP) in a specified domain.

Syntax

cfm loopback { **domain** *name* | **ma** *ma-name* | **src-mep** *mep-id* { **target-mip** *HH:HH:HH:HH:HH:HH* | **target-mep** *mep-id* }| **number** *value* | **timeout** *time*

Parameters

domain *name*
Specifies the maintenance domain to be used for a loopback message. The name attribute is case sensitive.

ma *ma-name*
Specifies the maintenance association to be used for a loopback message. The ma-name attribute is case-sensitive.

src-mep *mep-id*
Specifies the Source ID. The range of valid values is from 1 through 8192.

target-mip *HH:HH:HH:HH:HH:HH*
Specifies the MAC address of the MIP loopback destination.

target-mep *mep-id*
Specifies the destination ID. The range of valid values is from 1 through 8192.

number *value*
Specifies the number of loopback messages to be sent.

timeout *time*
Specifies the timeout used to wait for loopback reply in seconds.

Modes

Privileged EXEC mode

Usage Guidelines

The cfm loopback command sends a loopback message to a specific MEP or MIP in a specified domain for testing purposes.

Examples

Command example sending a message from MEP 2 to MEP 1 a total of ten times.

```
device# cfm loopback domain md1 ma ma1 src-mep 2 target-mep 1 timeout 10 number 10

cfm: Sending 10 Loopback to 000c.dbfb.5378, timeout 10 msec
Type Control-c to abort
Reply from 000c.dbfb.5378: time=1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
A total of 10 loopback replies received.
Success rate is 100 percent (10/10), round-trip min/avg/max=0/0/1 ms.
```

History

Release version	Command history
18x.1.00	This command was introduced.

cfm y1731 domain

Sets the on-demand two-way delay measurement or two-way synthetic loss measurement parameters.

Syntax

cfm y1731 domain *domain-name* **ma** *ma-name* **src-mep** *mep-id* **target-mep** *mep-id* **test-profile** *profile-name*

Parameters:

domain-name
Specifies the domain name.

ma
Specifies the maintenance association (MA).

ma-name
Specifies the MA name.

src-mep *mep-id*
Specifies the source mep-id.

target *mep-id*
Specifies the taraget mep-id.

profile
Specifies the default or configured test profile.

profile-name
Specifies the profile name.

Modes

Global configuration mode

Examples

This example shows how to run on-demand two-way delay measurement or two-way synthetic loss measurement parameters.

```
device# cfm y1731 domain md1 ma ma1 src-mep 1 target-mep 2 test-profile 2dm_default_profile
device# cfm y1731 domain md1 ma ma1 src-mep 1 target-mep 2 test-profile 2slm_default_profile
```

History

Release version	Command history
18x.1.00	This command was introduced.

channel-group

Enables Link Aggregation on an interface.

Syntax

channel-group *number* **mode** { **active** | **passive** | **on** } [**type standard**]

no channel-group

Command Default

The value for **type** is set to **standard**.

Parameters

number

Specifies a Link Aggregation Group (LAG) port-channel group number to which this link should administratively belong. Values range from 1 through 64.

mode

Specifies the mode of Link Aggregation.

active

Enables the initiation of LACP negotiation on an interface.

passive

Disables LACP on an interface.

on

Enables static link aggregation on an interface.

type standard

Specifies the 802.3ad standard-based LAG.

Modes

Interface subtype configuration mode

Usage Guidelines

This command adds an interface to a port-channel specified by the channel-group number. This command enables link aggregation on an interface, so that it may be selected for aggregation by the local system.

The maximum number of LAGs supported is 64.

A maximum of 32 links can be aggregated per port-channel.

To remove port-channel members, use the **no** form of this command.

Examples

The following example sets the channel-group ID to 10 and the mode to "passive".

```
device# configure terminal
device(config)# interface ethernet 0/9
device(conf-if-eth-0/9)# channel-group 10 mode passive
```

History

Release version	Command history
18x.1.00	This command was introduced.

cisco-interoperability

Configures the device to interoperate with some legacy Cisco switches.

Syntax

cisco-interoperability { **disable** | **enable** }

Command Default

Cisco interoperability is disabled.

Parameters

disable

Disables Cisco interoperability for the Multiple Spanning Tree Protocol (MSTP) device.

enable

Enables Cisco interoperability for the MSTP enabled device.

Modes

Protocol Spanning Tree MSTP mode

Usage Guidelines

For some devices, the MSTP field, Version 3 Length, does not adhere to the current standards.

If Cisco interoperability is required on any device in the network, then all devices in the network must be compatible, and therefore enabled using this command for interoperability with a Cisco switch.

Examples

To enable Cisco interoperability on a device:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# cisco-interoperability enable
```

To disable Cisco interoperability on a device:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# cisco-interoperability disable
```

History

Release version	Command history
18x.1.00	This command was introduced.

class

Creates a class map in a policy map and enters the class map configuration mode.

Syntax

class *class-mapname*

no class *class-mapname*

Command Default

A policy map is not created.

Parameters

class-mapname
The designated name for the class map.

Modes

Policy map configuration mode

Usage Guidelines

Use this command to configure a class map for a police policy map with QoS and policing parameters for inbound or outbound traffic. The class map must be previously created and associated with match criteria using the **class-map** command. (Refer to the **qos cos** command.)

When you enter the **class** command and access policy-map class configuration mode, you can configure QoS and policing parameters for the class map using the commands for the specific parameters.

Each policy map can contain one class map.

The **police cir** command is mandatory for configuring a class map.

Enter **no police** while in config-policymap-class mode to remove all policing parameters for the class map.

Enter **no police** command followed by a policing parameter name to remove a specific parameter.

NOTE
The **cir** is mandatory for configuring a class map. Other parameters are optional. If optional parameters are not set then they will be treated as disabled. To delete the mandatory CIR parameter, you must delete all policer parameters while in the policy map class configuration mode using the **no police** command.

Examples

This example configures a class-map called "default" within a policy-map.

```
device# configure terminal
device(config)# policy-map policymap1
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
```

History

Release version	Command history
18x.1.00	This command was introduced.

class-map

Enters class (classification) map configuration mode.

Syntax

class-map *class-map-name*

no class-map *class-map-name*

Command Default

The class map name "default" is reserved and cannot be created by users.

Parameters

class-map-name

Name of classification map. The map name is restricted to 64 characters.

Modes

Global configuration mode.

Usage Guidelines

Enter **no map class-map** *class-map-name* while in global configuration mode to remove the classification map.

Examples

The following example accesses class map configuration mode for the default class map:

```
device(config)# class-map default
device(config-classmap)#
```

The following example creates a class map, accesses class map configuration mode, and adds a match statement to a VLAN:

```
device(config)# class-map c1
device(config-classmap)# match vlan 500
```

The following example creates a class map, accesses class map configuration mode, and adds a match statement to a bridge domain:

```
device(config)# class-map BD-1000
device(config-classmap)# match bridge-domain 1000
```

Release version	Command history
18x.1.00	This command was introduced.

clear arp

Clears some or all Address Resolution Protocol (ARP) entries.

Syntax

clear arp [**ethernet** *slot* **/** *port* | **ip** *ip-address* | **ve** *ve-id*] [**no-refresh**] [**vrf** *vrf-name*]

Parameters

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

ip *ip-address*
Specifies a next-hop IP address.

ve *ve-id*
Specifies a virtual ethernet (VE) interface.

no-refresh
Clears the ARP cache without resending ARP requests to the local hosts.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

If the **no-refresh** keyword is not included, ARP requests are automatically triggered for the cleared entries. To avoid this triggering, include the **no-refresh** keyword.

Examples

The following example clears all ARP entries on the device.

```
device# clear arp
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear bfd neighbors

Clears Bidirectional Forwarding Detection (BFD) neighbors.

Syntax

clear bfd neighbors [*ipv4-addr* | | *ipv6-addr*]

Parameters

ipv4-addr
Specifies an IPv4 address.

ipv6-addr
Specifies an IPv6 address.

Modes

Privileged EXEC mode

Examples

The following example clears a specified IPv4 BFD neighbor.

```
device# clear bfd neighbors 10.1.1.1
```

The following example clears all BFD neighbor.

```
device# clear bfd neighbors
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear bgp evpn neighbor

Requests a dynamic refresh of BGP EVPN connections or routes from a neighbor, with a variety of options.

Syntax

clear bgp evpn neighbor { **all** | *ipv4-addr* | *ipv6-addr* } [**soft** [**in** | **out**]]

clear bgp evpn neighbor { **all** | *ipv4-addr* | *ipv6-addr* } [**soft-outbound**]

Parameters

all
Resets and clears all BGP EVPN connections to all neighbors.

ipv4-addr
Specifies an IPv4 address.

ipv6-addr
Specifies an IPv6 address.

soft
Refreshes routes received from or sent to the neighbor.

in
Refreshes received routes.

out
Refreshes sent routes.

soft-outbound
Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

NOTE
Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

Modes

Privileged EXEC mode

Examples

This example refreshes all BGP EVPN neighbor connections.

```
device# clear bgp evpn neighbor all
```

This example clears BGP EVPN connections with a specified IPv6 address.

```
device# clear bgp evpn neighbor 2001::1
```

This example refreshes routes received from a neighbor with the IP address 10.0.0.1.

```
device# clear bgp evpn neighbor 10.0.0.1 soft in
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear bgp evpn routes

Clears routes from the BGP EVPN route table and resets the routes.

Syntax

clear bgp evpn routes

clear bgp evpn routes type arp *ip address* **mac** *mac address* **ethernet-tag** *tag-id*

clear bgp evpn routes type ipv4-prefix *ip address/mask*

clear bgp evpn routes type ipv6-prefix *ipv6 address/mask*

clear bgp evpn routes type mac *mac address***ethernet-tag** *tag-id*

clear bgp evpn routes type nd *IPv6 address* **mac** *mac address* **ethernet-tag** *tag-id*

Parameters

arp
Specifies address-resolution protocol (ARP) routes.

ip address
Specifies an IP address.

mac *mac address*
Specifies Media Access Control (MAC) routes and a MAC address. The valid format is HHHH.HHHH.HHHH.

ethernet-tag *tag-id*
Specifies an Ethenet tag. Valid values range from 1 through 4294967295.

ipv4-prefix
Specifies IPv4 prefix routes.

IPv4 address/mask
Specifies an IPv4 address and mask.

ipv6-prefix
Specifies IPv6 prefix routes.

IPv6 address/mask
Specifies an IPv6 address and mask.

mac
Specifies MAC routes.

nd
Specifies neighbor-discovery (ND) routes.

Modes

Privileged EXEC mode

Examples

This example clears all routes from the BGP EVPN route table.

```
device# clear bgp evpn routes
```

This example clears all ARP routes from the BGP EVPN route table.

```
device# clear bgp evpn routes type arp
```

This example clears a specified MAC route from the BGP EVPN route table.

```
device# clear bgp evpn routes type mac 000.abba.baba ethernet-tag 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear cfm y1731 statistics

Clears all Y.1731 statistics.

Syntax

clear cfm y1731 statistics

Modes

Privileged EXEC mode

Examples

This example shows how to clears all Y.1731 statistics.

```
device# clear cfm y1731 statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear cfm y1731 statistics delay-measurement

Clears all Y.1731 statistics for Two-Way ETH-DM.

Syntax

clear cfm y1731 statistics delay-measurement

Modes

Privileged EXEC mode

Examples

This example shows how to clears all Y.1731 statistics for Two-Way ETH-DM.

```
device# clear cfm y1731 statistics delay-measurement
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear cfm y1731 statistics synthetic-loss-measurement

Clears all Y.1731 statistics for Two-way ETH-SLM.

Syntax

clear cfm y1731 statistics

Modes

Privileged EXEC mode

Examples

This example shows how to clears all Y.1731 statistics for Two-Way ETH-SLM.

```
device# clear cfm y1731 statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear counters

Clears the IP counter statistics on the switch.

Syntax

clear counters [**access-list** { **ip** | **ipv6** | **mac** } [**all** | **interface** { **fcoe** [*vn-number* | **all**] | **port-channel** *number* | **slot-id** *number* | **vlan** *vlan_id* } | **storm-control**]

Parameters

access-list
Clears the IP counter statistics on all interfaces on the switch.

all
Clears all IP counter statistics on the switch or selected interface.

interface
Specifies an interface.

port-channel *number*
Specifies a port-channel. The number of available channels range from 1 through 6144.

slot-id
Clears the IP counter statistics on a specified slot in the chassis.

storm-control
Clears counters about traffic controlled by configured rate limits.

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

clear counters access-list

Clears access control list (ACL) statistical information for a given network protocol and inbound or outbound direction.

Syntax

clear counters access-list interface { **ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan-id* } { **in** | **out** }

clear counters access-list interface ve *vlan-id* { **in** | **out** }

clear counters access-list { **ip** | **ipv6** } [*acl-name* { **in** | **out** }]

clear counters access-list { **ip** | **ipv6** } *acl-name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan-id* } { **in** | **out** }

clear counters access-list receive { **ip** | **ipv6** }

clear counters access-list mac [*acl-name* { **in** | **out** }]

clear counters access-list mac *acl-name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan-id* } { **in** | **out** }

Parameters

interface
Specifies an interface.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *index*
Specifies a port-channel. Available channels range from 1 through 6144.

in
Specifies incoming binding direction.

out
Specifies outgoing binding direction.

vlan *vlan-id*
(Available only on Layer 2) Specifies a VLAN.

ve *vlan-id*
(Available only on Layer 3) Specifies a virtual Ethernet (VE) interface.

ip
Specifies the IPv4 Layer 3 network protocol.

ipv6
Specifies the IPv6 Layer 3 network protocol.

mac
Specifies the medium access control (MAC) Layer 2 network protocol.

overlay type vxlan
Not supported for this release.

uda
Not supported for this release.

receive
Specifies an ACL that applies to device recieve-path traffic.

acl-name
Specifies the ACL name. To clear statistics on all counters of an ACL-type, do not specify *acl-name*.

Modes

Privileged EXEC mode

Usage Guidelines

You can clear all statistics for a specified ACL or only for that ACL on a specified interface.

You can also clear statistical information for all ACLs bound to a specified Ethernet interface, a port-channnel, VLAN, or VE.

Examples

The following example clears ACL statistics on a specified Ethernet interface.

```
device# clear counters access-list interface ethernet 0/1
```

The following example clears ACL statistics for a specified MAC ACL on a specified Ethernet interface.

```
device# clear counters access-list mac MAC_ACL_1 interface ethernet 0/2
```

The following example clears ACL statistics for a specified MAC ACL on all interfaces on which this ACL is applied.

```
device# clear counters access-list mac MAC_ACL_1
```

The following example clears ACL statistics for a specified IPv4 ACL on a specified interface.

```
device# clear counters access-list ip IP_ACL_1 interface ethernet 0/3
```

The following example clears ACL statistics for a specified IPv4 ACL on all interfaces on which it is applied.

```
device# clear counters access-list ip IP_ACL_1
```

The following example clears incoming ACL statistics for a specified IPv6 ACL on a virtual Ethernet (VE) interface.

```
device# clear counters access-list ipv6 ip_acl_3 interface ve 10 in
```

The following example clears IPv6 receive-path ACL statistics.

```
device# clear counters access-list receive ipv6
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear counters storm-control

Clears all broadcast, unknown unicast, and multicast (BUM) related counters in the system.

Syntax

clear counters storm-control

clear counters storm-control [**broadcast** | **multicast** | **unknown-unicast**] [**interface ethernet** *slot/port*]

Parameters

broadcast
Clears all BUM-related counters in the system for the broadcast traffic type.

multicast
Clears all BUM-related counters in the system for the multicast traffic type.

unknown-unicast
Clears all BUM-related counters in the system for the unknown-unicast traffic type.

interface ethernet *slot/port*
Clears all BUM-related counters in the system for the specified interface.

Modes

Privileged EXEC mode.

Usage Guidelines

This command clears the counters for broadcast, unknown-unicast, and multicast traffic for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on specified interfaces.

Examples

Clear counters for broadcast traffic on an Ethernet interface.

```
device# clear counters storm-control broadcast interface ethernet 4/1
```

Clear counters for all traffic types enabled on an Ethernet interface.

```
device# clear counters storm-control interface ethernet 4/1
```

Clear counters for all multicast traffic in the system.

```
device# clear counters storm-control multicast
```

Clear all BUM-related counters in the system.

```
device# clear counters storm-control
```

Release version	Command history
18x.1.00	This command was introduced.

clear dot1x statistics

Clears all accumulated dot1x port authentication statistics on the ports.

Syntax

clear dot1x statistics [**interface ethernet** *slot/port*]

Parameters

interface ethernet *slot/port*

Specifies to clear all dot1x statistics for a specified interface port.

Modes

Privileged EXEC mode

Examples

This example clears all accumulated dot1x port authentication statistics on all ports.

```
device# clear dot1x statistics
```

This example clears all dot1x statistics for a specified interface port.

```
device# clear dot1x statistics interface ethernet 1/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip arp inspection statistics

Clears Dynamic ARP Inspection (DAI) statistics for all DAI-enabled VLANs.

Syntax

clear ip arp inspection statistics

Modes

Privileged EXEC mode

Usage Guidelines

The capacity of each statistic counter is 64 bits, beyond which such a counter is reset to zero.

Examples

The following example clears DAI statistics for all DAI-enabled VLANs.

```
device# clear ip arp inspection statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip arp suppression-cache

Clears the IPv4 ARP-suppression cache and downloads the current forwarding database from BGP-EVPN. You can also clear the cache for a specified bridge domain or VLAN.

Syntax

clear ip arp suppression-cache [**bridge-domain** *bridge-domain-id* | **vlan** *vlan-id*]

Parameters

bridge-domain *bridge-domain-id*
Specifies a bridge domain. The range is from 1 through 1024.

vlan *vlan-id*
Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Usage Guidelines

Running this command might impact traffic.

Examples

The following example clears the ARP-suppression cache.

```
device#  clear ip arp suppression-cache
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip arp suppression-statistics

Clears ARP-suppression statistical information. You can also clear statistics for a specified bridge domain or VLAN.

Syntax

clear ip arp suppression-statistics [**bridge-domain** *bridge-domain-id* | **vlan** *vlan-id*]

Parameters

bridge-domain *bridge-domain-id*
Specifies a bridge domain. The range is from 1 through 1024.

vlan *vlan-id*
Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example clears all ARP-suppression statistics.

```
device#  clear ip arp suppression-statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip bgp dampening

Reactivates suppressed BGP4 routes.

Syntax

clear ip bgp dampening [*ip-addr* { **/** *mask* }] [**vrf** *vrf-name*]

Parameters

ip-addr
: IPv4 address of a specified route in dotted-decimal notation.

mask
: (Optional) IPv4 mask of a specified route in CIDR notation.

vrf *vrf-name*
: Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example unsuppresses all suppressed BGP4 routes.

```
device# clear ip bgp dampening
```

This example unsuppresses suppressed BGP4 routes for VRF "red".

```
device# clear ip bgp dampening vrf red
```

History

Release version	Command history
168x1.00	This command was introduced.

clear ip bgp flap-statistics

Clears the dampening statistics for a BGP4 route without changing the dampening status of the route.

Syntax

clear ip bgp flap-statistics [*ip-addr* { **/** *mask* } | **neighbor** *ip-addr* | **regular-expression** *string*] [**vrf** *vrf-name*]

Parameters

ip-addr
IPv4 address of a specified route in dotted-decimal notation.

mask
(Optional) IPv4 mask of a specified route in CIDR notation.

neighbor
Clears dampening statistics only for routes learned from the specified neighbor.

ip-addr
IPv4 address of the neighbor.

regular-expression
Specifies a regular expression.

string
Regular expression.

vrf *vrf-name*
Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears the dampening statistics for a BGP4 route.

```
device# clear ip bgp flap-statistics 10.0.0.0/16
```

This example clears the dampening statistics for a BGP4 route for VRF "red".

```
device# clear ip bgp flap-statistics 10.0.0.0/16 vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip bgp local routes

Clears BGP4 local routes from the IP route table and resets the routes.

Syntax

clear ip bgp local routes [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4 local routes.

```
device# clear ip bgp local routes
```

This example clears BGP4 local routes for VRF "red".

```
device# clear ip bgp local routes vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip bgp neighbor

Requests a dynamic refresh of BGP4 connections or routes from a neighbor, with a variety of options.

Syntax

clear ip bgp neighbor { **all** | *as-num* | *ip-addr* | *peer-group-name* } [**last-packet-with-error** | **notification-errors** | **soft** [**in** [**prefix-filter**] | **out**] | **soft-outbound** | **traffic**] [**vrf** *vrf-name*]

Parameters

all
Resets and clears all BGP4 connections to all neighbors.

as-num
Clears all BGP4 connections within this autonomous system. Range is from 1 through 4294967295.

peer-group-name
Clears all BGP4 connections in this peer group. Range is from 1 through 63 characters.

ip-addr
Clears all BGP4 connections with this IPv4 address, in dotted-decimal notation.

last-packet-with-error
Clears all BGP4 connections identified as having the last packet received with an error.

notification-errors
Clears all BGP4 connections identified as having notification errors.

soft
Refreshes routes received from or sent to the neighbor.

in
Refreshes received routes.

prefix-filter
Refreshes Outbound Route Filters (ORFs) that are prefix-based.

out
Refreshes sent routes.

soft-outbound
Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

NOTE
Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4 route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

traffic
Clears the counters (resets them to 0) for BGP4 messages.

vrf *vrf-name*
Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example refreshes all BGP4 neighbor connections.

```
device# clear ip bgp neighbor all
```

This example refreshes all BGP4 neighbor connections for VRF "red".

```
device# clear ip bgp neighbor all vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip bgp routes

Clears BGP4 routes from the IP route table and resets the routes.

Syntax

clear ip bgp routes [*ip-addr* [**/** *mask*]] [**vrf** *vrf-name*]

Parameters

ip-addr
: IPv4 address of a specified route in dotted-decimal notation.

mask
: (Optional) IPv4 mask of a specified route in CIDR notation.

vrf *vrf-name*
: Specifies the name of the VRF instance to associate with subsequent address-family configuration mode commands.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4 routes.

```
device# clear ip bgp routes 10.0.0.0/16
```

This example clears BGP4 routes for VRF instance "red":

```
device# clear ip bgp routes 10.0.0.0/16 vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip bgp traffic

Clears the BGP4 message counter for all neighbors.

Syntax

clear ip bgp traffic [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example clears the BGP4 message counters.

```
device# clear ip bgp traffic
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip dhcp relay statistics

Clears IP DHCP Relay statistics.

Syntax

clear ip dhcp relay statistics ip-address *ip-address*

Command Default

DHCP relay statistics are present on the DHCP server.

Parameters

ip-address *ip-address*

IPv4 address of DHCP server where client requests are to be forwarded.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clear IP DHCP Relay statistics for a specific IP DHCP Relay address or all addresses on the device.

Examples

The following example clears statistics for IP DHCP Relay

```
device# clear ip dhcp relay statistics ip-address 10.1.0.1
```

Release version	Command history
18x.1.00	This command was introduced.

clear ip ospf

Clears OSPF data processes, counters, neighbors, or routes.

Syntax

clear ip ospf all [**vrf** *vrf-name*]

clear ip ospf counters { **all** | **ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id* } [**vrf** *vrf-name*]

clear ip ospf neighbor { *ip-addr* | **all** } [**vrf** *vrf-name*]

clear ip ospf routes { *ip-addr/mask* | **all** } [**vrf** *vrf-name*]

Parameters

all
Clears all OSPF data processes.

vrf *name*
Specifies a VRF.

counters
Clears OSPF counters.

all
Clears all counters.

ethernet *slot* **/** *port*
Specifies an Ethernet slot and port.

loopback *number*
Specifies a loopback interface. Valid values range from 1 through 255.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

neighbor
Clears neighbors.

ip-addr
Specifies the IP address of the neighbor.

all
Clears all neighbors.

routes
Clears matching routes or clears all routes.

ip-addr/mask
Clears all routes that match the prefix and mask that you specify.

all
Clears all routes.

Modes

Privileged EXEC mode

Examples

The following example restarts the OSPF processes.

```
device# clear ip ospf all
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ip route

Clears a specified route or all IP routes in the IP routing tables.

Syntax

clear ip route { *A.B.C.D* | *A.B.C.D/M* } [**vrf** *vrf-name*]

clear ip route all [**vrf** *vrf-name*]]

clear ip route slot *line-card-number* [*A.B.C.D* | *A.B.C.D/M*] [**vrf** *vrf-name*]

Parameters

A.B.C.D
Specifies an IPv4 address.

A.B.C.D/M
Specifies an IPv4 address and mask.

vrf *vrf-name*
Specifies a VRF instance from which the user is currently retrieving routes.

all
Specifies all routes.

slot *line-card-number*
Specifies a line card.

Modes

Privileged EXEC mode

Examples

The following example clears the IP route specified by IP address 192.158.1.1/24.

```
device# clear ip route 192.158.1.1/24
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 bgp dampening

Reactivates suppressed BGP4 routes.

Syntax

clear ipv6 bgp dampening [*ipv6-addr* { **/** *mask* }] [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a specified route in dotted-decimal notation.

mask
IPv6 mask of a specified route in CIDR notation.

vrf *vrf-name*
Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example unsuppresses all suppressed BGP4+ routes.

```
device# clear ipv6 bgp dampening
```

The following example unsuppresses suppressed BGP4+ routes for VRF "red".

```
device# clear ipv6 bgp dampening vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 bgp flap-statistics

Clears route-flap statistics for BGP4+ routes.

Syntax

clear ipv6 bgp flap-statistics [*ipv6-addr* { **/** *mask* } | **neighbor** *ipv6-addr* | **regular-expression** *string*] [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a specified route in dotted-decimal notation.

mask
(Optional) IPv6 mask of a specified route in CIDR notation.

neighbor
Clears route-flap statistics only for routes learned from the specified neighbor.

ipv6-addr
IPv6 address of the neighbor.

regular-expression
Specifies a regular expression.

string
Regular expression.

vrf *vrf-name*
Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears all dampening statistics for a BGP4+ route.

```
device# clear ipv6 bgp flap-statistics
```

This example clears the dampening statistics for a BGP4+ route for VRF "red".

```
device# clear ipv6 bgp flap-statistics vrf red
```

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 bgp local routes

Clears BGP4+ local routes from the IP route table and resets the routes.

Syntax

clear ipv6 bgp local routes [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4+ local routes.

```
device# clear ipv6 bgp local routes
```

This example clears BGP4+ local routes for VRF "red".

```
device# clear ipv6 bgp local routes vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 bgp neighbor

Requests a dynamic refresh of BGP4+ connections or routes from a neighbor, with a variety of options.

Syntax

clear ipv6 bgp neighbor [**all** | *as-num* | *peer-group-name* | *ipv6-addr*] [**last-packet-with-error** | **notification-errors** | **soft** [**in** [**prefix-filter**] | **out**] | **soft-outbound** | **traffic**] [**vrf** *vrfname*]

Parameters

all
Resets and clears all BGP4+ connections to all neighbors.

as-num
Clears all BGP4+ connections within this autonomous system. Range is from 1 through 4294967295.

peer-group-name
Clears all BGP4+ connections in this peer group. Range is from 1 through 63 characters.

ipv6-addr
Clears all BGP4+ connections with this IPv6 address, in dotted-decimal notation.

last-packet-with-error
Clears all BGP4+ connections identified as having the last packet received with an error.

notification-errors
Clears all BGP4+ connections identified as having notification errors.

soft
Refreshes routes received from or sent to the neighbor.

in
Refreshes received routes.

prefix-filter
Refreshes Outbound Route Filters (ORFs) that are prefix-based.

out
Refreshes sent routes.

soft-outbound
Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

NOTE
Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4+ route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

traffic
Clears the counters (resets them to 0) for BGP4+ messages.

vrf *vrf-name*
Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example refreshes all BGP4+ neighbor connections.

```
device# clear ipv6 bgp neighbor all
```

This example resets all the counters for BGP4+ messages.

```
device# clear ipv6 bgp neighbor all traffic
```

This example clears BGP4+ connections with a specified peer group.

```
device# clear ipv6 bgp neighbor P1
```

This example clears BGP4+ connections with a specified peer group for VRF "red".

```
device# clear ipv6 bgp neighbor P1 vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 bgp routes

Clears BGP4+ routes from the IP route table and resets the routes.

Syntax

clear ipv6 bgp routes [*ipv6-addr* [**/** *mask*]] [**vrf** *vrfname*]

Parameters

ipv6-addr
IPv6 address of a specified route in dotted-decimal notation.

mask
(Optional) IPv6 mask of a specified route in CIDR notation.

vrf *vrf-name*
Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears specific BGP4+ routes.

```
device# clear ipv6 bgp routes 2000::/64
```

This example clears specific BGP4+ routes for VRF "red".

```
device# clear ipv6 bgp routes 2000::/64 vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 bgp traffic

Clears the BGP4+ message counter for all neighbors.

Syntax

clear ipv6 bgp traffic [**vrf** *vrf-name*]

Modes

Privileged EXEC mode

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Examples

This example clears all BGP4+ message counters.

```
device# clear ipv6 bgp traffic
```

This example clears BGP4+ message counters for VRF "red".

```
device# clear ipv6 bgp traffic vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 counters

Clears IPv6 counters on all interfaces or on a specified interface.

Syntax

clear ipv6 counters [**all** | **interface** { **ethernet** *slot/port* | **loopback** *port-number* | **ve** *ve-id* }

Parameters

all

Specifies all interfaces.

ethernet

Represents a valid, physical Ethernet subtype.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback

Specifies a loopback interface.

port-number

Port number of the loopback interface. The range is from 1 through 255.

ve

Specifies a virtual Ethernet (VE) interface.

ve_id

ID of the VE interface. The range is from 1 through 4096.

Modes

Privileged EXEC mode

Examples

The following example clears counters on Ethernet 2/3.

```
device# clear ipv6 counters interface ethernet 2/3
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 dhcp relay statistics

Clears IPv6 DHCP Relay statistics

Syntax

clear ipv6 dhcp relay statistics ip-address *ip-address*

Parameters

ip-address *ip-addr*

IPv6 address of DHCP server where client requests are to be forwarded.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clear all the DHCP Relay statistics.

Examples

Clear all the DHCP Relay statistics on the device.

```
device# clear ipv6 dhcp relay statistics
```

clear ipv6 nd suppression-cache

Clears the neighbor discovery (ND)-suppression cache. You can also clear the cache for a specified bridge domain or VLAN.

Syntax

clear ipv6 nd suppression-cache [**bridge-domain** *bridge-domain-id* | **vlan** *vlan-id*]

Parameters

bridge-domain *bridge-domain-id*

Specifies a bridge domain. The range is from 1 through 1024.

vlan *vlan-id*

Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example clears the ND-suppression cache.

```
device#  clear ipv6 nd suppression-cache
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 nd suppression-statistics

Clears neighbor discovery (ND)-suppression statistical information. You can also clear statistics for a specified bridge domain or VLAN.

Syntax

clear ipv6 nd suppression-statistics [**bridge-domain** *bridge-domain-id* | **vlan** *vlan-id*]

Parameters

bridge-domain *bridge-domain-id*
Specifies a bridge domain. The range is from 1 through 1024.

vlan *vlan-id*
Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example clears all ND-suppression statistics.

```
device#  clear ipv6 nd suppression-statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 neighbor

Removes entries from the IPv6 neighbor table.

Syntax

clear ipv6 neighbor [*ipv6-address*] [**ethernet** *slot/port* | **ve** *ve-number*] [**force-delete** | **no-refresh** | **vrf** *vrf-name*]

Parameters

ipv6-address
Removes cache entries for the specified IPv6 address.

ethernet *slot/port*
Removes neighbor entries for the Ethernet interface. A valid slot number is 0.

ve *ve-number*
Removes neighbor entries for the the specified Virtual Ethernet (VE) interface.

force-delete
Force deletes all the dynamic neighbor entries.

no-refresh
Deletes all the dynamic neighbor entries.

vrf *vrf-name*
Removes entries from the IPv6 neighbor table for the specified VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

You must specify the *ipv6-address* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373.

Examples

The following example removes neighbor entries for Ethernet interface 0/1.

```
device# clear ipv6 neighbor ethernet 0/1 force-delete
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 ospf

Clears OSPFv3 data processes, counts, force-spf, neighbors, redistribution, routes, and traffic.

Syntax

clear ipv6 ospf all [**vrf** *vrf-name*]

clear ipv6 ospf counts [**vrf** *vrf-name*]

clear ipv6 ospf counts neighbor *A.B.C.D* [**vrf** *vrf-name*]

clear ipv6 ospf counts neighbor interface { **ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id* } [*A.B.C.D*]

clear ipv6 ospf { **force-spf** | **redistribution** | **traffic** } [**vrf** *vrf-name*]

clear ipv6 ospf neighbor *A.B.C.D* [**vrf** *vrf-name*]

clear ipv6 ospf neighbor all [**vrf** *vrf-name*]

clear ipv6 ospf neighbor interface { **ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id* } [*A.B.C.D*]

clear ipv6 ospf routes { *IPv6addr* | **all** } [**vrf** *vrf-name*]

Parameters

all
Clears all OSPFv3 data.

counts
Clears OSPFv3 counters.

neighbor
Clears all OSPF counters for a specified neighbor.

A.B.C.D
Specifies a neighbor.

vrf *vrf-name*
Specifies a VRF.

interface
Specifies an interface.

ethernet *slot* **/** *port*
Specifies an Ethernet slot and port.

loopback *number*
Specifies a loopback interface. Valid values range from 1 through 255.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

force-spf
Performs the shortest path first (SPF) calculation without clearing the OSPFv3 database.

redistribution
Clears OSPFv3 redistributed routes.

traffic

Clears OSPFv3 traffic statistics.

routes

Clears OSPFv3 routes.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **force-spf** keyword to perform the shortest path first (SPF) calculation without clearing the OSPFv3 database.

Examples

The following example restarts the OSPFv3 processes.

```
device# clear ipv6 ospf all
```

The following example clears all OSPFv3 counters for a specified neighbor.

```
device# clear ipv6 ospf counts neighbor 10.10.10.1
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 route

Clears IPv6 routes.

Syntax

clear ipv6 route [*ipv6-address* **vrf** *vrf-name*] [**all vrf** *vrf-name*] [**slot** *slot-number*]

Parameters

i*ipv6-address*
: Removes IPv6 routes for the specified IPv6 address.

vrf *vrf-name*
: Removes IPv6 routes for the specified VPN Routing and Forwarding (VRF) instance.

all
: Removes all IPv6 routes.

slot *slot-number*
: Removes IPv6 routes for the specified line card.

Modes

Privileged EXEC mode

Examples

The following example clears IPv6 routes associated with the prefix 2000:7838::/32.

```
device# clear ipv6 route 2000:7838::/32
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear ipv6 vrrp statistics

Clears IPv6 VRRPv3 session statistics for all virtual groups, for a specified interface, or for a specified virtual group.

Syntax

clear ipv6 vrrp statistics [**all**]

clear ipv6 vrrp statistics [**interface** { **ethernet** *slot*/*port* | **ve** *vlan_id* }]

clear ipv6 vrrp statistics [**session** *VRID*]

Parameters

all
Clears all IPv6 VRRP statistics.

session *VRID*
Specifies the virtual group ID on which to clear statistics. The range is from 1 through 128.

interface
Specifies an interface.

ethernet *slot port*
Specifies a valid, physical Ethernet interface with a slot and port number.

ve *vlan_id*
Specifies the VE VLAN number. The range is from 1 through 4096.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported in IPv6 VRRPv3 and VRRP-E-v3.

Examples

The following example clears all IPv6 VRRPv3 statistics for all virtual groups.

```
device# clear ipv6 vrrp statistics all
```

The following example clears statistics for an IPv6 VRRPv3 session of virtual group 25.

```
device# clear ipv6 vrrp statistics session 25
```

The following example clears IPv6 VRRPv3 statistics on a specified virtual Ethernet interface.

```
device# clear ipv6 vrrp statistics interface ve 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear lacp

Clears the Link Aggregation Group Control Protocol (LACP) counters on a specific port-channel.

Syntax

clear lacp *number* **counters**

Parameters

number

Specifies the port channel-group number. Valid values range from 1 through 64.

counters

Clears traffic counters.

Modes

Privileged EXEC mode

Examples

To clear the LACP counters for a specific port-channel:

```
device# clear lacp 10 counters
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear lacp counters

Clears the Link Aggregation Group Control Protocol (LACP) counters on all port-channels.

Syntax

clear lacp counters

Modes

Privileged EXEC mode

Examples

To clear the counters for all port-channels:

```
device# clear lacp counters
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear link-oam statistics

Clears the Link OAM statistics.

Syntax

clear link-oam statistics

Modes

Privileged EXEC mode

Examples

This example shows how to clears the Link OAM statistics.

```
device# clear link-oam statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear lldp neighbors

Clears the Link Layer Discovery Protocol (LLDP) neighbor information on all or specified ethernet interfaces.

Syntax

clear lldp neighbors [**interface ethernet** *slot/port*]

Parameters

ethernet

Use this parameter to specify an ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, this command clears the LLDP neighbor information received on all the interfaces.

Examples

To clear the LLDP neighbor information for all interfaces:

```
device# clear lldp neighbors
```

To clear LLDP neighbor information on a specific ethernet interface:

```
device# clear lldp neighbors interface ?
Possible completions:
ethernet   Ethernet interface
device# clear lldp neighbors interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
  1/1
  1/2
  1/3
  1/4
  1/5
  1/6
  1/8
  1/9
  1/10
  1/11
  1/12
  1/13
  1/14
  1/15
  1/16
  1/17
  1/18
  1/19
  1/20
  1/21
  1/22
  1/23
  1/24
  1/25
  1/29
  1/30
  1/31
device# clear lldp neighbors interface ethernet 1/24
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear lldp statistics

Clears LLDP statistics for all interfaces or a specified Ethernet interface.

Syntax

clear lldp statistics [**interface ethernet** *slot/port*]

Parameters

ethernet

Use this parameter to specify an ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, this command clears all the LLDP statistics on all interfaces.

Examples

To clear all the LLDP statistics for all interfaces:

```
device# clear lldp statistics
```

To clear LLDP neighbor information on a specific ethernet interface:

```
device# clear lldp statistics interface ?
Possible completions:
ethernet   Ethernet interface
device# clear lldp statistics interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
  1/1
  1/2
  1/3
  1/4
  1/5
  1/6
  1/8
  1/9
  1/10
  1/11
  1/12
  1/13
  1/14
  1/15
  1/16
  1/17
  1/18
  1/19
  1/20
  1/21
  1/22
  1/23
device#clear lldp statistics interface ethernet 1/23
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear logging raslog

Clears RASLog messages from the router.

Syntax

clear logging raslog [**message-type** { **DCE** | **SYSTEM** }]

Command Default

Clear all RASLog messages on the local router.

Parameters

message-type

Clears RASLog messages of the specified repository type.

SYSTEM

Clears system LOG messages.

DCE

Clears DCE application messages.

Modes

Privileged EXEC mode

Usage Guidelines

This command clears all RASLog messages by default.

SLX-OS maintains two separate internal message storage repositories, SYSTEM and DCE. A RASLog message can have one or more type attributes. For example, a message can be of type DCE, FFDC, and AUDIT.

NOTE

A message cannot have both LOG and DCE type attributes. LOG type messages are stored in the SYSTEM message-type repository and DCE type messages are stored in the DCE message-type repository. LOG type messages are not stored in the DCE message-type repository and DCE type messages are not stored in the SYSTEM message-type repository.

Examples

To clear all RASLog messages:

```
device# clear logging raslog

DCE Raslogs are cleared
SYSTEM Raslogs are cleared
```

To clear all messages from the DCE message-type repository:

```
device# clear logging raslog message-type DCE

DCE Raslogs are cleared
```

To clear all messages from the SYSTEM message-type repository:

```
device# clear logging raslog message-type SYSTEM

SYSTEM Raslogs are cleared
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear loop-detection

Enables ports that were disabled by the loop detection (LD) protocol, and clears LD statistics at the global, interface, or VLAN level.

Syntax

clear loop-detection [**interface** { **ethernet** *interface* | **port-channel** *interface* } | **vlan** *vlan-id*]

Command Default

This feature is disabled.

Parameters

interface

Specifies an Ethernet or port-channel interface.

ethernet*interface*

Specifies an Ethernet interface.

port-channel*interface*

Specifies a port-channel interface.

vlan *vlan-id*

Specifies a VLAN.

Modes

Privileged EXEC mode

Examples

To enable LD-disabled ports and clear LD statistics on all interfaces:

```
device# clear loop-detection
```

To enable LD-disabled ports and clear LD statistics on an Ethernet interface:

```
device# clear loop-detection interface ethernet 2/6
```

To enable LD-disabled ports and clear LD statistics on a port-channel interface:

```
device# clear loop-detection interface port-channel 20
```

To enable LD-disabled ports and clear LD statistics on a VLAN:

```
device# clear loop-detection interface vlan 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear loop-detection bridge-domain

Enables ports associated with the bridge domain (BD) that were disabled as part of loop detection, and also clears the LD statistics per BD.

Syntax

clear loop-detection bridge-domain *BD_ID*

Command Default

None

Parameters

BD_ID

Specifies a BD.

Modes

Privileged EXEC mode

Examples

The following example enables ports associated with BD 8 and clears LD statistics for that BD.

```
device# clear loop-detection bridge-domain 8
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear mac-address-table

Removes interface entries from the MAC address table.

Syntax

clear mac-address-table { **cluster** *cluster-id* [**client** [*client-id*]] }

clear mac-address-table dynamic [**address** *mac-address* | **bridge-domain** [*id*] | **interface ethernet** *slot/port* | **port-channel** *number* | **logical-interface ethernet** *slot/port* [*:brk-out*]*. lif-id* | **vlan** *vlan-id*]

Parameters

bridge-domain
Specifies clearing MAC addresses learned under a bridge domain.

id
Specifies a bridge-domain identifier.

cluster *cluster-id*
Specifies clearing MAC addresses from an MCT cluster ID. The ID range is 1 - 65535.

client *client-id*
Specifies clearning the client instance. Specify the client ID with a maximum of 64 characters.

dynamic address *MAC-address*
Specifies clearning the dynamic MAC address. The valid format is *H.H.H* (available in Privileged EXEC mode only).

interface ethernet *slot/port*
Specifies clearning the ethernet interface with a valid slot number/port number.

port-channel *number*
Specifies clearning the port channel interface number. The range is from 1 - 512 based on the platform.

logical-interface ethernet *slot/port* [*:brk-out*]*. lif-id*
Specifies clearning the logical ethernet interface on a specified slot/port number. The breakout interface option can be used with the LIF ID.

vlan *vlan id*
Specifies clearning the VLAN interface. The VLAN ID range is from 1 - 4090.

Modes

Privileged EXEC mode.

Usage Guidelines

When a bridge-domain identifier is not specified, MAC addresses learned under all bridge domains are removed from the MAC address table. If a specific address is not specified, all dynamic mac-addresses are deleted from the MAC address table.

Examples

The following example shows how to clear MAC addresses learned under bridge domain 1 from the MAC address table.

```
device# clear mac-address-table dynamic bridge-domain 1
```

The following example shows how to clear MAC addresses learned from vlan 1 from the MAC address table.

```
device# clear mac-address-table dynamic vlan 1
```

The following example shows how to clear MAC addresses from a logical interface ethernet 3/10 LIF breakout interface.

```
device# clear mac-address-table dynamic 3/10:5.200
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear mvrp statistics

Clears the MVRP statistics for all Ethernet and port-channel interfaces, or for a specific Ethernet or port-channel interface.

Syntax

clear mvrp statistics [**interface** { **ethernet** *slot/port* | **port-channel** *number* }]

Parameters

interface

Clears the MVRP statistics for a specific interface.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies the port-channel interface.

Modes

Privileged Exec mode

Usage Guidelines

If you enter this command without any options, the MVRP statistics for all Ethernet and port-channel interfaces are cleared.

Examples

The following command clears the MVRP statistics for all Ethernet and port-channel interfaces.

```
device# clear mvrp statistics
```

The following command clears the MVRP statistics for a specified Ethernet interface.

```
device# clear mvrp statistics interface ethernet 1/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear overlay-gateway

Clear counters for the specified gateway.

Syntax

clear overlay-gateway *name* { **statistics** | **vlan statistics** }

Parameters

name
Specifies the name of the VXLAN gateway profile.

statistics
Clears all statistics for the VXLAN gateway.

vlan statistics
Clears per-VLAN statistics for the VXLAN gateway.

Modes

Privileged EXEC mode

Usage Guidelines

If you specify the VXLAN gateway name, the gateway must already be configured.

If you specify VLAN IDs, these VLANS must already be configured as exported VLANs for the gateway.

Examples

The following example clears all counters for the already configured VXLAN gateway named gateway1.

```
device# clear overlay-gateway gateway1 statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear policy-map-counters

Clears the policy map counters.

Syntax

clear policy-map-counters [**interface ethernet** *slot/port*] [**in** | **out**]

Parameters

interface
Specifies an interface.

ethernet
Represents a valid, physical Ethernet type for all available Ethernet speeds.

slot/port
Specifies a slot and port number.

in
Specifies clearing the ingress counters.

out
Specifies clearing the egress counters.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **clear policy-map-counters** command without any keyword options to clear all of the policy map counters.

Examples

To clear the policy map counters for a specific interface use the following command:

```
device# clear policy-map-counters interface ethernet 2/2
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear qos flowcontrol statistics

Clears flow control statistics for a specific interface, port channel, or all interfaces on the device.

Syntax

clear qos flowcontrol statistics { **all** | **ethernet** *slot/port* | **port-channel** *number* }

Parameters

all

Clears the flow control statistics on all interfaces in the device.

ethernet *slot/port*

Clears the flow control statistics on the specified interface.

port-channel *number*

Clears the flow control statistics on the interface for the specified port channel.

Modes

Privileged EXEC mode

Examples

The following example clears the flow control statistics for all interfaces, as displayed by the **show qos flowcontrol interface** command.

```
device# clear qos flowcontrol statistics interface all
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear spanning-tree counter

Clears all spanning-tree counters on an Ethernet or port-channel interface.

Syntax

clear spanning-tree counter [**interface** { **ethernet** *slot/port* | **port-channel** *number* }

Parameters

interface

Specifies an interface.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel. The number of available channels ranges from 1 through 6144.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, spanning-tree counters are cleared for all interfaces.

Examples

To clear spanning-tree counters for all interfaces:

```
device# clear spanning-tree counter
```

To clear spanning-tree counters for an Ethernet interface:

```
device# clear spanning-tree counter interface ethernet 0/1
```

To clear spanning-tree counters for port-channel 23:

```
device# clear spanning-tree counter interface port-channel 23
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear spanning-tree detected-protocols

Clears all spanning-tree detected protocols on an Ethernet or port-channel interface.

Syntax

clear spanning-tree detected-protocols [**interface** { **ethernet** *slot/port* | **port-channel** *number* }

Parameters

interface

Specifies an interface.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel. The number of available channels ranges from 1 through 6144.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, spanning-tree detected protocols are cleared for all interfaces.

Examples

To clear detected protocols on all interfaces:

```
device# clear spanning-tree detected-protocols
```

To clear detected protocols on an Ethernet interface:

```
device# clear spanning-tree detected-protocols interface ethernet 0/1
```

To clear detected protocols on port-channel 23:

```
device# clear spanning-tree detected-protocols interface port-channel 23
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear statistics bridge-domain

Clears the statistics for all the logical interfaces on bridge domains.

Syntax

clear statistics bridge-domain bd-id

Parameters

bd-id

The bridge domain ID.

Command Default

Statistics are disabled.

Modes

Privileged EXEC mode

Usage Guidelines

This command is also available in global configuration mode.

The **clear statistics bridge-domain** bd-id command clears the statistics for all the logical interfaces on a specific bridge domain.

Examples

The following example shows how to clear the statistics for all the logical interfaces on all bridge domains.

```
device# clear statistics bridge-domain
```

The following example shows how to clear the statistics for all the logical interfaces on bridge domain 2.

```
device# clear statistics bridge-domain 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear statistics vlan

Clears the statistics for all the ports and port channels on configured VLANs.

Syntax

clear statistics vlan vlan-id

Parameters

vlan-id

The specific VLAN ID.

Command Default

Statistics are disabled.

Modes

Privileged EXEC mode

Usage Guidelines

This command is also available in global configuration mode.

The **clear statistics vlan** vlan-id command clears the statistics for all the ports and port channels on the given VLAN.

Examples

The following example shows how to clear the statistics for all the ports and port channels on the given VLAN.

```
device# clear statistics vlan
```

The following example shows how to clear the statistics for all the ports and port channels on VLAN 10.

```
device# clear statistics vlan 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear tm voq-stat ingress-device

Clears the traffic management VOQ statistics on the ingress device for a specified ethernet port, or for all ports.

Syntax

clear tm voq-stat ingress-device {{ **ethernet** *slot/port* } {**egress-port ethernet** *slot/port*} | **all** }}

clear tm voq-stat ingress-device all egress-port ethernet *slot/port* | **all**

Parameters

ethernet *slot/port*
Specifies the ethernet interface in slot/port format.

egress-port ethernet *slot/port*
Specifies clearing the traffic management statistics on the egress ethernet slot/ port.

all
Specifies clearing the traffic management statistics for all ports.

Modes

Privileged EXEC mode.

Examples

To clear VOQ statistics information on the egress-port for ethernet 1/1, use the following command.

```
device# clear tm voq-stat ingress-device ethernet 1/1 egress-port ethernet 1/1
```

To clear all VOQ statistics information on the egress-port for ethernet 1/1, use the following command.

```
device# clear tm voq-stat ingress-device all egress-port ethernet 1/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear tunnel statistics

Clears statistics from the tunnel interfaces.

Syntax

clear tunnel statistics *tunnel-id*

Parameters

tunnel-id

Specifies the tunnel ID.

Modes

Privileged EXEC mode

Examples

This example removes statistics from a tunnel interface.

```
device# clear tunnel statistics 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

clear vrrp statistics

Clears VRRP statistics.

Syntax

clear vrrp statistics

clear vrrp statistics [**interface** { **ethernet** *slot*/*port* | **ve** *vlan_id* }]

clear vrrp statistics session *VRID*

Parameters

interface
Specifies an interface.

ethernet *slot port*
Specifies a valid, physical Ethernet interface with a slot and port number.

ve *vlan_id*
Specifies the VE VLAN number. The range is from 1 through 6144.

session *VRID*
Specifies the virtual group ID on which to clear statistics. The range is from 1 through 255.

Modes

Privileged EXEC mode

Usage Guidelines

This command clears VRRP session statistics for all virtual groups, for a specified interface or for a specified virtual group.

This command is for VRRP and VRRP-E. VRRP-E supports only the **ve** *vlan_id* interface type.

To clear all vrrp statistics, use the **clear vrrp statistics** command with no operands.

Examples

The following example clears all VRRP statistics for all virtual groups.

```
device# clear vrrp statistics
```

The following example clears statistics for Ethernet interface 1/6.

```
device# clear vrrp statistics interface ethernet 1/6
```

The following example clears statistics for a session for a VRRP virtual group called "vrrp-group-25".

```
device# clear vrrp statistics session 25
```

The following example clears VRRP statistics on a specified virtual Ethernet (VE) interface.

```
device# clear vrrp statistics interface ve 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

CLI

In a Python shell, runs a device CLI command or series of commands. You can also assign the output of such commands to a Python object.

Syntax

CLI `('` *device-CLI-command* `'` [**\n** `'` *device-CLI-command* `'`] [[**do_print =**] { **True** | **False** }] **)**

Parameters

device-CLI-command
An SLX-OS CLI command. You separate additional commands with **\n**.

do_print =
Specify whether or not to print the output of *device-CLI-command* to the default device. The default is to print the output.

True
Print the output.

False
Do not print the output.

Modes

Python command shell

Usage Guidelines

Divergences between Extreme CLI syntax and Python syntax include the following differences:

- Although in general, Extreme CLI syntax is not case-sensitive, our convention is to use lower-case.
- Python syntax is case sensitive. Regarding the syntax documented in the current topic, note the following:
  - The syntax of the command is upper case (CLI) and not lower case (cli).
  - The syntax of the **do_print =** options is to capitalize the first letter: { **True** | **False** }

In Python, double quotes (**"**) and single quotes (**'**) are equivalent.

As delimiter between multiple CLI commands, use \n.

There is a difference between running a sequence of SLX-OS CLI commands in the Python shell rather than in the standard SLX-OS interface. Whereas in the standard interface the result of a command is persistent, in the Python shell each `CLI( )` statement is independent of any preceding ones.

For support of the `CLI( )` command, although a Python script must include a `from CLI import CLI` statement, this statement is automatically implemented when launching the Python interpreter interactively.

Within a script or interactive session, if you assign an Extreme CLI command or series of commands to a Python variable, you can then append the following functions to the variable:

- **.rerun()**—updates the variable from a new run of the CLI command or series of commands.

```
device# python
Python 3.3.2 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_show_running_ve = CLI('show running-config interface ve')
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016

% No entries found.
# The SLX-OS show running-config interface ve command is run,
# and that command is assigned to the Python variable cmd_show_running_ve.

>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
# A series of three commands are run and assigned to the Python variable cmd_config_ve.
!Command: configure
 interface ve 101-103
!Time: Mon Aug 22 16:53:13 2016


>>> cmd_show_running_ve.rerun()
# The rerun() function appended to cmd_show_running_ve gives the following output:
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016

interface Ve 101
 shutdown
!
interface Ve 102
 shutdown
!
interface Ve 103
 shutdown
!
!
```

- **.get_output()**—returns the value of a new run of the CLI command or series of commands, as a list.

```
#Required in all scripts for SLX:
from CLI import CLI
# Import the Python Regular Expressions (re) module:
import re
# Create Python objects:
slot_firmware = {}

cmd_show_ver = CLI("show ver", False)
# Using .get_output(), assign the result of show ver to a Python object named output:
output = cmd_show_ver.get_output()
for line in output:
    found = re.search(r'^(\S+)\s+(\S+)\s+(\S+)\s+ACTIVE.*$', line, re.M)
    if found:
        slot_firmware[found.group(1)] = found.group(3)

print("SLOT_FIRMWARE:\n")
for key in slot_firmware:
    print("\t", key, "\t=> ", slot_firmware[key])
```

Examples

The following example launches the Python shell and then both assigns a series of CLI configuration commands to a Python variable and runs those commands.

```
device# python
Python 3.3.2 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
!Command: configure
 interface ve 101-103
!Time: Mon Aug 22 16:57:36 2016
>>>
```

The following example launches the Python shell and then both assigns a CLI operational command to a Python variable and runs that command.

```
device# python
Python 3.3.2 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_reload_system = CLI('reload system \n y')
```

History

Release version	Command history
18x.1.00	This command was introduced.

client

Configures a Multi-Chassis Trunking (MCT) client for a cluster and access cluster client configuration mode.

Syntax

client *client-name client-id*

no client *client-name client-id*

Parameters

client-name

Specifies the client name as an ASCII string. The name can be up to 64 characters in length.

client-id

Specifies the cluster client ID. The ID value range can be from 1 through 512.

Modes

Cluster client configuration mode

Usage Guidelines

The **no** form of the command removes the client from the MCT cluster configuration.

Examples

The following example configures a cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

client-interface

Configures a CEP or CCEP interface to the cluster client instance.

Syntax

client-interface { **ethernet** *slot/port* | **port-channel** *number* }

no client-interface

Parameters

ethernet *slot/port*
Configures the specified Ethernet port as the client CEP or CCEP.

port-channel *number*
Configures the specified port channel as the client CEP or CCEP. The port channel *number* specifies the LAG ID.

Modes

Cluster client configuration mode

Usage Guidelines

The **no** form of the command removes the client interface.

The same client interface cannot be added under multiple client entries.

A client interface is not allowed to be updated when the client is in deploy state. It needs to be removed first before adding a new interface.

Examples

The following example shows how to configure a client interface.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# client-interface port-channel 3
```

History

Release version	Command history
18x.1.00	This command was introduced.

client-interfaces-shutdown

Disables the local client interfaces administratively in the cluster to moves all the traffic on the device to remote MCT peer device, resulting in fail-over of traffic to the peer device.

Syntax

client-interfaces shutdown

no client-interfaces shutdown

Modes

Cluster configuration mode

Usage Guidelines

The **no** form of the command reenables the local client interfaces.

Examples

The following example shows the disabling of all the client interfaces in the cluster.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client-interfaces shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

client-isolation

Sets the client-isolation mode to strict when the EVPN control session goes down between the MCT devices for Broadcast, Unknown unicast and Multicast (BUM) handling over Cluster Client Edge Port (CCEP) interfaces.

Syntax

client-isolation { **loose** | **strict** }

no client-isolation

Command Default

By default, client-isolation mode is loose.

Parameters

loose

Specifies the loose isolation mode.

strict

Specifies the strict isolation mode.

Modes

Cluster configuration mode

Usage Guidelines

In strict mode, when the EVPN control session goes down, the interfaces on both the cluster devices are administratively shut down. In strict mode, the client is completely isolated from the network if the control session is not operational.

In loose mode, when the EVPN control session goes down, the peer device performs the master/slave negotiation. After negotiation, the slave shuts down its peer ports, and the master peer ports continue to forward the traffic (keep-alive VLAN configured).

MCT cluster devices can operate in two modes. Both peer devices must be configured with the same mode configuration.

NOTE
The CLI allows modification of the client isolation mode on MCT cluster devices even when the cluster is deployed. You must have the same isolation mode configuration on both cluster devices.

The **no** form of the command resets the default client isolation mode behavior.

Examples

The following example shows how to configure the client isolation strict mode.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# client-isolation strict
```

History

Release version	Command history
18x.1.00	This command was introduced.

client-to-client-reflection

Enables routes from one Route Reflector (RR) client to be reflected to other clients by the host device on which it is configured.

Syntax

client-to-client-reflection

no client-to-client-reflection

Command Default

Enabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

When this command is used, the host device on which it is configured becomes the route-reflector server.

The **no** form of the command disables route reflection between clients.

Examples

The following example configures client-to-client reflection on the BGP host device for the IPv4 unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# client-to-client-reflection
```

The following example disables client-to-client reflection on the BGP host device for the IPv6 unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# no client-to-client-reflection
```

History

Release version	Command history
18x.1.00	This command was introduced.

clock set

Sets the local clock time and date.

Syntax

clock set *hh:mm:ss mm-dd-yy/yyyy*

Parameters

hh:mm:ss
Specifies the local clock time in hours, minutes, and seconds.

mm-dd-yy/yyyy
Specifies the local clock date in month, day, and year format. Year may be specified with two or four numbers.

Modes

Privileged EXEC mode

Usage Guidelines

Valid date and time settings range from January 1, 1970 to December 31, 2035.

An active NTP server, if configured, automatically updates and overrides the local clock time.

Examples

The following example sets the time and date to 31 minutes past 4 pm in the afternoon on July 28, 2016, for the local device:

```
device# clock set 16:31:35 07-28-16
```

History

Release version	Command history
18x.1.00	This command was introduced.

clock timezone

Sets the device system clock time zone options using either Greenwich Mean time (GMT) or one of the US time zones that uses Universal Time Coordinated (UTC) plus or minus a number of hours.

Syntax

clock timezone { **gmt** *gmt-time* | **us** *us-time* }

no clock timezone { **gmt** *gmt-time* | **us** *us-time* }

Parameters

gmt *gmt-time*

Specifies the GMT time zone. The value can be one of the following: gmt+00 (United Kingdom), gmt+01 (France, Germany), gmt+02 (Eastern Europe, South Africa), gmt+03, gmt+03:30, gmt+04, gmt+04:30, gmt+05, gmt+05:30 (India), gmt+06, gmt+06:30, gmt+07, gmt+08 (China, Hong Kong, Taiwan), gmt+09 (Japan, Korea), gmt+09:30, gmt +10 (Australia), gmt+10:30, gmt+11, gmt+11:30, gmt+12, gmt-01, gmt-02, gmt-03, gmt-03:30, gmt-04, gmt-05, gmt-06, gmt-07, gmt-08, gmt-08:30, gmt-09, gmt-09:30, gmt-10, gmt-11, gmt-12.

us *us-time*

Specifies the US time zone. The value can be one of the following: alaska, aleutian, arizona, central, east-indiana, eastern, hawaii, michigan, mountain, pacific, samoa.

Modes

Global configuration mode

Examples

The following example sets the system date and time to the US Samoa time zone.

```
device(config)# clock timezone us samoa
```

History

Release version	Command history
18x.1.00	This command was introduced.

cluster

Configures a Multi-Chassis Trunking (MCT) cluster and access the cluster configuration mode.

Syntax

cluster *cluster-name cluster-id*

no cluster *cluster-name cluster-id*

Parameters

cluster-name

Specifies the cluster name as an ASCII string. The cluster name can be up to 64 characters in length.

cluster-id

Specifies the cluster ID. The ID value range can be from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

NOTE

The *cluster-id* variable must be the same on both cluster devices.

The **no** form of the command removes the MCT cluster configuration.

Examples

The following example configures an MCT cluster.

```
device(config)# cluster MCT1 1
device(config-cluster-1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

cluster management node-id

Configures the node identifier (ID) in the IP-based management cluster.

Syntax

cluster management node-id *node-id*

no cluster management node-id *node-id*

Parameters

node-id

Specifies the unique node ID. The ID value range can be from 1 through 255.

Modes

Privileged EXEC mode

Usage Guidelines

The **no** form of the command removes the node ID from the management cluster configuration.

A node must have a unique identifier; nodes cannot have same node ID in the same management cluster.

Examples

The following example configures a node in a management cluster.

```
device# cluster management node-id 1
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

cluster-id

Configures a cluster ID for the route reflector.

Syntax

cluster-id { *num* | *ip-addr* }

no cluster-id { *num* | *ip-addr* }

Command Default

The default cluster ID is the device ID.

Parameters

num

Integer value for cluster ID. Range is from 1 through 65535.

ip-addr

IPv4 address in dotted-decimal notation.

Modes

BGP configuration mode

Usage Guidelines

When configuring multiple route reflectors in a cluster, use the same cluster ID to avoid loops within the cluster.

The **no** form of the command restores the default.

Examples

The following example configures a cluster ID for the route reflector.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# cluster-id 1234
```

History

Release version	Command history
18x.1.00	This command was introduced.

compare-med-empty-aspath

Enables comparison of Multi-Exit Discriminators (MEDs) for internal routes that originate within the local autonomous system (AS) or confederation

Syntax

compare-med-empty-aspath

no compare-med-empty-aspath

Command Default

Disabled.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following example configures the device to compare MEDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# compare-med-empty-aspath
```

Release version	Command history
18x.1.00	This command was introduced.

compare-routerid

Enables comparison of device IDs, so that the path-comparison algorithm compares the device IDs of neighbors that sent otherwise equal-length paths.

Syntax

compare-routerid

no compare-routerid

Modes

BGP configuration mode

Examples

The following example configures the device always to compare device IDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# compare-routerid
```

History

Release version	Command history
18x.1.00	This command was introduced.

confederation identifier

Configures a BGP confederation identifier.

Syntax

confederation identifier *autonomous-system number*

no confederation identifier

Command Default

No BGP confederation identifier is identified.

Parameters

autonomous-system number

Specifies an autonomous system number (ASN). The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command removes a BGP confederation identifier.

Examples

The following example specifies that confederation 65220 belongs to autonomous system 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65220
device(config-bgp-router)# confederation identifier 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

confederation peers

Configures subautonomous systems to belong to a single confederation.

Syntax

confederation peers *autonomous-system number* [*...autonomous-system number*]

no confederation peers

Command Default

No BGP peers are configured to be members of a BGP confederation.

Parameters

autonomous-system number

Autonomous system (AS) numbers for BGP peers that will belong to the confederation. The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command removes an autonomous system from the confederation.

Examples

The following example configures autonomous systems 65520, 65521, and 65522 to belong to a single confederation under the identifier 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65020
device(config-bgp-router)# confederation identifier 100
device(config-bgp-router)# confederation peers 65520 65521 65522
```

History

Release version	Command history
18x.1.00	This command was introduced.

configure terminal

Enters global configuration mode.

Syntax

configure terminal

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

copy

Copies configuration data.

Syntax

copy *source_file destination_file*

Parameters

source_file

The source file to be copied. Specify one of the following parameters:

default-config
The default configuration.

running-config
The running configuration.

startup-config
The startup configuration.

flash://*filename*
A file in the local flash memory.

ftp://*username:password@host_ip_address/path*
A file on a remote host. Transfer protocol is FTP.

scp://*username:password@host_ip_address/path*
A file on a remote host. Transfer protocol is SCP.

sftp://*username:password@host_ip_address/path*
A file on a remote host. Transfer protocol is SFTP.

tftp://*username:password@host_ip_address/path*
A file on a remote host. Transfer protocol is TFTP.

usb://*path*
A file on an attached USB device.

destination_file

The destination file. Specify one of the following parameters:

default-config
The default configuration.

running-config
The running configuration.

startup-config
The startup configuration.

flash://*filename*
A file in the local flash memory.

ftp://*username:password@host_ip_address//path*
A file on a remote host. Transfer protocol is FTP.

scp://*username:password@host_ip_address//path*
A file on a remote host. Transfer protocol is SCP.

sftp://*username:password@host_ip_address/path*
A file on a remote host. Transfer protocol is SFTP.

tftp://*username:password@host_ip_address/path*
A file on a remote host. Transfer protocol is TFTP.

usb://*path*
A file on an attached USB device.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to back up and restore configuration files with various protocols.

This command is supported only on the local switch.

IPv4 and IPv6 addresses are supported.

The special characters of dollar sign "$" and exclamation point "!" can be used as part of the password variable, provided they are paired with the correct escape characters. The "$" must be paired with two backslashes "\\". For example, if your password choice was "$password" on a remote server, you must use "username:\\$password@1.1.1.1" for the **copy** command. The exclamation point must be paired with a single backslash in the **copy** command, such as "username:\!password@1.1.1.1".

Examples

To save the running configuration to a file:

```
device# copy running-config flash://myconfig
```

To overwrite the startup configuration with a locally saved configuration file:

```
device# copy flash://myconfig running-config
```

To overwrite the startup configuration with a remotely archived configuration file:

```
device# copy scp://user:password@10.10.10.10//myconfig startup-config
```

To overwrite the startup configuration with a configuration file saved on an attached USB device:

```
device# copy usb://myconfig startup-config
```

History

Release version	Command history
18x.1.00	This command was introduced.

cos (Y1731)

Configures class of service (CoS).

Syntax

cos *class-of-service*

no cos

Parameters:

class-of-service

Specifies the CoS value. The range is from 1 to 8. The default value is 7.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the CoS configuration.

Examples

This example shows how to configure CoS.

```
device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
```

History

Release version	Command history
18x.1.00	This command was introduced.

crypto ca authenticate

Downloads the CA certificate from the remote certificate server for the trust point.

Syntax

crypto ca authenticate { *trustpointCA_name* **directory** *remote_dir_name* **file** *cert_file* **host** *host_address* **protocol** {FTP | SCP} **user** *host_login* **password** *host_user_password*}

no crypto ca authenticate { *trustpointCA_name*}

Parameters

trustpointCA_name trustpointCA_name
Defines the name of the trust point you are authenticating. This name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command. The string for the name can not be left blank. The length of the string can range from 1 through 64 characters.

directory *remote_dir_name*
Defines the directory where the certification file resides.

file *cert_file*
Defines the name of the certification file.

host *host_address*
Defines the host name or IP address of the remote certificate server.

protocol {FTP | SCP}
Specifies the use of either FTP or SCP protocol for accessing the certification file.

user *host_login*
Defines user name for the host server.

password *host_user_password*
Defines the password for the user name on the host server.

NOTE
It is recommended to not list the password in command line for security purposes; the user will be prompted for the password.

Modes

Privileged EXEC mode

Usage Guidelines

This is the CA certificate of the Trusted CA that you want to sign the CSR and generate the identity certificate.

The *trustpoint_CAname* name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command.

The **no** form of the command deletes the certificate.

Examples

Typical command example.

```
device# crypto ca authenticate t1 cert-type https protocol SCP host 10.70.12.102 user fvt directory /
users/home/crypto file cacert.pem
Password: **********
```

History

Release version	Command history
18x.1.00	This command was introduced.

crypto ca enroll

Enrolls the trust point by generating the Certificate Signing Request (CSR) and exporting it to the remote certificate server.

Syntax

crypto ca enroll { *trustpointCA_name* **directory** *remote_dir_name* **host** *host_address* **protocol** {**FTP** | **SCP**} **user** *host_login* **password** *host_user_password* **country** *country* **state** *state* **locality** *locality* **organization** *organization* **orgunit** *orgunit* **common** *common_name*}

Parameters

trustpointCA_name
Defines the name of the trust point you are enrolling. This name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command. The string for the name can not be left blank. The length of the string can range from 1 through 64 characters.

directory *remote_dir_name*
Defines the path of the directory to export the Certificate Signing Request.

host *host_address*
Defines the host name or IP address of the remote certificate server.

protocol {**FTP** | **SCP**}
Specifies the use of either FTP or SCP protocol for exporting the certification file.

user *host_login*
Defines user name for the host server.

password *host_user_password*
Defines the password for the user name on the host server.

NOTE
It is recommended to not list the password in command line for security purposes; the user will be prompted for the password.

country *country*
Defines the two-letter country code for generating the CSR.

state *state*
Defines the state name for generating the CSR.

locality *locality*
Defines the locality name for generating the CSR.

organization *organization*
Defines the organizational unit name for generating the CSR.

orgunit *orgunit*
Defines the name of the certification file.

common *common_name*
This is the name used to connect to the device through HTTPS. Enter a Fully Qualified Domain Name (FQDN) or IP address. If a FQDN is used, you need to configure a domain name and name server on the device.

Modes

Privileged EXEC mode

Usage Guidelines

The *trustpoint_CAname* name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command.

Examples

Typical command example:

```
device# crypto ca enroll t1 cert-type https country US state CA locality SJ organization BRC orgunit
SFI common myhost.extreme.com protocol SCP host 10.70.12.102 user fvt directory /proj/crypto
Password: **********
```

History

Release version	Command history
18x.1.00	This command was introduced.

crypto ca import

Imports the Identity Certificate for security configuration.

Syntax

crypto ca import { *trustpointCA_name* **certificate directory** *remote_dir_name* **file** *cert_file* **host** *host_address* **protocol** {**FTP** | **SCP**} **user** *host_login* **password** *host_user_password*}

no crypto ca import {*trustpointCA_name*}

Parameters

trustpointCA_name
Defines the name of the trust point you are authenticating. This name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command. The string for the name can not be left blank. The length of the string can range from 1 through 64 characters.

directory *remote_dir_name*
Defines the directory where the certification file resides.

file *cert_file*
Defines the name of the certification file.

host *host_address*
Defines the host name or IP address of the remote certificate server.

protocol {**FTP** | **SCP**}
Specifies the use of either FTP or SCP protocol for accessing the certification file.

user *host_login*
Defines user name for the host server.

password *host_user_password*
Defines the password for the user name on the host server.

NOTE
It is recommended to not list the password in command line for security purposes; the user will be prompted for the password.

Modes

Privileged EXEC mode

Usage Guidelines

The *trustpoint_CAname* name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command.

Use the no form of the command to remove the Identity Certificate.

Examples

Typical command example:

```
device# crypto ca import t1 certificate cert-type https protocol SCP host 10.70.12.102 user fvt
directory /users/crypto file cacert.pem
Password: **********
```

History

Release version	Command history
18x.1.00	This command was introduced.

crypto ca trustpoint

Defines the trust point for HTTPS security configuration.

Syntax

crypto ca trustpoint *trustpointCA_name*

no crypto ca trustpoint *trustpointCA_name*

Parameters

trustpointCA_name

Defines the name of the trust point. The string for the name can not be left blank. The length of the string can range from 1 through 64 characters.

Modes

Global configuration mode

Usage Guidelines

Use the **no crypto ca trustpoint** command to remove the trust point.

Examples

Typical command example:

Example using the no form of the command:

```
device(config)# no crypto ca trustpoint t1
```

History

Release version	Command history
18x.1.00	This command was introduced.

crypto key

Generates an RSA/ECDSA/DSA key pair to sign or encrypt and decrypt the security payload during security protocol exchanges for applications. You must sign and/or encrypt and decrypt the RSA/ECDSA/DSA key pair before you obtain a certificate for your device.

Syntax

crypto key label *key_label* [**rsa** | **ecdsa** | **dsa**] [**modulus** *key_size*]

no crypto key label *key_label*

Parameters

label *key_label*
The name of the key pair.

rsa
Generates an RSA key pair.

ecdsa
Generates an ECDSA key pair.

dsa
Generates a DSA key pair.

modulus *key_size*
Specifies the key size. The corresponding key sizes supported for each key type are:

- RSA: 1024 or 2048
- DSA: 1024
- ECDSA: 256,384, or 521

Modes

Global configuration mode

Usage Guidelines

Use the no form of this command to remove the key pair.

The key label must contain alphanumeric characters.

Examples

Typical command example for generating the key pair.

```
device(config)# crypto key label k1 rsa modulus 2048
device(config)# do show running-config crypto
crypto key label k1 rsa modulus 2048
```

The following is an example of using the no form of the command:

```
device(config)# no crypto key label k1
```

History

Release version	Command history
18x.1.00	This command was introduced.

dampening

Sets dampening parameters for the route in BGP address-family mode.

Syntax

dampening { *half-life reuse suppress max-suppress-time* | **route-map** *route-map* }

no dampening

Command Default

Disabled.

Parameters

half-life
Number of minutes after which the route penalty becomes half its value. Range is from 1 through 45. Default is 15.

reuse
Minimum penalty below which the route becomes usable again. Range is from 1 through 20000. Default is 750.

suppress
Maximum penalty above which the route is suppressed by the device. Range is from 1 through 20000. Default is 2000.

max-suppress-time
Maximum number of minutes a route can be suppressed by the device. Range is from 1 through 255. Default is 40.

route-map
Enables selection of dampening values established in a route map by means of the **route-map** command.

route-map
Name of the configured route map.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to disable dampening.

Use **dampening** without operands to set default values for all dampening parameters.

To use the dampening values established in a route map, configure the route map first, and then enter the **route-map** command, followed by the name of the configured route map.

A full range of dampening values (*half-life*, *reuse*, *suppress*, *max-suppress-time*) can also be set by means of the **set as-path prepend** command.

Examples

The following example enables default dampening as an IPv4 address-family function.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# dampening
```

The following example changes all the dampening values as an IPv6 address-family function.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# dampening 20 200 2500 40
```

History

Release version	Command history
18x.1.00	This command was introduced.

database-overflow-interval (OSPFv2)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

Command Default

0 seconds. If the device enters OverflowState, you must reboot before the device leaves this state.

Parameters

interval

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

This command specifies how long a device that has entered the OverflowState waits before resuming normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the device lapses back into OverflowState. If the configured value of the database overflow interval is zero, then the device never leaves the database overflow condition.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the device enters OverflowState. In this state, the device flushes all non-default AS-external-LSAs that the device had originated. The devie also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

The **no** form of the command disables the overflow interval configuration.

Examples

The following example configures a database-overflow interval of 60 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# database-overflow-interval 60
```

History

Release version	Command history
18x.1.00	This command was introduced.

database-overflow-interval (OSPFv3)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

Command Default

10 seconds. If the router enters OverflowState, you must reboot before the router leaves this state.

Parameters

interval

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds (24 hours).

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

This command specifies how long after a router that has entered the OverflowState before it can resume normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the router lapses back into OverflowState.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the router enters OverflowState. In this state, the router flushes all non-default AS-external-LSAs that the router had originated. The router also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

The **no** form of the command disables the overflow interval configuration.

Examples

The following example configures a database-overflow interval of 120 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# database-overflow-interval 120
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug access-list-log buffer

Configures or clears the ACL buffer.

Syntax

debug access-list-log buffer { **circular** | **linear** } **packet-count** *count-value*

debug access-list-log buffer clear

no debug access-list-log buffer

Parameters

circular
Specifies circular buffer type.

linear
Specifies linear buffer type.

packet-count *count-value*
Specifies a value from 64 through 2056.

clear
Clears the buffer contents.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Use the **no** form of this command to disable debugging.

Examples

The following example clears the buffer.

```
device# debug access-list-log buffer clear
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug arp packet buffer

Configures or clears the ARP-packet buffer.

Syntax

debug arp packet buffer all

no debug arp packet buffer all

debug arp packet buffer { **circular** | **linear** } **packet-count** *num-packets* [**vrf** *vrf-name*]

debug arp packet buffer clear [**vrf** *vrf-name*]

debug arp packet buffer interface { **ethernet** *slot* **/** *port* | **ve** *ve-id* } [**rx** | **tx**]

no debug arp packet buffer interface { **ethernet** *slot* **/** *port* | **ve** *ve-id* } [**rx** | **tx**]

Parameters

all
Specifies all ARP-packet buffers.

circular
Specifies circular buffer type.

linear
Specifies linear buffer type.

packet-count *num-packets*
Specifies a value from 64 through 2056.

clear
Clears the buffer contents.

vrf *vrf-name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

interface
Specifies an Ethernet or VE interface.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

port-channel *number*
(Not supported for the current version) Specifies a port-channel interface. The range is from 1 through 6144.

ve *ve-id*
Specifies a virtual ethernet (VE) interface.

rx
Specifies whether to capture only transmitted packets.

tx

Specifies whether to capture received packets.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

If neither **rx** nor **tx** are specified, both transmitted and received packets are captures.

To disable ARP packet capture on a specified interface, use the **no debug dhcp packet buffer interface** command.

To disable ARP packet capture on all interfaces, use the **no debug dhcp packet buffer all** command.

Examples

The following command enables ARP packet capture for transmitting data on Ethernet interface 0/5.

```
device# debug arp packet buffer interface ethernet 0/5 tx
```

The following command disables ARP packet capture on all interface.

```
device# no debug arp packet buffer all
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug dhcp packet buffer

Configures a buffer to capture DHCP packets.

Syntax

debug dhcp packet buffer [**all** | **circular** *packet count* | **clear** *vrf name* | **interface** *ethernet/port-channel* | **linear***packet count*]

Command Default

The buffer wraps around to overwrite earlier captures (circular).

Parameters

circular
Buffer wraps around to overwrite earlier captures.

linear
Buffer stops capture when the packet-count value is reached.

clear
Clears the packet buffer.

all
Captures DHCP packets on all interfaces.

interface
Represents a valid interface such as Ethernet or port channel.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

This command configures the capturing buffer behavior by allowing captures to wrap and overwrite earlier captures or stop capturing when a packet-count limit is reached. The current buffer content is cleared when the configuration changes.

Use the **no** form of this command to disable debugging.

Examples

The following example configures a buffer to capture 510 maximum packets in a circular fashion.

```
device# debug dhcp packet buffer circular packet-count 510
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug dot1x packet

Displays processing information related to IEEE 802.1X port-based access control.

Syntax

debug dot1x packet { **all** | **interface ethernet** *slot/port* } [**detail**] [**both** | **rx** | **tx**]

no debug dot1x packet { **all** | **interface ethernet** *slot/port* }

Parameters

all

Causes the display of information for all interfaces.

interface

Causes the display of information for a specific interface.

ethernet *slot/port*

Specifies an Ethernet interface in slot and port number format; when the device does not contain slots, the slot number must be 0.

detail

Causes the display of detailed information.

both

Causes the display of information about received and transmitted packets. By default, information about both received and transmitted packets is displayed.

rx

Causes the display of information about only received packets.

tx

Causes the display of information about only transmitted packets.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

The **no** form of the command disables the display of processing information related to IEEE 802.1X port-based access control.

Examples

The following example shows how to display detailed processing information related to IEEE 802.1X port-based access control for all interfaces.

```
device# debug dot1x packet all detail

2017/04/26-04:16:35.131863 [DOT1X]: [EAP-Request]: TX SA(609c.9f5a.251e) DA(0180.c200.0003) Port:
Ethernet 0/6 Type: Identity
```

The follow example shows how to disable the display of processing information related to IEEE 802.1X port-based access control for port 0/1.

```
device# no debug dot1x packet interface ethernet 0/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug ip bgp

Displays information related to the processing of BGP4, with a variety of options.

Syntax

debug ip bgp { **cli** | **dampening** | **events** | **general** | **graceful-restart** | **ip-prefix** *ip-addr/mask-len* | **ip-prefix-list** *name* | **keepalives** | **route-map** *name* | **route-selection** | **traces** | **updates** [**rx** | **tx**] } [**all-vrfs** | **vrf** *vrf-name*]

no debug ip bgp

Parameters

cli
Displays information about BGP CLI

dampening
Displays BGP4 dampening.

events
Displays all BGP4 events.

general
Displays BGP4 common events.

graceful-restart
Displays BGP graceful restart events.

ip-prefix
Displays information filtered by IP prefix.

ip-addr
IPv4 address in dotted-decimal notation.

mask-len
IPv4 mask length in CIDR notation.

ip-prefix-list
Displays information filtered by IP prefix list.

name
Name of IP prefix list.

keepalives
Displays BGP4 keepalives.

route-map
Displays configured route map tags.

name
Name of route map.

route-selection
Displays BGP4 route selection.

traces
Displays BGP traces.

updates
Displays BGP4 updates.

rx
Displays BGP4 received updates.

tx
Displays BGP4 transmitted updates

all-vrfs
Specifies all VRFs.

vrf
Specifies a VRF instance or all VRFs.

vrf-name
Specifies a VRF instance

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

If you want to see BGP4 keepalives for a specific neighbor, you must first specify the neighbor using the **debug ip bgp neighbor** command. Only keepalive traces for the specified neighbor will appear in the debugging message.

The **no** form of the command disables debugging.

Examples

The following example sets debugging on BGP4 events.

```
device# debug ip bgp events
```

The following example sets debugging on BGP4 graceful restart events.

```
device# debug ip bgp graceful-restart
```

The following example specifies that BGP4 keepalives for a specified neighbor appear in debugging messages.

```
device# debug ip bgp keepalive
device# debug ip bgp neighbor 10.1.1.1
```

The following example sets debugging on BGP4 events for VRF instance "red".

```
device# debug ip bgp events vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug ip bgp neighbor

Displays information related to the processing of BGP4 for a specific neighbor.

Syntax

debug ip bgp neighbor *ip-addr* [**all-vrfs** | **vrf** *vrf-name*]

no debug ip bgp neighbor *ip-addr* [**all-vrfs** | **vrf** *vrf-name*]

Parameters

ip-addr
IPv4 address in dotted-decimal notation.

all-vrfs
Specifies all VRFs.

vrf
Specifies a VRF instance or all VRFs.

vrf-name
Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

The **no** form of the command disables debugging.

History

Release version	Command history
18x.1.00	This command was introduced.

debug ip igmp

Enables or disables debugging for IGMP information.

Syntax

debug ip igmp { **all** | **errors** | **group** *A.B.C.D* | **packet** | **rx** | **tx** | **interface** *ethernet* | *port-channel tunnel* | **vlan** *vlan_id* }

no debug ip igmp

Parameters

all
Enables all debugs.

errors
Enables only error type debugs, such as memory allocation failures etc.

group *A.B.C.D*
Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses included in the multicast group.

packet
Enables debug for query/reports per the chosen option.

rx
Specifies only ingressing flow debugs to be captured in traces.

tx
Specifies only egressing packet flows to be captured in traces.

interface
Specifies the interface (ethernet, port-channel, tunnel) to be monitored.

vlan
Specifies the VLAN to me monitored.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

When debugging is enabled, all of the IGMP packets received and sent and IGMP-host related events are displayed.

Use the **no** form of this command to disable debugging.

History

Release version	Command history
18x.1.00	This command was introduced.

debug ip pim

Enables debugging for IP Protocol Independent Multicast.

Syntax

debug ip pim { **add-del-oif** | **bootstrap** | **group** | **join-prune** | **nbr-change** | **packets** | **parent** | **regproc** | **route-change** | **rp** | **source** | **state** | **all** }

no debug ip pim all

Command Default

All flags are disabled.

Parameters

add-del-oif
Controls the OIF change flag.

bootstrap
Controls the bootstrap processing flag.

group
Controls the processing for a group flag.

join-prune
Controls the Join/Prune processing flag.

nbr-change
Controls the neighbor changes flag.

packets
Controls the packet processing flag.

parent
Controls the parent change processing flag.

regproc
Controls the register processing flag.

route-change
Controls the route changes flag.

rp
Controls the Rendezvous Point (RP) processing flag.

source
Controls the processing for a source flag.

state
Controls the state processing flag.

all
Controls all of the states.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Use the **no debug ip pim all** command to disable debugging.

History

Release version	Command history
18x.1.00	This command was introduced.

debug ipv6 bgp

Displays debug information related to BGP processing for IPv6 prefix lists.

Syntax

debug ipv6 bgp ipv6-prefix *ipv6-address /mask* [**all-vrfs** | **vrf** *vrf-name*]

debug ipv6 bgp ipv6-prefix *name* [**all-vrfs** | **vrf** *vrf-name*]

debug ipv6 bgp ipv6-prefix-list *name* [**all-vrfs** | **vrf** *vrf-name*]

no debug ipv6 bgp ipv6-prefix *ipv6-address /mask* [**all-vrfs** | **vrf** *vrf-name*]

no debug ipv6 bgp ipv6-prefix *name* [**all-vrfs** | **vrf** *vrf-name*]

no debug ipv6 bgp ipv6-prefix-list *name* [**all-vrfs** | **vrf** *vrf-name*]

Parameters

ipv6-address /mask
Specifies an IPv6 address and network mask.

all-vrfs
Specifies all VRFs.

vrf
Specifies a VRF instance or all VRFs.

vrf-name
Specifies a VRF instance

name
Specifies a prefix list name.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Use the **no** form of this command to disable debugging.

Examples

This example enables debugging for IPv6 prefix list "myv6list" for VRF instance "red".

```
device# debug ipv6 bgp ipv6-prefix-list myv6list vrf red
```

This example enables debugging for a specified IPv6 address for all VRFs.

```
device# debug ipv6 bgp ipv6-prefix 2001::/16 all-vrfs
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug ipv6 bgp neighbor

Displays debug information related to BGP processing for a specified neighbor.

Syntax

debug ipv6 bgp neighbor *ipv6-addr* [**all-vrfs** | **vrf** *vrf-name*]

no debug ipv6 bgp neighbor *ipv6-addr* [**all-vrfs** | **vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a neighbor.

all-vrfs
Specifies all VRFs.

vrf
Specifies a VRF instance or all VRFs.

vrf-name
Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

The **no** form of the command disables debugging.

Examples

The following example sets debugging for a neighbor.

```
device# debug ipv6 bgp neighbor 2000::1
```

The following example specifies that BGP keepalives for a specified neighbor appear in debugging messages.

```
device# debug ip bgp keepalive
device# debug ipv6 bgp neighbor 2001::1
```

The following example sets debugging for a neighbor for VRF instance "red".

```
device# debug ipv6 bgp neighbor 2000::1 vrf red
```

The following example sets debugging for a neighbor for all VRFs.

```
device# debug ipv6 bgp neighbor 2000::1 all-vrfs
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug lacp

Enables or disables debugging for the Link Aggregation Control Protocol (LACP).

Syntax

debug lacp { **all** | **cli** | **event** | **ha** | **pdu** [**rx** { **all** | **interface ethernet** *slot/port* | **tx** { **all** | **sync** | **timer** | **trace level** *number* }

no debug lacp

Command Default

LACP debugging is disabled.

Parameters

all
Turns on all debugging.

cli
Turns on command line interface debugging.

event
Turns on event debugging.

ha
Echo HA events to the console.

pdu
Echo PDU content to the console.

rx all
Turns on debugging for received LACP packets on all interfaces.

rx interface
Turns on debugging for received LACP packets on the specified interface.

interface
Specifies the interface to be monitored.

ethernet
Represents a valid, physical Ethernet interface.

slot
Specifies a valid slot number. The only valid value is 0.

port
Specifies a valid port number.

tx all
Turns on debugging for transmitted LACP packets on all interfaces.

tx interface
Turns on debugging for transmitted LACP packets on the specified interface.

sync
Echo synchronization to consoles.

timer
Echo timer expiration to console.

trace level *number*
Specifies the trace level number. Valid values range from 1 through 7.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **terminal monitor** to display debugging outputs on a particular cmsh session.

Enter **no debug lacp** to disable LACP debugging.

Examples

To enable debugging of LACP PDUs for transmitted and received packets on all interfaces:

```
device# debug lacp pdu tx all

device # debug lacp pdu rx all

device# show debug lacp
LACP rx debugging is on
LACP tx debugging is on
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug lldp dump

Dumps debugging information for the Link Layer Discovery Protocol (LLDP) to the console.

Syntax

debug lldp dump { **all** | [**ethernet** *slot/port*] [**both**]] | [**detail** [**both** | **rx** | **tx**]]

Command Default

LLDP debugging is disabled.

Parameters

all

Dumps all information to the console.

ethernet

Represents a valid, physical Ethernet port.

slot

Specifies a valid slot number. The only valid value is 0.

port

Specifies a valid port number.

both

Turns on debugging for both transmit and receive packets.

detail

Turns on debugging with detailed information.

both

Turns on detailed debugging for both transmit and receive packets.

rx

Turns on detailed debugging for only received LLDP packets.

tx

Turns on detailed debugging for only transmitted LLDP packets.

Modes

Privileged EXEC mode

Examples

Typical use of this command.

```
device# debug lldp dump all
LLDP Interface Debug Information for 0/2
Admin Status:  RX_TX
Associated Profile:
Link-level FCoE Priority: 0x08 (Configured: No)
Link-level iSCSI Priority: 0x10 (Configured: No)
Link Properties:
    CEE Incapable
    FCoE LLS not Ready
    FCF-Forward Disabled
Sending TLVs:
    CHASSIS_ID: 0x50eb1a173ff1 (MAC)
    PORT_ID: 0/2 (IF Name)
    TTL: Hold (4) x Interval (30)
    SYSTEM_NAME
    IEEE_DCBX
    DCBX_FCOE_APP
    DCBX_FCOE_LOGICAL_LINK
    Configured FCoE App
    Configured FCoE Link
    DCBX_CTRL
<truncated>
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug lldp packet

Enables or disables debugging for the Link Layer Discovery Protocol (LLDP).

Syntax

debug lldp packet { **all** | [**ethernet** *slot/port*] [**both**]] | [**detail** [**both** | **rx** | **tx**]]

no debug lldp packet { **all** | **interface ethernet** *slot/port* }

Command Default

LLDP debugging is disabled.

Parameters

all

Turns on LLDP packet debugging on all interfaces.

ethernet

Represents a valid, physical Ethernet port.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

both

Turns on debugging for both transmit and receive packets.

detail

Turns on debugging with detailed information.

both

Turns on detailed debugging for both transmit and receive packets.

rx

Turns on detailed debugging for only received LLDP packets.

tx

Turns on detailed debugging for only transmitted LLDP packets.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **terminal monitor** to display debugging outputs on a particular cmsh session.

Enter **no debug lldp packet** to disable LLDP debugging.

Examples

To enable debugging of LLDP for both received and transmitted packets on the 10-gigabit Ethernet interface 0/1:

```
device# debug lldp packet interface ethernet 0/1 both

device# show debug lldp

LLDP debugging status:
Interface 0/1    : Transmit Receive
```

History

Release version	Command history
18x.1.00	This command was introduced.

debug spanning-tree

Enables debugging for the Spanning Tree Protocol (STP).

Syntax

debug spanning-tree { **all** | **bpdu** [**rx** | **tx** [**all** | [**interface** { **ethernet** *slot/port* | **port-channel** *number* }

no debug spanning-tree { **all** | **bpdu** [**rx** | **tx** [**all** | [**interface** { **ethernet** *slot/port* | **port-channel** *number* }

Command Default

STP debugging is disabled.

Parameters

all
Turns on spanning tree packet debugging on all interfaces.

bpdu
Turns on Bridge Protocol Data Unit debugging.

rx
Turns on debugging for only received spanning-tree packets.

tx
Turns on debugging for only transmitted spanning-tree packets.

interface
Specifies an interface.

ethernet
Specifies an Ethernet interface.

slot
Specifies a valid slot number. Must be 0 if the switch does not contain slots.

port
Specifies a valid port number.

port-channel *number*
Specifies a port-channel. The number of available channels ranges from 1 through 6144.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Enter **terminal monitor** to display debugging outputs.

Enter **no debug spanning-tree** to disable debugging.

Examples

To enable debugging of spanning-tree for both Rx and Tx on Ethernet interface 0/1:

```
device# debug spanning-tree bpdu rx interface ethernet 0/1

device# debug spanning-tree bpdu tx interface ethernet 0/1

device# show debug spanning-tree

MSTP debugging status:
Spanning-tree rx debugging is off
Eth 0/1 rx is on
Spanning-tree tx debugging is off
Eth 0/1 tx is on
```

History

Release version	Command history
18x.1.00	This command was introduced.

default-information-originate (BGP)

Configures the device to originate and advertise a default BGP route.

Syntax

default-information-originate

no default-information-originate

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following example originates and advertises a default BGP4 route.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# default-information-originate
```

The following example originates and advertises a default BGP4+ route for VRF "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# default-information-originate
```

History

Release version	Command history
18x.1.00	This command was introduced.

default-information-originate (OSPFv2)

Controls distribution of default information to an OSPFv2 device.

Syntax

default-information-originate [**always**] [**metric** *metric*] [**metric-type** { **type1** | **type2** }] [**route-map** *name*]

no default-information-originate

Command Default

The default route is not advertised into the OSPFv2 domain.

Parameters

always

Always advertises the default route. If the route table manager does not have a default route, the router advertises the route as pointing to itself.

metric *metric*

specifies the cost for reaching the rest of the world through this route. If you omit this parameter and do not specify a value using the *default-metric* router configuration command, a default metric value of 1 is used. Valid values range from 1 through 65535. The default is 10.

metric-type

Specifies how the cost of a neighbor metric is determined. The default is **type1**. However, this default can be changed with the **metric-type** command.

type1

Type 1 external route.

type2

Type 1 external route,

route-map *name*

Specifies that the default route is generated if the route map is satisfied. This parameter overrides other options. If the **set metric** and **set metric-type** commands are specified in the route-map, the command-line values of metric and metric-type if specified, are “ignored” for clarification.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

This configuration provides criteria for the redistribution of any default routes found in the route table manager (RTM),whether static or learned from another protocol, to its neighbors.

The corresponding route-map should be created before configuring the **route-map** option, along with the **default-information-originate** command. If the corresponding route-map is not created beforehand, an error message is displayed stating that the route-map must be created.

The route-map option cannot be used with a non-default address in the match conditions. The default route LSA is not generated if a default route is not present in the routing table and a **match ip address** condition for an existing non-default route is configured in the route-map. The **match ip address** command in the route-map is a no-op operation for the default information originate command.

The **no** form of the command disables default route origination.

Examples

The following example creates and advertises a default route with a metric of 30 and a type 1 external route.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-information-originate metric 30 metric-type type1
```

History

Release version	Command history
18x.1.00	This command was introduced.

default-information-originate (OSPFv3)

Controls distribution of default information to an OSPFv3 device.

Syntax

default-information-originate [**always**] [**metric** *metric*] [**metric-type** { **type1** | **type2** }]

no default-information-originate

Command Default

The default route is not advertised into the OSPFv3 domain.

Parameters

always

Always advertises the default route. If the route table manager (RTM) does not have a default route, the router advertises the route as pointing to itself.

metric *metric*

Used for generating the default route, this parameter specifies the cost for reaching the rest of the world through this route. If you omit this parameter, the value of the **default-metric** command is used for the route. Valid values range from 1 through 65535.

metric-type

Specifies the external link type associated with the default route advertised into the OSPF routing domain.

type1

The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.
The default is **type1**.

type2

The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

This configuration provides criteria for the redistribution of any default routes found in the RTM (whether static or learned from another protocol) to its neighbors.

The **no** form of the command disables default route origination.

Examples

The following example specifies a metric of 20 for the default route redistributed into the OSPFv3 routing domain and an external metric type of Type 2.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# default-information-originate metric 20 metric-type
type2
```

History

Release version	Command history
18x.1.00	This command was introduced.

default-ipv6-gateway

Configures the IPv6 address of the default gateway on a VLAN.

Syntax

default-ipv6-gateway *ipv6-address* [*metric*]

no default-ipv6-gateway

Parameters

ipv6-address
IPv6 address of the default gateway.

metric
A decimal value from 1 through 5.

Modes

VLAN configuration mode

Usage Guidelines

A device should have a default gateway, for the following reasons:

- Although IPv6 discovers neighbors and routes dynamically, in some cases Router Advertisement (RA) and Router Solicitation (RS) operations are disabled and a default gateway is required to send traffic. RA and RS are not suppressed if a default gateway is confifured.
- Management devices (for example, TFTP servers, Telnet or SSH clients) are not members of the same subnet as the management IPv6 address.

If a management VLAN is not configured, the device can have only one IPv6 default gateway in the global configuration.

If a management VLAN is configured, the device can have a maximum of 5 IPv6 default gateways, with an optional metric (1 through 5), under the management VLAN. Multiple gateways can have the same metric value.

Configured gateway addresses and the default gateway address must be in same subnet.

The best default gateway is first chosen as the device whose neighbors are reachable (in the REACH state), in the sequence of metric values. Otherwise, the gateway with the highest priority (the lowest metric value) is chosen.

If a static default gateway is configured, that gateway takes precedence over the best default gateway configured by means of RA. If the static default-gateway configuration is removed, the best default gateway learned by RA is restored.

Use the **no** form of the command to remove the IPv6 address and disable the default gateway.

Selection of the best default router among configured IPv6 routers occurs under the following conditions:

- Disabling an interface
- Processing of an NA message receipt
- Adding or deleting an IPv6 neighbor to or from the neighbor list
- Configuring the IPv6 static default gateway by means of the CLI

The process of resolving the link layer for the IPv6 default gateway by sending NS occurs during the following conditions:

- Configuration of the default gateway configured by means of the CLI
- Addition or deletion of a management VLAN configuration

Examples

The following example configures the maximum of 5 IPv6 default gateways with the management VLAN configuration, and specifies metrics for each.

```
device# configure terminal
device(config)# vlan 66
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:129 3
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:129 2
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:130 2
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:131 1
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:132 5
```

Use the **show ipv6** command to confirm the configuration and view the best default gateway (router).

```
device(config)# show ipv6
Global Settings
  IPv6 is enabled
  Link-local address(es):
    fe80::768e:f8ff:fef9:6d80 [Preferred]
  Global unicast address(es):
    2620:100:c:fe23:768e:f8ff:fef9:6d80 [Preferred],  subnet is 2620:100:c:fe23::/64
  Joined group address(es):
    ff02::1:fff9:6d80
    ff02::1
  Best Default Router : 2620:100:c:fe23:10:37:65:129 PMTUS : 0
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 3
  ND reachable time is 30000 miliseconds
  ND retransmit interval is 1000 miliseconds
  Current Hop Limit is 64
  Hosts use stateless autoconfig for addresses
  No Inbound Access List Set
  No Outbound Access List Set
  No IPv6 Domain Name Set
  No IPv6 DNS Server Address set
```

History

Release version	Command history
18x.1.00	This command was introduced.

default-local-preference

Enables setting of a local preference value to indicate a degree of preference for a route relative to that of other routes.

Syntax

default-local-preference *num*

no default-local-preference

Parameters

num

Local preference value. Range is from 0 through 65535. The default is 100.

Modes

BGP configuration mode

Usage Guidelines

Local preference indicates a degree of preference for a route relative to that of other routes. BGP4 neighbors can send the local preference value as an attribute of a route in an UPDATE message.

Examples

The following example sets the local preference value to 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# default-local-preference 200
```

History

Release version	Command history
18x.1.00	This command was introduced.

default-metric (BGP)

Changes the default metric used for redistribution.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 1.

Parameters

value

Metric value. Range is from 0 through 4294967295.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following example changes the default metric used for redistribution to 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# default-metric 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

default-metric (OSPF)

Sets the default metric value for the OSPFv2 or OSPFv3 routing protocol.

Syntax

default-metric *metric*

no default-metric

Parameters

metric

OSPF routing protocol metric value. Valid values range from 1 through 65535. The default is 10.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

This command overwrites any incompatible metrics that may exist when OSPFv2 or OSPFv3 redistributes routes. Therefore, setting the default metric ensures that neighbors will use correct cost and router computation.

The **no** form of the command restores the default setting.

Examples

The following example sets the default metric to 20 for OSPF.

```
device# configure terminal
device(config)# rrouter ospf
device(config-router-ospf-vrf-default-vrf)# default-metric 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

default-passive-interface

Marks all OSPFv2 and OSPFv3 interfaces passive by default.

Syntax

default-passive-interface

no default-passive-interface

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

When you configure the interfaces as passive, the interfaces drop all the OSPFv2 and OSPFv3 control packets.

You can use the **ip ospf active** and **ip ospf passive** commands in interface subconfiguration mode to change active/passive state on specific OSPFv2 interfaces. You can use the **ipv6 ospf active** and **ipv6 ospf passive** commands in interface subconfiguration mode to change the active and passive state on specific OSPFv3 interfaces.

The **no** form of the command disables the passive state.

Examples

The following example marks all OSPFv2 interfaces as passive.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-passive-interface
```

History

Release version	Command history
18x.1.00	This command was introduced.

delay

For an implementation of an event-handler profile, specifies a delay from when a trigger is received until execution of the event-handler action.

Syntax

delay *seconds*

no delay

Command Default

There is no delay from when a trigger is received until execution of the event-handler action.

Parameters

seconds

Specifies the number of seconds from when a trigger is received until the execution of the specified action begins. Valid values are 0 or a positive integer.

Modes

Event-handler activation mode

Usage Guidelines

The **no** form of this command resets the **delay** setting to the default 0 seconds.

Examples

The following example specifies a delay of 60 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# delay 60
```

The following example resets **delay** to the default value of 0 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no delay
```

History

Release version	Command history
18x.1.00	This command was introduced.

delay-link-event

Configures the port transition hold timer to set a delay in the sending of port up or down port events, or both, to Layer 2 protocols.

Syntax

delay-link-event *multiple-iteration* { **down** | **up** | **both** }

no delay-link-event

Command Default

The sending of an up or down port event is not delayed.

Parameters

multiple-iteration
Specifies the number of times that the polling iteration occurs. Enter an integer from 1 to 200. The polling iteration is 50 ms. The delay time is the *multiple-iteration* times 50 ms.

both
Sets the delay for the port down and up events.

down
Sets the delay for the port down event.

up
Sets the delay for the port up event.

Modes

Interface Ethernet configuration mode.

Usage Guidelines

Use the **no** form of the command to remove the delay from the port events on the interface.

While link down events are reported immediately in the Syslog, their effect on higher level protocols such as OSPF is delayed according to how the hold timer is configured. When configured, the timer affects the physical link events. However, the resulting logical link events are also delayed.

NOTE
All LAG member ports must have the same delayed-link-event configuration.

NOTE
The delayed-link-event configuration is applicable only on a physical interface. It is not valid on a VLAN, VE, LAG, or loopback interfaces.

NOTE
The port transition hold timer does not take effect when the interface is administratively shut down.

Examples

The following example shows the steps in the previous configuration.

```
device# configure terminal
device(config)# interface ethernet 4/2
device(conf-if-eth-4/2)# delay-link-event 2 down
```

History

Release version	Command history
18x.1.00	This command was introduced.

delete

Deletes a user-generated file from the flash memory.

Syntax

delete *file*

Parameters

file

The name of the file to be deleted.

Modes

Privileged EXEC mode

Usage Guidelines

The delete operation is final; there is no mechanism to restore the file.

System configuration files cannot be deleted. If you try to delete a system configuration file, an appropriate message is displayed.

Examples

To delete a user-generated copy of a configuration file:

```
device# delete myconfig

% Warning: File will be deleted (from flash:)!
Continue?(y/n): y
```

History

Release version	Command history
18x.1.00	This command was introduced.

delete-packet

Configures the logging or monitoring interval for all Traffic Management (TM) deleted packets on the SLX-OS device.

Syntax

delete-packet { **logging-interval** *minutes* } | { **threshold** *deleted-packets* }

no delete-packet logging-interval | **threshold**

Command Default

The logging interval is 60 minutes.

The default threshold is zero (0) deleted packets.

Parameters

logging-interval *minutes*
Specifies the logging interval in minutes. Enter an integer from from 10 to 2880.

threshold *deleted-packets*
Specifies the threshold limit for all deleted packets of the TM device. Enter a value from 0 to 10000. The value of 0 disables the monitoring of the all TM deleted packets.

Modes

System monitor TM configuration mode

Usage Guidelines

Use the **no** version of this command to reset the default interval or threshold values.

A RASlog message for the TM device statistics is generated within the logging interval similar to the following format:

```
M1 | Active, WARNING, SLX, TM threshold, Head deleted packets 34462
on device 3.1.1.
```

Examples

The following example configures the logging interval to 120 minutes.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# delete-packet logging-interval 120
```

The following example configures the threshold to 50 deleted packets.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# delete-packet threshold 50
```

History

Release version	Command history
18x.1.00	This command was introduced.

deploy

Deploys the MCT cluster, or cluster client.

Syntax

deploy

no deploy

Modes

Cluster configuration mode

Cluster client configuration mode

Usage Guidelines

Before deploying a cluster, the cluster client must be configured.

Before deploying a cluster client, the client interface and ESI settings must be configured under the client configuration.

The client will not operate in MCT mode unless the remote client is also deployed.

The **no** form of the command undeploys the cluster or cluster client.

When the client is undeployed, all MAC addresses are removed locally and a withdraw message is sent to the MCT peer to remove all associated client MAC addresses.

Examples

The following example shows the deployment of a cluster.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# deploy
```

The following example shows the deployment of a cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# deploy
```

History

Release version	Command history
18x.1.00	This command was introduced.

description (BD)

Specify a string that contains the description for a bridge-domain or multiple bridge-domains.

Syntax

description [*description-string*]

no description [*description-string*]

Parameters

description-string

Specifies the description in a string format. The space character between the **description** keyword and the *description-string* is allowed.

Modes

Global bridge-domain configuration mode.

Usage Guidelines

The **no description** of the command removes the description specified for a bridge-domain.

The **show bridge-domain** command displays an extra field in the output displaying the description of the bridge-domain.

Examples

The following example shows how to specify a description for bridge-domain 10.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# description myBD10
```

History

Release version	Command history
18x.1.00	This command was introduced.

description (event handler)

Defines a description for an event-handler profile.

Syntax

description *description-text*

no description

Command Default

No description is defined.

Parameters

description-text

Characters describing the event-handler profile. The string can be 1 through 128 ASCII characters in length. Do not use the ? character. If you need to use ! or \, precede each with \.

Modes

Event-handler configuration mode

Usage Guidelines

An event-handler profile supports only one description.

To delete a description, use the **no** form of this command.

To change a description, you do not need to first delete the existing description. Just create a new description.

Examples

The following example defines a description for eventHandler1.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)# description This is a sample description.
```

History

Release version	Command history
18x.1.00	This command was introduced.

description (interfaces)

Specify a string that contains the description of a specified interface.

Syntax

description *line*

Parameters

line

Specifies characters describing the interface. The string must be between 1 and 63 ASCII characters in length.

Modes

Interface subtype configuration mode

Examples

To set the string describing internal Ethernet interface 3/2:

```
device# configure terminal
device(config)# interface ethernet 3/2
device(conf-if-eth-3/2)# description converged_101
```

History

Release version	Command history
18x.1.00	This command was introduced.

description (LLDP)

Specifies a string that contains the LLDP description.

Syntax

description *string*

no description

Parameters

string

Characters describing LLDP. The string must be between 1 and 50 ASCII characters in length.

Modes

Protocol LLDP and profile configuration modes

Usage Guidelines

Enter **no description** to remove the LLDP description.

The LLDP description can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

Examples

To set the strings describing LLDP:

```
device(conf-lldp)# description Extreme-LLDP
```

To set the strings describing LLDP for a specific LLDP profile, test2, enter the following:

```
device(conf-lldp)# profile test1
device(config-profile-test1)# description mytest1
device(config-profile-test1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

description (STP)

Describes an xSTP configuration.

Syntax

description *description*

no description

Parameters

description

Characters describing the xSTP configuration. The string must be between 1 and 64 ASCII characters in length.

Modes

xSTP configuration mode

Usage Guidelines

Enter **no description** to remove the description.

Examples

To specify the bridge priority:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# description STP-S1

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# description RSTP-S1

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# description MSTP-S1
```

History

Release version	Command history
18x.1.00	This command was introduced.

description (VRRP)

Describes a Virtual Router Redundancy Protocol extended (VRRP-E) interface.

Syntax

description *description*

no description

Parameters

description

Characters describing the VRRP-E interface. The string must be between 1 and 64 ASCII characters in length.

Modes

Virtual-router-group configuration mode

Usage Guidelines

Enter **no description** to remove the description.

Examples

To describe the VRRP-E group 10 interface:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 10
device(config-vrrp-extended-group-10)# description vrrpe_group_10
```

History

Release version	Command history
18x.1.00	This command was introduced.

designated-forwarder-hold-time

Configures the time in seconds to wait before electing a designated forwarder.

Syntax

designated-forwarder-hold-time *seconds*

designated-forwarder-hold-time

Command Default

The default setting is three seconds.

Parameters

seconds

Specifies the hold time in seconds. Enter an integer from 1 to 60.

Modes

Cluster configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default setting of three seconds.

The designated forwarder is a PE in a set of multi-homing PEs connected to the same Ethernet segment that is responsible for sending BUM traffic to a client for a particular VLAN ID on an Ethernet segment.

DF election is not triggered unless at least one remote CCEP is configured. When a CCEP goes up or down, DF election is triggered as soon as the Ethernet route acknowledgment from remote peer is received.

When a client is deployed locally or remotely, or the BGP session comes up, the DF timer does not start and DF election is not performed until the timer expired.

Examples

The following example configures a 20-second hold time for DF election.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# designated-forwarder-hold-time 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

destination

Configures the destination address for the tunnel interface.

Syntax

destination *ip-address*

no destination *ip-address*

Command Default

No tunnel interface destination is configured.

Parameters

ip-address

Specifies the IPv4 address.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no tunnel destination** command to remove the destination configuration.

You must ensure that a route to the tunnel destination exists on the tunnel source device and create a static route if necessary.

Examples

This example configures the IP address 10.1.2.3 as the destination address.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# destination 10.1.2.3
```

History

Release version	Command history
18x.1.00	This command was introduced.

dhcp ztp cancel

The Zero Touch Provisioning (ZTP) session indefinitely retries detecting the DHCP server to establish a network connection for firmware download. Once canceled, the ZTP session stops retrying.

Syntax

dhcp ztp cancel

Modes

Privileged EXEC mode

Usage Guidelines

Once canceled, the ZTP session stops retry, irrespective of whether the process succeeds or fails. If firmware download completes successfully, the device returns to the normal mode. The following limitations apply:

- If firmware download has not started, you will need to reboot the switch manually to bring the switch back to normal mode.
- If firmware download has already started, you must wait for firmware download to complete before running any other CLI, power cycling the switch, starting a new firmware download, or starting a new ZTP session.
- If firmware download completes and the switch fails to reboot, you must reboot the switch manually to bring the switch back to normal mode.

Examples

The following example cancels the ZTP retry.

```
device# dhcp ztp cancel
Warning: This command will terminate the existing ZTP session
Do you want to continue? [y/n] y
```

You can confirm that ZTP is canceled by running the **dhcp ztp cancel** command again. The output confirms that ZTP is disabled.

```
device# dhcp ztp cancel
ZTP is not enabled.
```

History

Release version	Command history
18x.1.00	This command was introduced.

dhcp ztp log

Displays the Zero Touch Provisioning progress log.

Syntax

dhcp ztp log

Modes

Privileged EXEC mode

Usage Guidelines

The progress log displays if Zero Touch Provisioning is enabled.

Examples

The following example shows the ZTP progress log.

```
device# dhcp ztp log
ZTP, Wed Jun 29 17:32:36 2016, ========== ZTP start ==========
ZTP, Wed Jun 29 17:32:36 2016, disable raslog
ZTP, Wed Jun 29 17:32:36 2016, CLI is ready
ZTP, Wed Jun 29 17:33:11 2016, inband ports are enabled
ZTP, Wed Jun 29 17:33:11 2016, serial number = EXH3343L014
ZTP, Wed Jun 29 17:33:11 2016, model name = SLX9140
ZTP, Wed Jun 29 17:33:11 2016, use inband interfaces only
ZTP, Wed Jun 29 17:33:13 2016, get link down on all the interfaces
ZTP, Wed Jun 29 17:33:13 2016, retry in 10 seconds
ZTP, Wed Jun 29 17:33:23 2016, inband ports are enabled
ZTP, Wed Jun 29 17:33:24 2016, serial number = EXH3343L014
ZTP, Wed Jun 29 17:33:24 2016, model name = SLX9140
ZTP, Wed Jun 29 17:33:24 2016, use inband interfaces only
ZTP, Wed Jun 29 17:33:24 2016, get link down on all the interfaces
ZTP, Wed Jun 29 17:33:24 2016, retry in 10 seconds
ZTP, Wed Jun 29 17:33:34 2016, inband ports are enabled
ZTP, Wed Jun 29 17:33:34 2016, serial number = EXH3343L014
ZTP, Wed Jun 29 17:33:34 2016, model name = SLX9140
ZTP, Wed Jun 29 17:33:34 2016, use inband interfaces only
ZTP, Wed Jun 29 17:33:35 2016, checking inband interfaces link status
ZTP, Wed Jun 29 17:34:25 2016, find link up on intefaces: Eth0.6 Eth0.8
ZTP, Wed Jun 29 17:34:25 2016, start dhcp process on interfaces: Eth0.6 Eth0.8
ZTP, Wed Jun 29 17:34:34 2016, interface Eth0.8 receives dhcp response
ZTP, Wed Jun 29 17:34:34 2016, config ip address 192.169.0.147/24 on interface Eth0.8
ZTP, Wed Jun 29 17:34:39 2016, ping ftp server 192.169.0.2
ZTP, Wed Jun 29 17:34:40 2016, ping succeed
ZTP, Wed Jun 29 17:34:41 2016, download ZTP config file from ftp://192.169.0.2/config/ztp.cfg
ZTP, Wed Jun 29 17:34:41 2016, receive ZTP configuration file [ztp.cfg]
ZTP, Wed Jun 29 17:34:41 2016, interface Eth0.8 connectivity test pass
ZTP, Wed Jun 29 17:34:41 2016, download script file [ztp.py]
ZTP, Wed Jun 29 17:34:41 2016, ZTP configuration sanity check pass
ZTP, Wed Jun 29 17:38:22 2016, ========== ZTP continue ==========
ZTP, Wed Jun 29 17:38:22 2016, disable raslog
ZTP, Wed Jun 29 17:38:22 2016, CLI is ready
ZTP, Wed Jun 29 17:38:58 2016, running configuration script [ztp.py]
ZTP, Wed Jun 29 17:39:25 2016, commit configuration
ZTP, Wed Jun 29 17:39:25 2016, ZTP succeed
ZTP, Wed Jun 29 17:39:25 2016, enable raslog
ZTP, Wed Jun 29 17:39:25 2016, ========== ZTP completed ==========
```

History

Release version	Command history
18x.1.00	This command was introduced.

dir

Lists the contents of the device flash memory.

Syntax

dir

Modes

Privileged EXEC mode

Examples

The following example lists the contents of the flash memory.

```
device# dir
total 572
drwxr-xr-x 2  251 1011   4096 Jun  5 07:08 .
drwxr-xr-x 3  251 1011   4096 Mar 11 00:00 ..
-rw-r--r-- 1 root sys     410 Jun  3 00:56 defaultconfig.standalone
-rw-r--r-- 1 root sys     695 Jun  3 00:56 defaultconfig.cluster
-rw-r--r-- 1 root root 185650 Jun  5 09:38 startup-config
```

History

Release version	Command history
18x.1.00	This command was introduced.

discard-packet

Configures the logging or monitoring interval for all Traffic Management (TM) discarded packets on the SLX-OS device.

Syntax

discard-packet { **logging-interval** *minutes* } | { **threshold** *discarded-packets* }

no discard-packet logging-interval | **threshold**

Command Default

The logging interval is 60 minutes.

The default threshold is zero (0) discarded packets.

Parameters

logging-interval *minutes*
Specifies the logging interval in minutes. Enter an integer from from 10 to 2880.

threshold *discarded-packets*
Specifies the threshold limit for all discarded packets of the TM device. Enter a value from 0 to 10000. The value of 0 disables the monitoring of the all TM device packets.

Modes

System monitor TM configuration mode

Usage Guidelines

Use the **no** version of this command to reset the default interval or threshold values.

A RASlog message for the TM device statistics is generated within the logging interval. The message consists of the time stamp, the number of discarded packets, and ingress slot, tower and core, similar to the following example:

```
device# show logging raslog reverse count 10
2017/01/05-10:56:58, [SYSD-1005], 788, M2 | Active | DCE, WARNING, SLX,  TM threshold, Tail discarded
packets 20734462 on device 3.1.1.
```

Examples

The following example configures the logging interval to 120 minutes.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# discard-packet logging-interval 120
```

The following example configures the threshold to 50 discarded packets.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# discard-packet threshold 50
```

History

Release version	Command history
18x.1.00	This command was introduced.

discard-voq-packet

Configures the logging interval or threshold for all Virtual Output Queue (VOQ) discarded packets.

Syntax

discard-voq-packet { **logging-interval** *minutes* } | { **threshold** *discarded-packets* }

no discard-voq-packet logging-interval | **threshold**

Command Default

The logging interval is 60 minutes.

The default threshold is zero (0) discarded packets.

Parameters

logging-interval *minutes*
Specifies the logging interval in minutes. Enter an integer from from 10 to 2880.

threshold *discarded-packets*
Specifies the threshold limit for all VOQ discarded packets. Enter a value from 0 to 10000. The value of 0 disables the monitoring of the all VOQ packets.

Modes

System monitor TM configuration mode

Usage Guidelines

Use the **no** version of this command to reset the default interval or threshold values.

A RASlog message for the TM VOQ statistics is generated within the logging interval. The message consists of the time stamp, destination slot and port, priority, and ingress slot, tower and core, similar to the following example.

```
device# show logging raslog reverse count 100 | inc SYSD-1003
2017/01/05-11:03:59, [SYSD-1003], 793, M2 | Active | DCE, WARNING, SLX,  TM threshold
2017/01/05-11:00:34, Discarded packets 930587727, interface 3/2 prio 0 on device 3.1.0
```

The slot and port in the message determines the destination port that is congested at the ingress slot, tower, and core.

Examples

The following example configures the logging interval to 120 minutes.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# discard-voq-packet logging-interval 120
```

The following example configures the threshold to 50 discarded packets.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# discard-voq-packet threshold 50
```

History

Release version	Command history
18x.1.00	This command was introduced.

distance (BGP)

Changes the default administrative distances for eBGP, iBGP, and local BGP.

Syntax

distance *external-distance internal-distance local-distance*

no distance

Parameters

external-distance
eBGP distance. Range is from 1 through 255.

internal-distance
iBGP distance. Range is from 1 through 255.

local-distance
Local BGP4 and BGP4+ distance. Range is from 1 through 255.

Modes

BGP configuration mode

Usage Guidelines

To select one route over another according to the source of the route information, the device can use the administrative distances assigned to the sources. The administrative distance is a protocol-independent metric that IP devices use to compare routes from different sources. Lower administrative distances are preferred over higher ones.

Examples

The following example configures the device to change the administrative distance.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# distance 100 150 200
```

History

Release version	Command history
18x.1.00	This command was introduced.

distance (OSPF)

Configures an administrative distance value for OSPFv2 and OSPFv3 routes.

Syntax

distance { **external** | **inter-area** | **intra-area** } *distance*

no distance

Command Default

The administrative distance value for OSPFv2 and OSPFv3 routes is 110.

Parameters

external
Sets the distance for routes learned by redistribution from other routing domains.

inter-area
Sets the distance for all routes from one area to another area.

intra-area
Sets the distance for all routes within an area.

distance
Administrative distance value assigned to OSPF routes. Valid values range from 1 through 255. The default is 110.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

You can configure a unique administrative distance for each type of OSPF route.

The distances you specify influence the choice of routes when the device has multiple routes from different protocols for the same network. The device prefers the route with the lower administrative distance. However, an OSPFv2 or OSPFv3 intra-area route is always preferred over an OSPFv2 or OSPFv3 inter-area route, even if the intra-area route's distance is greater than the inter-area route's distance.

The **no** form of the commands reverts to the default setting.

Examples

The following example sets the distance value for all external routes to 125.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distance external 125
```

The following example sets the distance value for intra-area routes to 80.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distance intra-area 80
```

The following example sets the distance value for inter-area routes to 90.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# distance inter-area 90
```

History

Release version	Command history
18x.1.00	This command was introduced.

distribute-list prefix-list (OSPFv3)

Applies a prefix list to OSPF for IPv6 routing updates. Only routes permitted by the prefix-list can go into the routing table.

Syntax

distribute-list prefix-list *list-name* **in**

no distribute-list prefix-list

Command Default

Prefix lists are not applied to OSPFv3 for IPv6 routing updates.

Parameters

list-name

Name of a prefix-list. The list defines which OSPFv3 networks are to be accepted in incoming routing updates.

in

Applies the prefix list to incoming routing updates on the specified interface.

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

The **no** form of the command removes the prefix list.

Examples

The following example configures a distribution list that applies the filterOspfRoutes prefix list globally:

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# distribute-list prefix-list filterOspfRoutes in
```

History

Release version	Command history
18x.1.00	This command was introduced.

distribute-list route-map

Creates a route-map distribution list.

Syntax

distribute-list route-map *map* **in**

no distribute-list route-map

Parameters

map
Specifies a route map.

in
Creates a distribution list for an inbound route map.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The distribution list can filter Link State Advertisements (LSAs) received from other OSPF devices before adding the corresponding routes to the routing table.

The **no** form of the command removes the distribution list.

Examples

The following example creates a distribution list using a route map named filter1 that has already been configured.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distribute-list route-map filter1 in
```

History

Release version	Command history
18x.1.00	This command was introduced.

domain-name

Creates a maintenance domain at a specified level and name and enters the maintenance domain mode specified in the command argument.

Syntax

domain-name *name* **level** *level*

no domain-name *name* **level** *level*

Command Default

There is no domain configured.

Parameters

name
Specifies the domain name.

level *level*
Sets the domain level.

Modes

CFM protocol configuration mode

Usage Guidelines

The *name* parameter is case sensitive. The level parameter sets the domain level in the range 0 - 7. When the domain already exists, the level argument is optional. Typically, the levels are:

- Customer's Domain Levels: 5 - 7
- Provider Domain Levels: 3 - 4
- Operator Domain Levels: 0 – 2

The **no** form of the command removes the specified domain from the CFM protocol configuration mode.

Examples

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain-name md1 level 4
device(config-cfm-md-md1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x authentication

Enables 802.1x authentication on a port.

Syntax

dot1x authentication

no dot1x authentication

Command Default

802.1x authentication is disabled for ports.

Modes

Interface configuration mode

Usage Guidelines

Port control must be configured to activate authentication on an 802.1x-enabled interface using the **dot1x port-control auto** command from interface configuration mode.

Enter the **no dot1x authentication** command to disable dot1x on the port and remove the configuration from 802.1x management.

Examples

The following example enables 802.1x authentication on a specific port:

```
device# configure terminal
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x authentication
```

Release version	Command history
18x.1.00	This command was introduced.

dot1x enable

Enables 802.1X authentication globally.

Syntax

dot1x enable

Command Default

802.1x authentication is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **dot1x enable** command enables 802.1x authentication globally on all ports.

NOTE
802.1x port authentication is not supported by LAG (Link Aggregation Group) or interfaces that participate in a LAG.

Examples

The following example enables 802.1X authentication globally on all interfaces.

```
device(config)# dot1x enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x filter-strict-security

Enables or disables strict filter security for dot1x authentication on the interface.

Syntax

dot1x filter-strict-security

no dot1x filter-strict-security

Command Default

Strict filter security is enabled.

Modes

Interface configuration mode

Usage Guidelines

By default, strict security mode is enabled; that is the client is not authenticated if the Filter-Id attribute returned by RADIUS contains invalid information, or if insufficient system resources are available to implement the IP ACLs or MAC address filters.

When strict security mode is enabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, a MAC address filter or IP ACL configured on the device), then the client will not be authenticated, regardless of any other information in the message (for example, if the Tunnel-Private-Group-ID attribute specifies a VLAN on which to assign the port).
- If the Vendor-Specific attribute specifies the syntax for a filter, but there are insufficient system resources to implement the filter, then the client will not be authenticated.
- If the device does not have the system resources available to dynamically apply a filter to a port, then the client will not be authenticated.

When strict security mode is disabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, a MAC address filter or IP ACL configured on the device), then the client is still authenticated, but no filter is dynamically applied to it.
- If the Vendor-Specific attribute specifies the syntax for a filter, but there are insufficient system resources to implement the filter, then the client is still authenticated, but the filter specified in the Vendor-Specific attribute is not applied to the port.

The **no** form of the command disables strict filter security.

Examples

The following example enables strict filter security.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x filter-strict-security
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x max-req

Configures the retransmission parameter that defines the maximum number of times EAP request/challenge frames are retransmitted when EAP response/identity frame is not received from the client.

Syntax

dot1x max-req *count*

no dot1x max-req *count*

Command Default

The device retransmits the EAP-request/challenge twice.

Parameters

count

Specifies the number of EAP frame re-transmissions. Th range is from from 1 through 10. The default value is 2.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables this functionality.

Examples

The following example configures the device to retransmit an EAP-request/challenge frame to a client a maximum of three times.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x max-req 3
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x port-control

Controls port-state authorization and configures the port control type to activate authentication on an 802.1X-enabled interface.

Syntax

dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** }

no dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** }

Command Default

The default port state is **auto**.

Parameters

auto

Enables authentication on a port. It places the controlled port in the unauthorized state until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized. This activates authentication on an 802.1X-enabled interface. The controlled port remains in the authorized state until the Client logs off.

force-authorized

Places the controlled port unconditionally in the authorized state, allowing all traffic to pass between the client and the authenticator. This also allows connection from multiple clients.

force-unauthorized

Places the controlled port unconditionally in the unauthorized state, denying any traffic to pass between the client and the authenticator.

Modes

Interface subtype configuration mode

Usage Guidelines

Before activating the authentication using the **dot1x port-control auto** command on a port, you must remove the configured static ACL and static VLANs, if any, from the port.

802.1x port authentication is not supported by LAG (Link Aggregation Group) or interfaces that participate in a LAG.

The **no** form of the command resets the port control type to the default state.

Examples

The following example configures the interface to place the port unconditionally in the unauthorized state until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control auto
```

The following example configures the interface to place the controlled port unconditionally in the authorized state.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control force-authorized
```

The following example configures the interface to place the controlled port unconditionally in the unauthorized state.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control force-unauthorized
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x quiet-period

Configures the time interval that the device remains idle between a failed authentication and a reauthentication attempt.

Syntax

dot1x quiet-period *seconds*

no dot1x quiet-period

Command Default

The default quiet period is 60 seconds.

Parameters

seconds

Specifies the time between failed reauthentication and reauthentication attempt. Valid values range from 1 through 65535 seconds.

Modes

Interface configuration mode

Usage Guidelines

Changing the quiet-period interval time to a number lower than the default can result in a faster response time.

The **no dot1x quiet-period** command restores the default setting.

Examples

The following example sets the idle time as 200 seconds for the device before attempting reauthentication after an authentication failure.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x quiet-period 200
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x reauthenticate

Initiates 802.1X reauthentication on a specified interface.

Syntax

dot1x reauthenticate interface ethernet *slot/port*

Parameters

interface ethernet *slot/port*

Specifies a physical inteface ethernet port in terms of slot number and port nummber.

Modes

Privileged EXEC mode

Examples

```
device# dot1x reauthenticate interface tengigabitethernet 1/0/16
```

The following example initiates reauthentication of a client connected to physical interface 1/1:

```
device# dot1x reauthenticate interface ethernet 1/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x reauthentication

Configures the device to periodically reauthenticate the clients connected to 802.1X-enabled interfaces at regular intervals.

Syntax

dot1x reauthentication

no dot1x reauthentication

Command Default

Periodic reauthentication is disabled.

Modes

Interface configuration mode

Usage Guidelines

When periodic reauthentication is enabled using the **dot1x reauthentication** command, the device reauthenticates the clients every 3,600 seconds by default.

The reauthentication interval is configurable using the **dot1x timeout re-authperiod** command. The reauthentication interval configured using the **dot1x timeout re-authperiod** command takes precedence.

The **no dot1x reauthentication** command disables periodic reauthentication.

Examples

The following example enables 802.1x reauthentication.

```
device# configure terminal
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x reauthentication
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x reauthMax

Sets the maximum number of times that a port attempts 802.1x reauthentication before the port changes to the unauthorized state.

Syntax

dot1x reauthMax *number*

no dot1x reauthMax

Command Default

The number of times that a port attempts 802.1x authentication is 2.

Parameters

number

Specifies the maximum number of reauthentication attempts before the port goes to the unauthorized state. Valid values range from 1 through 10.

Modes

Interface configuration mode

Usage Guidelines

The **no dot1x reauthMax** command restores the default setting.

Examples

The following example sets the maximum number of reauthentication attempts to 5.

```
device# configure terminal
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x reauthMax 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x test eapol-capable

Executes the 802.1x readiness check on the switch.

Syntax

dot1x test eapol-capable interface ethernet *slot/port*

Parameters

interface ethernet *slot/port*

Specifies a physical inteface ethernet port in terms of slot number and port nummber.

Modes

Privileged EXEC mode

Usage Guidelines

This command monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. When you configure the **dot1x test eapol-capable** command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is designated as 802.1x-capable.

The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone). The readiness check is not available on a port that is configured with the command **dot1x port-control force-unauthorized** .

The readiness check is typically used before 802.1x is enabled on the switch.

802.1x authentication cannot be initiated while the 802.1x readiness test is in progress.

The 802.1x readiness test cannot be initiated while 802.1x authentication is active.

802.1x readiness can be checked on a per-interface basis. Readiness check for all interfaces at once is not supported.

Examples

The following example configures readiness check on an interface to determine if the devices connected to the ports are 802.1x-capable.

```
device# dot1x test eapol-capable interface ethernet 1/1
device# 2016/07/18-00:49:03, [DOT1-1012], 5006, M2 | Active | DCE, INFO, sw0, DOT1X_PORT_EAPOL_CAPABLE:
Peer connected to port Ethernet 1/1 is EAPOL capable.
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x test timeout

Sets the 802.1X readiness test timeout.

Syntax

dot1x test timeout *timeout*

Command Default

The default readiness test interval is 10 seconds.

Parameters

timeout

Specifies the readiness test interval value in seconds. Valid values range from 1 through 65535.

Modes

Global configuration mode

Examples

The following example sets the test timeout to 30 seconds:

```
device(config)# dot1x test timeout 30
```

History

Release version	Command history
18x.1.00	This command was introduced.

dot1x timeout

Configures the timeout parameters that determine the time interval for client reauthentication and EAP retransmissions.

Syntax

dot1x timeout {**re-authperiod** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds* }

no dot1x timeout {**re-authperiod** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds* }

Command Default

The timeout parameters are not applied to the device.

Parameters

re-authperiod *seconds*

Specifies the interval at which clients connected to 802.1X authentication enabled ports are periodically reauthenticated. When periodic reauthentication is enabled using the **dot1x reauthentication** command, the device reauthenticates the clients every 3,600 seconds by default. The **re-authperiod** option allows you to specify the time interval between reauthentication attempts. The reauthentication interval configured using the **dot1x timeout re-authperiod** command takes precedence.

supp-timeout *seconds*

Specifies the EAP response timeout for 802.1x authentication. By default, when the device relays an EAP-Request frame from the RADIUS server to the client, it expects to receive a response from the client within 30 seconds. If the client does not respond within the allotted time, the device retransmits the EAP-Request frame to the client. The timeout value for retransmission of EAP-Request frames to the client can be configured using the **supp-timeout** *seconds* parameters.

tx-period *seconds*

Specifies the EAP request retransmission interval, in seconds, with the client. By default, if the device does not receive an EAP-response/identity frame from a client, the device waits 30 seconds, then retransmits the EAP-request/identity frame. You can optionally change the amount of time the device waits before re-transmitting the EAP-request/identity frame to the client. If the client does not send back an EAP-response/identity frame within 60 seconds, the device will transmit another EAP-request/identity frame. The tx-period is a value from 1 through 4294967295. The default is 30 seconds.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables dot1x timeout.

Examples

The following example sets 25 seconds as the amount of time between reauthorization attempts on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout re-authperiod 25
```

The following example sets 45 seconds as the switch-to-client retransmission time for the EAP request frame on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout supp-timeout 45
```

The following example sets 34 seconds as the waiting period for a response to an EAP-request or identity frame from the client before retransmitting the request on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout tx-period 34
```

History

Release version	Command history
18x.1.00	This command was introduced.

dpod

Manages Dynamic Ports on Demand (POD) assignments.

Syntax

dpod *slot/port* { **reserve** | **release** }

Parameters

slot

Specifies a slot number.

port

Specifies a port number.

reserve

Reserves a POD assignment for a port that is currently not able to come online but is expected to be viable in the future. A port license assignment that is reserved will be associated with the first port set that has a vacancy.

release

Removes a port from the port set to which it is currently assigned.

Modes

Global configuration mode

Usage Guidelines

A port POD assignment can only be released if the port is currently offline. Enter **shutdown** to take the port offline.

Do not release a port unless you plan to disconnect the optical link or disable the port persistently. If the link (server or optical) is left in a state where the port could be brought online, the Dynamic POD mechanism will detect this unassigned port and attempt to reassign it to a port set.

Examples

The following example reserves a POD assignment.

```
device# configure terminal
device(config)# dpod 8/15 reserve
device(config-dpod-8/15)# exit
```

The following example removes a port from a POD port set.

```
device# configure terminal
device(config)# dpod 8/15 release
device(config-dpod-8/15)# exit
```

History

Release version	Command history
18x.1.00	This command was introduced.

dscp (Tunnel)

Configures the tunnel differentiated services code point (DSCP).

Syntax

dscp *dscp-value*

no dscp

Parameters

dscp-value

Specifies the DSCP value. The range is from 0 to 63.

Command Default

The default value is 0.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no** form of this command to remove the DSCP configuration.

Examples

This example configures DSCP value for the tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
device(config-intf-tunnel-5)# dscp 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

dscp-ttl-mode

Configures tunnel differentiated services code point (DSCP) time to live (TTL) mode.

Syntax

dscp-ttl-mode { **pipe** | **uniform** }

no dscp-ttl-mode

Command Default

By default, set to pipe mode for all tunnels.

Parameters

pipe

Specifies pipe mode.

uniform

Specifies uniform mode.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no** form of this command to remove the QoS mode configuration.

Supporting the QoS mutation configuration on the VE is not supported.

Examples

This example shows how to configure the quality of service (QoS) mode.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
```

History

Release version	Command history
18x.1.00	This command was introduced.

duplicate-mac-timer (EVPN default instance)

Configures a duplicate MAC detection timer for the detection of continuous MAC moves.

Syntax

duplicate-mac-timer *interval* **max-count** *interval*

no duplicate-mac-timer *interval* **max-count** *interval*

Parameters

interval

Specifies the duplicate MAC detection timer interval in seconds. Valid values range from 5 through 300. The default is 5.

max-count *value*

Specifies the maximum threshold of MAC moves that can occur within the configured time interval before the MAC address is treated as a duplicate address and further advertisements for that MAC address are blocked. Valid values range from 3 through 10. The default is 3.

Modes

EVPN instance configuration mode

Usage Guidelines

The **no** form of the command restores the default values.

Examples

The following example sets the duplicate MAC detection timer interval to 180 and the maximum count to 5 for the default EVPN instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# duplicate-mac-timer 180 max-count 5
```

The following example restores the default duplicate MAC detection timer and maximum count values.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# no duplicate-mac-timer
```

History

Release version	Command history
18x.1.00	This command was introduced.

Commands E - F

encryption-level

Configures the encryption level to use for communication with the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

encryption-level *encryption_level_value*]

no encryption-level

Command Default

The default value is 7; the key is stored in encrypted format.

Parameters

encryption_level_value

Specifies the encryption level value for shared-secret key operation. Valid values are 0 and 7. A value of 0 sprecifies that the key is stored in cleartext format. A value of 7 specifies that the key is stored in encrypted format. The default value is 7.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

NOTE

Before downgrading to a software version that does not support the **encryption-level** command, set the encryption level value to 0. Otherwise, the firmware download displays an error requesting that the encryption level value be set to 0.

Examples

The following example shows how to specify an encryption level of 0; the shared secret key is stored in cleartext format

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# encryption-level 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

enforce-first-as

Enforces the use of the first autonomous system (AS) path for external BGP (eBGP) routes.

Syntax

enforce-first-as

no enforce-first-as

Command Default

The device does not require the first AS listed in the AS_SEQUENCE field of an AS path update message from eBGP neighbors be the AS of the neighbor that sent the update.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command disables this feature.

This command causes the router to discard updates received from eBGP peers that do not list their AS number as the first AS path segment in the AS_PATH attribute of the incoming route.

The device accepts the update only if the AS numbers match. If the AS numbers do not match, the device sends a notification message to the neighbor and closes the session. This requirement applies to all updates received from eBGP neighbors.

Examples

The following example configures the device to enforce the use of the first AS path.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# enforce-first-as
```

History

Release version	Command history
18x.1.00	This command was introduced.

endpoint-tracking enable

Enables endpoint tracking on a Layer 2 (switchport) interface, and optionally enables the reauthentication timer used by each session on the port.

Syntax

endpoint-tracking enable [**reauth-period** *seconds*]

no endpoint-tracking enable [**reauth-period**]

Command Default

Endpoint tracking is disabled.

The endpoint tracking reauthentication timer is disabled.

Parameters

reauth-period *seconds*

Specifies the reauthentication timer in seconds used by each session on the port. Enter an integer from 300 to 86400.

Modes

Interface subtype configuration mode

Usage Guidelines

This feature is supported on the SLX 9850 and SLX 9540 devices only.

The interface must be configured as a Layer 2 (switchport) interface.

Use the **no endpoint-tracking enable** command to disable endpoint tracking.

Use the **no endpoint-tracking enable reauth-period** command to disable the reauthentication timer. Note that this command does not disable endpoint tracking. You must enter the **no endpoint-tracking enable** command to disable endpoint tracking.

If you enter the **endpoint-tracking enable reauth-period** command when endpoint tracking is disabled, the timer is configured but endpoint tracking remains disabled. You must enter the **endpoint-tracking enable** command to enable endpoint tracking.

Examples

The following example configures endpoint tracking configured on an interface configured as a switchport, and configures the reauthentication timer.

```
device: configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# switchport
device(conf-if-eth-0/1)# switchport mode trunk
device(conf-if-eth-0/1)# endpoint-tracking enable
device(conf-if-eth-0/1)# endpoint-tracking enable reauth-period 300
```

error-disable-timeout enable

Enables the timer to bring the interface out of the error-disabled state.

Syntax

error-disable-timeout enable

Modes

Spanning tree configuration mode

Usage Guidelines

When the Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) guard disables a port, the port remains in the disabled state unless the port is enabled manually. This command allows you to enable the interface from the disabled state.

The command is the same regardless of which type of STP is enabled.

Examples

To bring the interface out of the disabled state:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# error-disable-timeout enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

error-disable-timeout interval

Sets the timeout interval for errors on an interface.

Syntax

error-disable-timeout interval *seconds*

no error-disable-timeout interval

Command Default

300 seconds

The timeout feature is disabled.

Parameters

seconds

Specifies the time for the interface to time out. Valid values range from 10 through 1000000 seconds.

Modes

Spanning tree configuration mode

Usage Guidelines

Enter **no error-disable-timeout interval** to return to the default setting.

The command is the same regardless of which type of STP is enabled.

Examples

Follow these examples to set the timeout interval.

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# error-disable-timeout interval 100

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# error-disable-timeout interval 100

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# error-disable-timeout interval 100

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# error-disable-timeout interval 100

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# error-disable-timeout interval 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

esi

Sets the Ethernet Segment ID (ESI) value, which is used to uniquely identify the client for the MCT client, or configures an auto-generated ESI value for a port channel client interface running LACP.

Syntax

esi {*HH:HH:HH:HH:HH:HH:HH:HH:HH:HH* | **auto lacp** }

no esi

Parameters

HH:HH:HH:HH:HH:HH:HH:HH:HH:HH
Specifies the 9-octect ESI value. Enter *HH* in hexadecimal format.

auto lacp
Configures an auto-generated ESI value for a port channel client interface running LACP.

Modes

Cluster client configuration mode

Usage Guidelines

Use the **no** form of the command to delete the ESI setting for the client.

Only one ESI is allowed under a client.

You must configure the same ESI value on both devices in an MCT cluster.

For an MCT client, the configuration of the ESI value creates the MCT client LAG.

The same ESI cannot be added under multiple client entries.

The **esi auto lacp** command is available only in cluster client configuration mode. When a client interface is a port channel and LACP is running on the port channel, MCT supports an automatically-generated ESI value, as defined in RFC 7432. This ESI is encoded as type 1, as follows:

- 1-byte ESI type = 1
- 9-byte ESI value = 6-byte LACP system MAC address of the client followed by the 2-byte LACP port key, and then a 1-byte 0x00

The manually configured ESI uses type 0.

Examples

The following example shows the setting of the ESI value for the cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# esi 00.a1.b2.c3.d4.e5.f6.89.00
```

The following example shows the configuration of an auto-generated ESI for the cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# esi auto lacp
```

History

Release version	Command history
18x.1.00	This command was introduced.

event

Configures an event and action.

Syntax

event{ *average-threshold* | *max-threshold* | *ccm-down* | *ccm-up* } **actions** { *interface-down* | *event-handler* | *all* }

no event

Parameters:

average-threshold
Specifies average thereshold.

max-threshold
Specifies maximum thereshold.

ccm-down
Specifies CCM is down

ccm-up
Specifies CCM is up.

actions
Specifies the actions.

interface-down
Specifies interface down.

event-handler
Specifies event handler.

all
Specifies all.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command delete the corresponding configured action profile also corresponding associations with Source and Target MEP pair.

Examples

This example shows how to create an action profile.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# y1731
device(config-cfm-y1731)# action-profile action-prof-act1
device((protocol-cfm)# event max-threshold actions all
```

History

Release version	Command history
18x.1.00	This command was introduced.

event-handler

Creates or accesses an event-handler profile, which can execute a Python script when a specified trigger occurs.

Syntax

event-handler *event-handler-name* [**action python-script** *file-name*]

event-handler *event-handler-name* [**description** *description-text*]

event-handler *event-handler-name* [**trigger** *trigger-id* **raslog** *raslog-id* [**pattern** *posix-ext-regex*]]

no event-handler *event-handler-name*

Command Default

No event-handler profile is enabled.

Parameters

event-handler-name
Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

action python-script *file-name*
Specifies a Python file that runs when a trigger-condition occurs. Valid values range from 4 through 32 characters (including the **.py** extension). The first character must be alphanumeric.

description *description-text*
Specifies a string describing the event-handler profile. The string can be 1 through 128 ASCII characters in length. Do not use the ? character. If you need to use ! or \, precede each with \.

trigger *trigger-id*
Defines an event-handler trigger and specifies an ID number for the trigger. Valid values are 1 through 100, and must be unique per event-handler profile. When the trigger-condition occurs, a Python script is run.

raslog *raslog-id*
Specifies a RASlog message ID as the trigger.

pattern *posix-ext-regex*
Specifies a POSIX extended regular expression to search for a match within the specified RASlog message ID. For examples, refer to the "trigger" topic.

Modes

Global configuration mode

Event-handler configuration mode for an existing event handler. (There is no need to enter the **exit** command to return to global configuration mode.)

Usage Guidelines

You can create multiple event-handler profiles.

You can optionally specify a description, a trigger, or the Python script with this command; or specify them later.

An **event-handler** command creates or accesses an event-handler profile and can also define one of the following parameters:

- Description
- One trigger
- The Python-script action that runs on any trigger

You can also define the above parameters—including one or more triggers—from event-handler configuration mode.

A Python event-handler script runs only if all of the following occur:

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.
- Either using the **event-handler** command or in configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.
  - Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

If an event-handler profile is not activated, the **no** form of this command deletes it.

Examples

The following example creates an event-handler profile and accesses its configuration mode.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

event-handler abort action

Under Python event-management, aborts a specified event handler that is currently running.

Syntax

event-handler abort action *event-handler-name*

Parameters

event-handler-name

Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

Modes

Privileged EXEC mode

Examples

The following command successfully aborted event-handler action "eh1".

```
device# event-handler abort action eh1
This operation will abort an event handler action that is currently running and may leave the switch in
an inconsistent state.  Do you want to continue? [y/n]:y
Operation completed successfully.
```

History

Release version	Command history
18x.1.00	This command was introduced.

event-handler activate

Activates an event handler and accesses event-handler activation mode, from which you can enter advanced configuration commands. You can also append the advanced commands to **event-handler activate**.

Syntax

event-handler activate *event-handler-name*

event-handler activate *event-handler-name* [**action-timeout** *minutes*] [**delay** *seconds*] [**iterations** *num-iterations*] [**interval** *seconds*] [**trigger-mode** *mode*] [**trigger-function** { OR | AND [**time-window** *seconds*] }]

no event-handler activate *event-handler-name*

Command Default

No event handler is activated on the device.

Parameters

event-handler-name
Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

action-timeout *minutes*
Specifies the number of minutes to wait for an action-script to complete execution. If you specify "0", no timeout is set. Valid timeout values are any positive integer.

delay *seconds*
Specifies a number of seconds from when a trigger is received until the execution of the specified action begins. Valid values are 0 or a positive integer.

iterations *num-iterations*
Specifies the number of times an event-handler action is run, when triggered. Valid values are any positive integer. The default value is 1.

interval *seconds*
Specifies the number of seconds between iterations of an event-handler action, if triggered. Valid values are 0 or a positive integer. The default is 0.

trigger-mode *mode*
Specifies if an event-handler action can be triggered only once or more than once. The default is each time the trigger condition occurs, the event-handler action is launched.

each-instance
The event-handler action is launched on each trigger instance received.

on-first-instance
As long as the device is running, the event-handler action is launched only once. Following a device restart, the event-handler action can be triggered again.

only-once
For the duration of a device's configuration, the event-handler action is launched only once.

trigger-function

For an implementation of an event-handler profile, if multiple triggers are defined for an event-handler action, specifies if the action runs only if all of the triggers occur; or if one is sufficient.

OR

The event-handler action runs if any of the triggers occur.

AND

The event-handler action runs only if all of the triggers occur.

time-window *seconds*

In seconds, specify the time window within which all of the triggers must occur in order that the event-handler action runs. Once all triggers have been received and on each subsequent trigger received, the action will be launched when the time difference between the latest trigger and the oldest trigger is less than or equal to the configured time-window.

Modes

Global configuration mode

Event-handler activation mode for an existing event handler. (There is no need to enter the **exit** command.)

Usage Guidelines

You can activate up to 10 different event-handler profiles on a device.

A Python event-handler script runs only if all of the following occur:

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.
- In configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.
  - Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

For additional usage guidelines regarding the advanced configuration commands, see the following topics:

- **action-timeout**
- **delay**
- **iterations**
- **interval**
- **trigger-mode**
- **trigger-function**

Following an initial triggering of an event-handler action, any subsequent trigger launches the action an additional time if the following conditions are true:

- The **trigger-mode** parameter is set to the default **each-instance**.
- The subsequent trigger occurs within the specified **time-window**.

To inactivate an event-handler instance on a device, use the **no** form of this command. If an event-handler Python script is running, it is executed to completion before inactivation of the event handler.

Examples

This example activates eventHandler1 on the device.

```
device# configure terminal
event-handler activate eventHandler1
device(config-activate-eventHandler1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

evpn

Creates an EVPN instance and enables EVPN instance configuration mode.

Syntax

evpn [*name*]

no evpn { **default** |*name* }

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove the EVPN instance.

When you enter the **evpn** command without a name, a default EVPN instance is created.

The device allows only one EVPN instance.

Examples

The following example configures the default EVPN instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)#
```

The following example creates an EVPN instance named myinstance.

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

export-vrf-leaked-routes

Allows exporting VRF leaked routes to Layer VPN.

Syntax

export-vrf-leaked-routes

no export-vrf-leaked-routes

Modes

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command disables exporting VRF leaked routes to Layer VPN.

Examples

This example shows how to export VRF leaked routes to Layer VPN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family vpnv4 unicast
device(config-bgp-vpnv4u)# export-vrf-leaked-routes
```

History

Release version	Command history
18x.1.00	This command was introduced.

export-map

Exports the target-VPN community.

Syntax

export-map *route-map*

no export-map *route-map*

Parameters

route-map

Specifies the route-map name.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of the command to apply a route-map filter on the routes to be exported.

Examples

The following example shows how to export the target-VPN community.

```
device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd 1:2
device#(config-vrf-vpn1)# vpn-statistics
device#(config-vrf-vpn1)# address-familin ipv4 unicast
device#(config-vrf-vpn1-ipv4-unicast)# route-target-import 100:1
device#(config-vrf-vpn1-ipv4-unicast)# export-map import-route-map1
```

History

Release version	Command history
18x.1.00	This command was introduced.

extend bridge-domain

Configures a bridge domain (BD) to a site for a VXLAN Layer 2 gateway.

Syntax

extend bridge-domain { **add** | **remove** } *bridge_domain_id*

Parameters

add
Adds a bridge-domain ID to a tunnel.

remove
Removes a bridge-domain ID from a tunnel.

bridge_domain_id
Specifies the configured bridge domain ID.

Modes

Site configuration mode

Examples

The following example configures the bridge domain to the site of the VXLAN Layer 2 gateway.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-overlay-gw-gateway1-site-mysite)# extend bridge-domain add 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

extend vlan

Configures switchport VLANs for the tunnels to the containing site in VXLAN overlay gateway configurations.

Syntax

extend vlan { **add** | **remove** } *vlan_id*

no extend vlan

Parameters

add
Specifies a VLAN ID or range of VLAN IDs to be added to a tunnel.

remove
Specifies a VLAN ID or range of VLAN IDs to be removed from a tunnel.

vlan_id
A VLAN ID or range of VLAN IDs. See the Usage Guidelines.

Modes

VXLAN overlay gateway site configuration mode

Usage Guidelines

The VXLAN Network Identifier (VNI) classification is derived from the "map vlan" configuration of the parent overlay gateway. This command results in the provisioning or unprovisioning of the VLANs. Use the **no extend vlan** *vlan_id* command to unprovision a VLAN.

All of the VLAN IDs that are specified must be VLANs that have been mapped by means of the **map vlan** *vlan_id* **vni** *vni* command on the parent overlay gateway, unless automatic VNI mapping has been enabled by means of the **map vlan vni auto** command.

Use the **no attach vlan** *vlan_id* command to remove all switchport configurations from the tunnels to the containing site.

Examples

Use the **no attach vlan** *vlan_id* command to remove all switchport configurations from the tunnels to the containing

To configure a switchport VLAN and range of VLANs:

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-overlay-gw-gateway1-site-mysite)# extend vlan add 10,20-30
```

History

Release version	Command history
18x.1.00	This command was introduced.

external-lsdb-limit (OSPFv2)

Configures the maximum size of the external link state database (LSDB).

Syntax

external-lsdb-limit *value*

no external-lsdb-limit

Parameters

value

Maximum size of the external LSDB. Valid values range from 1 through 14913080. The default is 14913080.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

If you change the value, make sure to save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

The **no** form of the command restores the default setting.

Examples

The following example sets the limit of the LSDB to 20000.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# external-lsdb-limit 20000
```

History

Release version	Command history
18x.1.00	This command was introduced.

external-lsdb-limit (OSPFv3)

Configures the maximum size of the external link state database (LSDB).

Syntax

external-lsdb-limit *value*

no external-lsdb-limit

Parameters

value

Maximum size of the external LSDB. Valid values range from 1 through 250000. The default is 250000.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

If you change the value, you must save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

The **no** form of command reverts to the default setting.

Examples

The following example sets the limit of the external LSDB to 15000.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# external-lsdb-limit 15000
```

History

Release version	Command history
18x.1.00	This command was introduced.

fast-external-fallover

Resets the session if a link to an eBGP peer goes down.

Syntax

fast-external-fallover

no fast-external-fallover

Modes

BGP configuration mode

Usage Guidelines

Use this command to terminate and reset external BGP sessions of a directly adjacent peer if the link to the peer goes down, without waiting for the timer, set by the BGP **timers** command, to expire. This can improve BGP conversion time, but can also lead to instability in the BGP routing table as a result of a flapping interface.

Examples

The following example configures the device to reset the session if a link to an eBGP peer goes down.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# fast-external-fallover
```

History

Release version	Command history
18x.1.00	This command was introduced.

firmware commit

Commits a firmware upgrade.

Syntax

firmware commit

Modes

Privileged EXEC mode

Usage Guidelines

The **firmware download** command updates the secondary partitions only. When the **firmware download** command completes successfully and the device reboots, the system swaps partitions. The primary partition (with the previous firmware) becomes the secondary partition, and the secondary partition (with the new firmware) becomes the primary partition.

By default, **firmware download** automatically commits the firmware after the device reboots. If you disable auto-commit mode when running **firmware download**, you must execute **firmware commit** to commit the new firmware to the secondary partition.

You must run the **firmware download** command with the **nocommit** parameter set for the following firmware commit operation to succeed.

Examples

To commit the firmware:

```
device# firmware commit

Validating primary partition...
Doing firmwarecommit now.
Please wait ...
Replicating kernel image
.............
FirmwareCommit completes successfully.
```

History

Release version	Command history
18x.1.00	This command was introduced.

firmware download

Downloads the firmware on the local device and updates the ONIE image and diag OS images automatically as part of the process.

Syntax

firmware download [**default-config**] [**http** |**ftp** | **scp** | **sftp** | **tftp** | **usb** | **interactive** [**coldboot**] **host** *host_ip_address* **user** *username* **password** *password* **directory** *directory* [**file** *file_name*]]

Command Default

By default, **firmware download** invokes the **firmware download coldboot**command (downloads the firmware to the system, reboots the system, and commits the firmware automatically).

Parameters

default-config

Installs new firmware on the switch and brings the configuration state of the switch to a default state when it boots up on the new firmware. Its effect can be perceived as “firmware download” and “copy default-config startup-config” combined..

http |**ftp** | **scp** | **sftp** | **tftp** | **usb**

Valid protocols are **http** (Hyper Text Transfer Protocol), **ftp** (File Transfer Protocol), **scp** (Secure Copy), **sftp** (SSH File Transfer Protocol)
, **tftp** (Trivial File Transfer Protocol)
, or **usb** (Universal Serial Bus)

interactive

Runs firmware download in interactive mode. You are prompted for input.

coldboot

Installs new firmware on the switch and reboots the switch automatically after installation.

host

Specifies the host by IP address.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

user *username*

Specifies the user login name for the host.

password *password*

Specifies the account password.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *file_name*

Specifies the firmware .xlist file. This parameter is optional; if unspecified, the default file, release.xlist, is used.

Modes

Privileged EXEC mode

Usage Guidelines

You can use one of the following options for firmware upgrade/downgrade; coldboot, or default-config.

The coldboot and default-config options involve system reboots and are disruptive to traffic.

In addition, default-config causes the loss of configuration because it resets the configuration back to the default settings during the firmware upgrade process.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

Examples

When the user invokes the firmware download command with the http protocol, only the host and directory parameters are required. The user and password are not needed, for example:

```
device# firmware download http host 192.168.1.1 directory fw
```

History

Release version	Command history
18x.1.00	This command was introduced.

firmware install

Installs new firmware but deletes all configuration in the system.

Syntax

firmware install [**local**] [**ftp** | **scp host** *host_ip* **user** *user_id* **password** *user_pw* **directory** *firmware_directory*]

Command Default

New firmware is not installed.

Parameters

local
Install the firmware using local bin image.

ftp
Specifies FTP as the protocol used to install the firmware.

scp
Specifies SCP as the protocol used to install the firmware.

host
Specifies the host by DNS name or IP address.

host_ip_address
Specifies the host IP address. IPv4 and IPv6 addresses are supported.

user *username*
Specifies the user login name for the host.

password *password*
Specifies the account password.

directory *directory*
Specifies a fully qualified path to the directory where the firmware is located.

Modes

Privileged EXEC mode

Usage Guidelines

The **firmware install** command cleans the existing firmware on the system before installing the new firmware. All configurations in the system is completely lost.

During the installation, the switch will be rebooted. After the installation, the switch goes back to the factory default state. It is imperative that the user save the configuration before invoking this command.

CAUTION
Do not use this command unless instructed by Extreme Technical Support.

Examples

To install new firmware, delete all existing configurations, or to recover a switch with inconsistent firmware, enter this command:

```
device# firmware install scp host 10.6.46.54 directory /slxosx/slxos18x.1.00/slxos18x.1.00 user fvt
Password: **********
Performing system sanity check...

You are installing the slxos, this command will cause the switch to reboot, and will restore the switch
back to factory default. You will need to save the configuration before proceeding.

Do you want to continue? [y/n]:
```

History

Release version	Command history
18x.1.00	This command was introduced.

flex-cli show link-fault-signaling

Displays information pertaining to link fault signaling (LFS).

Syntax

flex-cli show link-fault-signaling

Modes

Privileged EXEC mode

Command Output

The **flex-cli show link-fault-signaling** command displays the following information:

Output field	Description
Port	Port number
Rx-Link-Fault	Displays rx link fault
Tx-Link-Fault	Displays tx link fault

Examples

This example displays information pertaining to LFS.

```
device# flex-cli show link-fault-signaling
Port    Rx-Link-Fault    Tx-Link-Fault
0/1     ON               ON
0/2     ON               ON
0/3     ON               ON
0/4     ON               ON
0/5     ON               ON
0/6     ON               ON
0/7     ON               ON
0/8     ON               ON
0/9     ON               ON
0/10    ON               ON
0/11    ON               ON
0/12    ON               ON
0/13    ON               ON
0/14    ON               ON
0/15    ON               ON
0/16    ON               ON
0/17    ON               ON
0/18    ON               ON
0/19    ON               ON
0/20    ON               ON
0/21    ON               ON
0/22    ON               ON
```

History

Release version	Command history
18x.1.00	This command was introduced.

flex-cli show local-fault interface

Displays the local faults of an interface.

Syntax

flex-cli show local-fault interface [**ethernet** *slot/port* | **port-channel** *port-chnnel-number*]

Parameters

ethernet

Specifies Ethernet interface.

slot-number

Specifies the slot number.

port-channel

Specifies port-channel.

port-channel numbe

Specifies the port-channel number.

Modes

Privileged EXEC mode

Examples

This example displays the local faults of an interface.

```
device# flex-cli show local-fault interface ethernet 0/9
Port    Local-Fault-Detected      Local-Fault-Count  Time-Last-Local-Fault-Dete
ted
0/9     No                                      0  N/A
dutC-Aval#
0/4     No                                      0  N/A
0/5     No                                      0  N/A
0/6     No                                      0  N/A
0/7     No                                      0  N/A
0/8     No                                      0  N/A
0/9     No                                      0  N/A
0/10    No                                      0  N/A
0/11    No                                      0  N/A
0/12    No                                      0  N/A
0/13    No                                      0  N/A
0/14    No                                      0  N/A
0/15    No                                      0  N/A
0/16    No                                      0  N/A
0/17    No                                      0  N/A
0/18    No                                      0  N/A
0/19    No                                      0  N/A
0/20    No                                      0  N/A
0/21    No                                      0  N/A
```

History

Release version	Command history
18x.1.00	This command was introduced.

flex-cli show local-fault slot

Displays the local faults of a slot.

Syntax

flex-cli show local-fault slot *slot-number*

Parameters

slot-number

Specifies the slot number.

Modes

Privileged EXEC mode

Examples

This example displays the local faults of a slot.

```
device# flex-cli show local-fault slot 1
Port    Local-Fault-Detected      Local-Fault-Count  Time-Last-Local-Fault-Deteted
0/1     No                                      0  N/A
0/2     No                                      0  N/A
0/3     No                                      0  N/A
```

History

Release version	Command history
18x.1.00	This command was introduced.

flex-cli show remote-fault interface

Displays the remote faults of an interface.

Syntax

flex-cli show remote-fault interface [**ethernet** *slot/port* | **port-channel** *port-chnnel-number*]

Parameters

ethernet
Specifies Ethernet interface.

slot-number
Specifies the slot number.

port-channel
Specifies port-channel.

port-channel numbe
Specifies the port-channel number.

Modes

Privileged EXEC mode

Examples

This example displays the remote faults of an interface.

```
device# flex-cli show remote-fault interface ethernet 0/10
Port    RFN-Detected      Remote-fault-count  Time-last-RFN-Detected
0/10    No                                0  N/A
```

History

Release version	Command history
18x.1.00	This command was introduced.

flex-cli show remote-fault slot

Displays the remote faults of a slot.

Syntax

flex-cli show remote-fault slot *slot-number*

Parameters

slot-number

Specifies the slot number.

Modes

Privileged EXEC mode

Examples

This example displays the remote faults of a slot.

```
device# flex-cli show remote-fault slot 1
Port    RFN-Detected      Remote-fault-count  Time-last-RFN-Detected
0/1     No                                0  N/A
0/2     No                                0  N/A
0/3     No                                0  N/A
0/4     No                                0  N/A
0/5     No                                0  N/A
0/6     No                                0  N/A
0/7     No                                0  N/A
0/8     No                                0  N/A
0/9     No                                0  N/A
0/10    No                                0  N/A
0/11    No                                0  N/A
0/12    No                                0  N/A
0/13    No                                0  N/A
0/14    No                                0  N/A
0/15    No                                0  N/A
0/16    No                                0  N/A
0/17    No                                0  N/A
0/18    No                                0  N/A
0/19    No                                0  N/A
0/20    No                                0  N/A
0/21    No                                0  N/A
0/22    No                                0  N/A
```

History

Release version	Command history
8x.1.00	This command was introduced.

format RFC-5424

Configures a specified syslog server to log messages using the RFC-5424 format.

Syntax

format RFC-5424

no format RFC-5424

Parameters

RFC-5424

Syslog message format defined in RFC-5424.

Modes

Syslog server configuration mode

Usage Guidelines

Use this command to configure the router to generate log messages with the RFC-5424 format.

The RFC-5424 syslog message header consists of the following fields:

<*prival*><*version*><space>< *time-stamp*><space><*host-name*><space><*app name*><space><*process id*><space><*Msg Id*>

Where:

- *prival* is the priority field. This is always <190> for SLXOS 17r.2.00.
- *version* is the version number of the syslog protocol standard. Currently, this can only be 1.
- *time-stamp* is the ISO 8601 compatible standard timestamp format (yyyy-mm-ddThh:mm:ss+-ZONE).
- *host-name* is the machine that originally sent the message, or if no hostname, a "–" is present instead.
- *app name* is the device or application that generated the message, or if no application, a "–" is present instead.
- *process id* is the process name or PID (process ID) of the syslog application that sent the message, or if no PID, a "–" is present instead. This is always – in the SLX-OS 17r.2.00 release.
- *Msg Id* is the ID number of the message, or if no Message ID, a "–" is present instead. This is always – in the SLX-OS 17r.2.00 release.

For example:

```
<190>1 2017-06-19T09:19:52.000003+00:00 SLX raslogd - -
```

NOTE

In the SLX-OS 17r.2.00 release, the *process id* and *Msg Id* fields are not filled and are replaced with – –.

Use the **no format RFC-5424** command to remove the RFC-5424 log message format from the syslog server configuration.

Examples

First, access the global configuration level of the CLI and configure the IP address for the syslog server. Then, enter the **format RFC-5424** command to configure the router to use the RFC-5424 format as shown in the following example.

```
device# configure terminal
device(config)# logging syslog-server 192.168.163.233
device(config-syslog-server-192.168.163.233)# format RFC-5424
```

To verify the syslog server log message format, enter the **show running-config logging syslog-server** command as shown in the following example.

```
device# running-config logging syslog-server
logging syslog-server 192.168.163.233
format RFC-5424
```

To remove the RFC-5424 format from the configured syslog server, enter the **no format RFC-5424** command as shown in the following example.

```
device(config)# logging syslog-server 192.168.163.233
device(config-syslog-server-192.168.163.233)# no format RFC-5424
```

History

Release version	Command history
18x.1.00	This command was introduced.

forward-delay

Specifies the time an interface spends in each of the listening and learning states.

Syntax

forward-delay *seconds*

no forward-delay

Command Default

15 seconds

Parameters

seconds

Specifies the time that an interface spends in the Spanning Tree Protocol (STP) learning and listening states. Valid values range from 4 through 30 seconds.

Modes

Spanning tree configuration mode

Usage Guidelines

This command specifies how long the listening and learning states last before the interface begins the forwarding of all spanning-tree instances.

STP interface states:

- Listening - The interface processes the Bridge Protocol Data Units (BPDUs) and awaits possible new information that might cause it to return to the blocking state.
- Learning - The interface does not yet forward frames (packets), instead it learns source addresses from frames received and adds them to the filtering database (switching database).
- Forwarding - An interface receiving and sending data, normal operation. STP still monitors incoming BPDUs that can indicate it should return to the blocking state to prevent a loop.
- Blocking - An interface that can cause a switching loop, no user data is sent or received, but it might go to the forwarding state if the other links in use fail and the STP determines that the interface may transition to the forwarding state. BPDU data continues to be received in the blocking state.

When you change the spanning-tree forward-delay time, it affects all spanning-tree instances. When configuring the forward-delay, the following relationship should be kept:

```
(2 × (forward-delay – 1)) >= max-age >= (2 × (hello-time + 1))
```

Enter **no forward-delay** to return to the default settings.

The command is the same regardless of which type of STP is enabled.

Examples

To configure the forward-delay time to 18 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# forward-delay 18

device# configure terminal
device(config)## protocol spanning-tree rstp
device(conf-rstp)# forward-delay 18

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# forward-delay 18

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# forward-delay 18

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# forward-delay 18
```

History

Release version	Command history
18x.1.00	This command was introduced.

Commands G - J

graceful-restart (BGP)

Enables the BGP graceful restart capability.

Syntax

graceful-restart [**purge-time** *seconds* | **restart-time** *seconds* | **stale-routes-time** *seconds*]

no graceful-restart

Command Default

Disabled.

Parameters

purge-time

Specifies the maximum period of time, in seconds, for which a restarting device maintains stale routes in the BGP routing table before purging them. The default value is 600 seconds. The configurable range of values is from 1 to 3600 seconds.

restart-time

Specifies the restart-time, in seconds, advertised to graceful restart-capable neighbors. The default value is 120 seconds. The configurable range of values is from 1 to 3600 seconds.

stale-routes-time

Specifies the maximum period of time, in seconds, that a helper device will wait for an End-of-RIB (EOR) message from a peer. All stale paths are deleted when this time period expires. The default value is 360 seconds. The configurable range of values is from 1 to 3600 seconds.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family EVPN configuration mode

Usage Guidelines

Use this command under a BGP address-family configuration mode to enable or disable the graceful-restart capability for all BGP neighbors in the address family. When this command is enabled, graceful-restart capability is negotiated with neighbors in the BGP OPEN message when a session is established. If the neighbor advertises support for graceful restart, that function is activated for that neighbor session. Otherwise, graceful restart is not activated for that session, even though it is enabled locally. If the neighbor has not sent graceful-restart parameters, the restarting device will not wait for the neighbor to start route calculation, but graceful restart will be enabled.

If the graceful-restart capability is enabled after a BGP session has been established, the neighbor session must be cleared for graceful restart to take effect.

The **purge-time** parameter is applicable for both restarting and helper devices. The timer starts when a BGP connection is closed. The timer ends when an EOR is received from all nodes, downloaded into BGP and an EOR sent to all neighbors. The configured purge-time timer value is effective only on the configured node.

The **restart-time** parameter is applicable only for helper devices. The timer starts at the time the BGP connection is closed by the remote peer and ends when the Peer connection is established. The configured restart-time timer value is effective only on the peer node, and not in the configured node. During negotiation time, the timer value is exchanged.

The **stale-routes-time** parameter is applicable only for helper devices. The timer starts when the peer connection is established after the HA-failover. The timer ends at the time an EOR is received from the peer. The configured stale-time timer value is effective only on the configured node.

For non-default VRF instances, graceful restart timers are inherited from the default VRF. The **purge-time**, **restart-time**, and **stale-routes-time** parameters are not available in BGP address-family IPv4 unicast VRF configuration mode and BGP address-family IPv6 unicast VRF configuration mode.

Use the **clear ip bgp neighbor** command with the **all** parameter for the changes to the graceful-restart parameters to take effect immediately.

The **no** form of the command disables the BGP graceful-restart capability globally for all BGP neighbors in the address family.

Examples

The following example enables the BGP graceful restart capability.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
```

The following example sets the purge time to 240 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv4u)# graceful-restart purge-time 240
```

The following example sets the restart time to 60 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv4u)# graceful-restart restart-time 60
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sets the stale-routes time to 180 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1000::1 remote-as 2
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 1000::1 activate
device(config-bgp-ipv6u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv6u)# graceful-restart stale-routes-time 180
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example enables the BGP graceful restart capability and sets the purge time to 220 seconds in EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# graceful-restart purge-time 220
```

History

Release version	Command history
18x.1.00	This command was introduced.

graceful-restart (OSPFv2)

Enables the OSPF Graceful Restart (GR) capability.

Syntax

graceful-restart [**helper-disable** | **restart-time** *seconds*]

no graceful-restart

Command Default

Graceful restart and graceful restart helper capabilities are enabled.

Parameters

helper-disable

Disables the GR helper capability.

restart-time

Specifies the maximum restart wait time, in seconds, advertised to neighbors. The default value is 120 seconds. The configurable range of values is from 10 through 1800 seconds.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Use **no graceful-restart helper-disable** to re-enable the GR helper capability.

The **no** form of the command disables the graceful restart capability.

Examples

The following example disables the GR helper capability.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# graceful-restart helper-disable
```

The following example re-enables the GR helper capability.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# no graceful-restart helper-disable
```

The following example re-enables the GR capability and changes the maximum restart wait time from the default value to 240 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# graceful-restart restart-time 240
```

History

Release version	Command history
18x.1.00	This command was introduced.

graceful-restart helper (OSPFv3)

Enables the OSPFv3 graceful restart (GR) helper capability.

Syntax

graceful-restart helper { **disable** | **strict-lsa-checking** }

no graceful-restart helper

Command Default

GR helper is enabled.

Parameters

disable

Disables the OSPFv3 GR helper capability.

strict-lsa-checking

Enables the OSPFv3 GR helper mode with strict link-state advertisement (LSA) checking.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command disables the GR helper capability on a device.

Examples

The following example enables GR helper and sets strict LSA checking.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# graceful-restart helper strict-lsa-checking
```

History

Release version	Command history
18x.1.00	This command was introduced.

hardware

Accesses hardware configuration mode to access the connector, port-group, and profile configuration modes.

Syntax

hardware

Modes

Global configuration mode

Examples

The following example shows the accessing of hardware configuration mode.

```
device# configure terminal
device(config)# hardware
device(config-hardware)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

hello (LLDP)

Sets the interval between LLDP hello messages.

Syntax

hello *seconds*

no hello

Command Default

30 seconds

Parameters

seconds

Valid values range from 4 through 180 seconds.

Modes

LLDP protocol and profile configuration modes

Usage Guidelines

The LLDP hello messages can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

Enter **no hello** to return to the default setting.

Examples

To set the time interval to 10 seconds between the transmissions:

```
device# configure terminal
device (config)# protocol lldp
device(conf-lldp)# hello ?
Possible completions:
<4-180>   Seconds[30 seconds]
device(conf-lldp)# hello 10
```

To set the time interval to 8 seconds between the transmissions for a specific LLDP profile:

```
device(conf-lldp)# profile test1
device(config-profile-test1)# hello 8
device(config-profile-test1)#
```

History

Release version	Command history
18x. 1.00	This command was introduced.

hello-interval

Configures a global hello interval for the loop-detection (LD) protocol.

Syntax

hello-interval *milliseconds*]

no hello-interval

Command Default

See the Usage Guidelines.

Parameters

milliseconds

Range is from 100 through 5000 milliseconds. The default is 1000 milliseconds.

Modes

Protocol Loop Detection configuration mode.

Usage Guidelines

Use the **no** form of this command to revert to the default hello interval.

Examples

To configure a hello interval of 2000 milliseconds:

```
device# configure terminal
device(config)# protocol loop-detection
device(config-loop-detect)# hello-interval 2000
```

To revert to the default hello interval:

```
device# configure terminal
device(config)# protocol loop-detection
device(config-loop-detect)# no hello-interval
```

History

Release version	Command history
18x.1.00	This command was introduced.

hello-interval (PIM)

Sets the frequency with which the device sends PIM hello messages to its neighbors.

Syntax

hello-interval *seconds*

no hello-interval

Command Default

The default is 30 seconds.

Parameters

seconds

Specifies the hello interval value in seconds. The range is 10 to 3600 seconds.

Modes

PIM Router configuration mode

Examples

The following example sets the PIM hello interval.

```
device(config)# router pim
device(config-pim-router)# hello-interval 50
```

History

Release version	Command history
18x.1.00	This command was introduced.

hello-time

Sets the interval between the hello Bridge Protocol Data Units (BPDUs) sent on an interface.

Syntax

hello-time *seconds*

no hello-time

Command Default

2 seconds

Parameters

seconds

Specifies the time interval between the hello BPDUs sent on an interface. Valid values range from 1 through 10 seconds.

Modes

Spanning tree configuration mode

Usage Guidelines

This command configures the spanning-tree bridge hello time, which determines how often the device broadcasts hello messages to other devices.

If the VLAN parameter is not provided, the **hello-time** value is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration. When configuring the **hello-time**, the **max-age** command setting must be greater than the **hello-time** setting. The following relationship should be kept:

```
(2 × (forward-delay - 1)) >= max-age >= (2 × (hello-time + 1))
```

Enter **no hello-time** to return to the default settings.

The command is the same regardless of which type of STP is enabled.

Examples

To configure spanning tree bridge hello time to 5 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# hello-time 5

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# hello-time 5

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# hello-time 5

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# hello-time 5

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# hello-time 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

hold-time

Sets the time that a previously down backup VRRP router, which also must have a higher priority than the current master VRRP router, will wait before assuming mastership of the virtual router.

Syntax

hold-time *range*

Command Default

0 seconds

Parameters

range

A value between 1 and 3600 seconds that specifies the time a formerly down backup router waits before assuming mastership of the virtual router.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The hold-time must be set to a number greater than the default of 0 seconds for this command to take effect.

This command can be used for both VRRP and VRRP-E.

Examples

To set the hold time to 60 seconds for backup routers in a specific virtual router:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 1
device(config-vrrp-extended-group-1)# hold-time 60
```

History

Release version	Command history
18x.1.00	This command was introduced.

host-table aging-mode conversational

Enables conversational address-resolution protocol (ARP) and conversational neighbor discovery (ND). Such enablement improves hardware utilization by programming only active flows into the forwarding plane.

Syntax

host-table aging-mode conversational

no host-table aging-mode conversational

Command Default

Conversational ARP/ND is disabled.

Modes

Global configuration mode

Usage Guidelines

You can change the aging-time value from the 300 second default—either before or during enablement—by entering the **host-table aging-time conversational** command.

Conversational ARP/ND can be CPU-intensive.

If conversational ARP/ND is not enabled, make sure that the software ARP/ND cache size is less than the hardware profile limit.

To disable conversational ARP/ND, enter the **no** form of this command.

Upon disablement, the conversational ARP/ND timers no longer apply: All current entries become permanent as do all new entries.

Examples

The following example enables conversational ARP/ND.

```
device# configure terminal
device(config)# host-table aging-mode conversational
```

History

Release version	Command history
18x.1.00	This command was introduced.

host-table aging-time conversational

Specifies a non-default aging-time value for conversational ARP/ND.

Syntax

host-table aging-time conversational *seconds*

no host-table aging-time conversational

Command Default

If conversational ARP/ND is enabled (by entering the **host-table aging-mode conversational** command), the default aging-time value is 300 seconds.

Parameters

seconds

Specifes the aging-time value for conversational ARP/ND. Values range from 60 through 100000 seconds. The default is 300.

Modes

Global configuration mode

Usage Guidelines

You can modify the aging-time value either before or after enabling conversational ARP/ND.

Pre-existing entries age out using the old configured value. A changed age-time configuration applies only entries added following the change.

To restore the default aging-time value of 300 seconds, enter the **no** form of this command.

Examples

The following example sets the aging-time value to 600 seconds and then enables conversational ARP/ND.

```
device# configure terminal
device(config)# host-table aging-time conversational 600
device(config)# host-table aging-mode conversational
```

History

Release version	Command history
18x.1.00	This command was introduced.

http server

Configures HTTP or HTTPS service on a device.

Syntax

http server use-vrf *vrf-name* **shutdown**

http server shutdown

no http server use-vrf *vrf-name* **shutdown**

no http server shutdown

Parameters

use-vrf *vrf-name*
Specifies a user-defined VRF.

shutdown
Disables HTTP or HTTPS service.

Modes

Global configuration mode

Usage Guidelines

Use the **http server** command with the **use-vrf** parameter to enable HTTP or HTTPS service and associate it with the specified VRF. The **use-vrf** parameter configures HTTP or HTTPS service for the specified VRF only. Service for that VRF is enabled or disabled with no effect on service for other VRFs.

Use the **http server** command with the **use-vrf** and **shutdown** parameters to disable HTTP or HTTPS service for the specified VRF. When both HTTP and HTTPS are enabled, executing the **http server** command with the **use-vrf** and **shutdown** parameters disables both HTTP and HTTPS at the same time.

Use the **no http server** command with the **use-vrf** parameter to disable HTTP or HTTPS service and remove its association with the specified VRF. You can disable service for any VRF, including the management VRF. Disabling service for the management VRF is allowed, but removing the server's association with the management VRF is not allowed.

Use the **http server** command with the **shutdown** parameter to disable HTTP or HTTPS service on the management VRF. Use the **no http server** command with the **shutdown** parameter to re-enable HTTP or HTTPS service on management VRF.

HTTPS crypto certificates are required to enable HTTPS mode. HTTPS crypto certificates determine whether the service is HTTP or HTTPS.

Examples

The following example creates and enables HTTP or HTTPS service on a device and specifies using a user-defined VRF (myvrf).

```
device# configure terminal
device(config)# http server use-vrf myvrf
```

The following example disables HTTP or HTTPS service (or both HTTP and HTTPS services when both are enabled) on a device for a user-defined VRF.

```
device# configure terminal
device(config)# http server use-vrf myvrf shutdown
```

The following example enables HTTP or HTTPS service on an device for a user-defined VRF when service is disabled.

```
device# configure terminal
device(config)# no http server use-vrf myvrf shutdown
```

The following example disables HTTP or HTTPS service on a device for a user-defined VRF and removes its association with that VRF.

```
device# configure terminal
device(config)# no http server use-vrf myvrf
```

The following example disables HTTP or HTTPS service on a device for the management VRF.

```
device# configure terminal
device(config)# http server shutdown
```

The following example enables HTTP or HTTPS service on a device for the management VRF.

```
device# configure terminal
device(config)# no http server shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

import-map

Imports the target-VPN community.

Syntax

import-map *route-map*

no import-map *route-map*

Parameters

route-map

Specifies the route-map name .

Modes

VRF configuration mode

Usage Guidelines

The **no** form of the command to apply a route-map filter on the routes to be imported.

Examples

The following example shows how to import target-VPN community.

```
device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd 1:2
device#(config-vrf-vpn1)# vpn-statistics
device#(config-vrf-vpn1)# address-familin ipv4 unicast
device#(config-vrf-vpn1-ipv4-unicast)# route-target-import 100:1
device#(config-vrf-vpn1-ipv4-unicast)# import-map immport-route-map1

device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd 1:2
device#(config-vrf-vpn1)# vpn-statistics
device#(config-vrf-vpn1)# address-familin ipv6 unicast
device#(config-vrf-vpn1-ipv6-unicast)# route-target-import 100:1
device#(config-vrf-vpn1-ipv6-unicast)# import-map immport-route-map1
```

History

Release version	Command history
18x.1.00	This command was introduced.

inactivity-timer

Configures the time a forwarding entry can remain unused before the device deletes it.

Syntax

inactivity-timer *seconds*

no inactivity-timer *seconds*

Command Default

The default inactive time is 180 seconds.

Parameters

seconds

Specifies the time in seconds. The range is 60 through 3600 seconds. The default is 180 seconds.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the default inactive time, 180 seconds.

A device deletes a forwarding entry if the entry is not used to send multicast packets. The Protocol Independent Multicast (PIM) inactivity timer defines how long a forwarding entry can remain unused before the device deletes it.

Examples

This example configures an inactive time to 90 seconds.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# inactivity-timer 90
```

History

Release version	Command history
18x.1.00	This command was introduced.

install-igp-cost

Configures the device to use the IGP cost instead of the default BGP Multi-Exit Discriminator (MED) value as the route cost when the route is added to the Routing Table Manager (RTM).

Syntax

install-igp-cost

no install-igp-cost

Modes

BGP configuration mode

Usage Guidelines

By default, BGP uses the BGP MED value as the route cost when the route is added to the RTM. Use this command to change the default to the IGP cost.

The **no** form of the command restores the defaults.

Examples

The following example configures the device to compare MEDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# install-igp-cost
```

History

Release version	Command history
18x.1.00	This command was introduced.

instance

Maps a VLAN to a Multiple Spanning Tree Protocol (MSTP) instance. You can group a set of VLANs to an instance.

Syntax

instance *instance_id* [**vlan** *vlan_id* | **priority** *priority_id*]

no instance

Command Default

The priority value is 32768.

Parameters

instance_id

Specifies the MSTP instance. Valid values range from 1 through 31.

vlan *vlan_id*

Specifies the VLAN to map an MSTP instance. Refer to the Usage Guidelines.

priority *priority_id*

Specifies the priority for the specified instance. Valid values range from 0 through 61440. The priority values can be set only in increments of 4096.

Modes

Spanning tree MSTP configuration mode

Usage Guidelines

The following rules apply:

- VLANs must be created before mapping to instances.
- The VLAN instance mapping is removed from the configuration if the underlying VLANs are deleted.

Enter **no instance** to remove the VLAN mapping from the MSTP instance.

CAUTION
This command can be used only after the VLAN is defined.

Examples

To map a VLAN to an MTSP instance:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# instance 1 vlan 2,3
device(conf-mstp)# instance 2 vlan 4-6
device(conf-mstp)# instance 1 priority 4096
```

History

Release version	Command history
18x.1.00	This command was introduced.

interface (telemetry)

Configures the interfaces to be used in the data streaming profile.

Syntax

interface *interface-range*

no interface *interface-range*

Command Default

No interfaces are included with a profile.

Parameters

interface-range

Specifies the range of interfaces to be accessed by the streaming profile.

Modes

Telemetry profile configuration mode

Usage Guidelines

This command configures the interfaces for the interface streaming profile. Without this parameter configured, the profile has no effect.

To remove interfaces from a profile, use the **no** form of this command.

Examples

The following example configures the interfaces to be used in the interface streaming profile.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)# interface 1/2-3,2/1-3,3/6-9
```

History

Release version	Command history
18x.1.00	This command was introduced.

interface ethernet

Configures an Ethernet interface

Syntax

interface ethernet { *slot/port* }

Command Default

No Ethernet interface is configured.

Parameters

slot/port

Specifies a slot and port.

Modes

Global configuration mode

Examples

To configure interface Ethernet 1/1:

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

interface loopback

Configures a loopback interface.

Syntax

interface loopback *port_number*

no interface loopback *port_number*

Command Default

A loopback interface is not configured.

Parameters

port_number

Specifies the port number for the loopback interface. Range is 1 through 255.

Modes

Global configuration mode

Usage Guidelines

A loopback is a logical interface traditionally used to ensure stable routing operations.

Use the **no** form of this command to remove the specified loopback interface.

The following restrictions apply when the loopback interface is part of an active VXLAN overlay gateway. These restrictions are enforced to maintain consistency across the gateway.

- The loopback interface cannot be deleted.
- The IPv4 address cannot be changed.
- The VRF instance cannot be changed.

You must first use the **no activate** command in VXLAN overlay gateway configuration mode to modify the loopback interfaces. .

Use the **no** form of this command with a port parameter to remove the specified loopback interface.

Examples

The following example creates a loopback interface with a port number of 25.

```
device# configure terminal
device(config)# interface loopback 25
device(config-Loopback-25)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

interface port-channel

Configures a port-channel interface.

Syntax

interface port-channel { *number*]

no interface port-channel { *number*]

Command Default

No port-channel interface is configured.

Parameters

number

Specifies a port-channel. The range is from 1 through 64.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to disable the interface.

Examples

To configure a port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

interface ve

Configures a virtual Ethernet (VE) interface.

Syntax

interface ve *vlan_id*

no interface ve *vlan_id*

Parameters

vlan_id

Specifies the corresponding VLAN that must already be created before the VE interface can be created. Refer to the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

Before you can configure a VE interface, you must create a corresponding VLAN. The VE interface must use the corresponding VLAN ID.

Use the **no** form of this command to remove a specified VE interface.

Examples

The following example shows the steps needed to create a VE interface with the VLAN ID of 56. This example assumes that VLAN 56 has already been created.

```
device# configure terminal
device(config)# interface ve 56
device(config-Ve-56)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

interval

For an implementation of an event-handler profile, specifies the number of seconds between iterations of an event-handler action, if triggered.

Syntax

interval *seconds*

no interval

Command Default

Iterations occur with no interval between them.

Parameters

seconds

Specifies the number of seconds between iterations of an event-handler action, if triggered. Valid values are 0 or a positive integer.

Modes

Event-handler activation mode

Usage Guidelines

The **interval** command is effective only if the **iterations** value is non-zero.

The **no** form of this command resets the **interval** setting to the default 0 seconds.

Examples

The following example sets the number of iterations to 3 and specifies an interval of 10 seconds between each iteration.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# iterations 3
device(config-activate-eventHandler1)# interval 10
```

The following example resets **interval** to the default value of 0 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no interval
```

History

Release version	Command history
18x.1.00	This command was introduced.

interval (telemetry)

Configures the interval delay for telemetry data streaming.

Syntax

interval *seconds*

no interval

Command Default

For the **interface** profile-type, the default value is 30 seconds.

For the **system-utilization** profile-type, the default value is 60 seconds.

Parameters

seconds

Specifies the streaming interval. For the **interface** profile-type, values range from 10 through 3600 seconds, in five-second increments. For the **system-utilization** profile-type, values range from 60 through 14400 seconds, in five-second increments.

Modes

Telemetry profile configuration mode

Usage Guidelines

Use the **no interval** command to reset the interval to the default value.

Examples

Example of setting the interval in an interface configuration for an interface profile.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(interface-default_interface_statistics)# interval 2000
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip access-group

Applies rules specified in an IPv4 access control list (ACL) to traffic entering or exiting an interface.

Syntax

ip access-group *ACLname* { **in** | **out** }

no ip access-group *ACLname* { **in** | **out** }

Parameters

ACLname
Specifies the name of the standard or extended IPv4 access list.

in
Applies the ACL to incoming switched and routed traffic.

out
Applies the ACL to outgoing switched and routed traffic.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to apply an IPv4 ACL to one of the following interface types:

- User interfaces
  - Physical Ethernet interfaces
  - (Ingress only) Logical interfaces (LAGs)
  - Virtual Ethernet (VE) (attached to a VLAN or to a bridge domain)
- All supported management interfaces

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

You can apply a maximum of two ACLs to a management interface, as follows:

- One ingress IPv4 ACL
- One ingress IPv6 ACL

You can apply an ACL to multiple interfaces. And you can apply an ACL twice—ingress and egress—to a given user interface.

To remove an ACL from an interface, enter the **no** form of this command.

Examples

The following example applies an ingress IP ACL on an Ethernet interface:

```
device(config)# interface ethernet 0/2
device(conf-if-eth-0/9)# ip access-group ipacl2 in
```

The following example removes an ingress IP ACL from an Ethernet interface:

```
device(config)# interface ethernet 0/2
device(conf-if-eth-0/9)# no ip access-group ipacl2 in
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip access-list

Creates a standard or extended IPv4 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

ip access-list { **standard** | **extended** } *ACLname*

no ip access-list { **standard** | **extended** } *ACLname*

Parameters

standard | **extended**

Specifies one of the following types of access lists:

standard

Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

extended

Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

ACLname

Specifies an ACL name unique among all ACLs (Layer 2 and Layer 3). The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a–z, A–Z or 0–9. You can also use underscore (_) or hyphen (-) in an ACL name, but not as the first character.

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after:

- Applied to an interface, using the **{ ip | ipv6 | mac } access-group** command.
- Applied at device-level, using the **{ ip | ipv6 } receive access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

Examples

The following example creates an IPv4 standard ACL.

```
device# configure
device(config)# ip access-list standard stdACL3
```

The following example creates an IPv4 extended ACL.

```
device# configure terminal
device(config)# ip access-list extended extdACL5
```

The following example creates rules on an IPv4 standard ACL.

```
device# configure terminal
device(config)# ip access-list standard stdACL3
device(config-ipacl-std)# seq 5 permit host 10.20.33.4
device(config-ipacl-std)# seq 15 deny any
```

The following example deletes an IPv4 ACL.

```
device# configure
device(config)# no ip access-list standard stdACL3
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip address

Configures an IP address on an interface.

Syntax

ip address *ip-address/mask* **ospf-ignore**]]

Parameters

ip-address
Specifies the IP address.

mask
Specifies the mask for the associated IP subnet. Dotted-decimal notation is not supported. For non-loopback interfaces, valid values are from 1 through 31. For loopback interfaces, the only valid value is 32.

ospf-ignore
Disables adjacency formation with OSPF neighbors and disables advertisement of the interface to OSPF.

ospf-passive
Disables adjacency formation with OSPF neighbors but does not disable advertisement of the interface to OSPF.

Modes

Interface configuration mode

Management interface configuration mode

Usage Guidelines

- Use this command to configure a primary or secondary IP address for a specific interface. You can also use this command to prevent OSPF from running on specified subnets. Multiple primary IP addresses are supported on an interface.
- You can use this command to configure a primary or secondary IP address for a management interface.
- For a management interface, only one primary IP address is supported. Secondary IP addresses are not supported.
- A primary IP address cannot overlap with a previously configured IP subnet.
- A primary IP address must be configured before you configure a secondary IP address in the same subnet.
- To remove the configured static or DHCP address, enter **no ip address**. This resets the address to 0.0.0.0/0.
- The **no** form of the command removes a specific IP address from the interface.

Gateway IPs from multiple subnets (maximum of 32) can be configured for each FVG session. Multiple gateway IPs from the same subnet can be configured, but the number of FVG sessions for each interface remains one. A single RBridge becomes the ARP responder for all the gateway IPs configured for the session.

Multiple gateway IPs are supported only for IPv4.

All restrictions for configuring an FVG gateway applies to multiple gateway IP addresses as well. If IP conflicts are detected for any gateway IP configured on the session, the configuration is accepted with a RASLOG, but the session is invalidated until the conflict is resolved.

Periodic gratuitous address resolution protocol (GARP), if configured, would be sent out only for the first gateway address. When a session moves to Master, GARP is sent out for all Gateway IP addresses configured on the session.

When downgrading to earlier versions of Network OS, if multiple gateway IPs are present then all gateway IP configurations are removed after downgrade. If only one gateway IP present, then it is retained.

Examples

The following example configures a primary IP address on a specified Ethernet interface.

```
device(config)# interface ethernet 3/2
device(conf-if-eth-3/2)# ip address 10.1.1.1/24

device(config)# interface ethernet 3/2
device(conf-if-eth-3/2)# ip address 10.1.1.2/24 secondary
```

The following example configures a primary IP address on a management interface.

```
device(config)# interface Management 1/0
device(config-Management-1/0)# no ip address
device(config-Management-1/0)# ip address 10.1.1.2/24
```

Release version	Command history
18x.1.00	This command was introduced.

ip address (site)

Specifies the destination IPv4 address of a tunnel for a site in a VXLAN overlay gateway configuration.

Syntax

ip address *IPv4_address*

no ip address [*IPv4_address*]

Parameters

IPv4_address

Specifies the IPv4 address of the destination tunnel.

Modes

Site configuration mode

Usage Guidelines

The tunnel mode and the source IP address are derived from the parent overlay gateway.

To change an IP addresses, you must first remove the existing address, by means of the **no ip address** *IPv4_address* or the **no ip address** commands. This also deletes all tunnels to the site.

Only one IPv4 address is allowed. The following IPv4 addresses are not allowed:

- Broadcast addresses (0.0.0.0 through 0.255.255.255)
- Localhost loopback addresses (127.0.0.0 through 127.255.255.255)
- Multicast addresses (224.0.0.0 through 239.255.255.255)
- Reserved addresses (240.0.0.0 through 255.255.,255.255)

Examples

The following example configures an IPv4 address of a destination tunnel for the site.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-site-mysite)# ip address 10.11.12.13
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip anycast-address

Configures an anycast-gateway IPv4 address on an interface, which uses the gateway IPv4 address for the host.

Syntax

ip anycast-address { *IPv4-address*/ *mask* }

no ip anycast-address

Command Default

No address is configured.

Parameters

IPv4-address / *mask*
IPv4 address and mask.

Modes

interface configuration mode on a virtual Ethernet (VE) interface.

Usage Guidelines

An IPv4 and IPv6 anycast MAC address cannot be configured as the same MAC address.

Use the **no** form of this command to delete the configured IPv4 anycast address from the interface.

Examples

To configure an IPv4 address and mask on a virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# interface ve 10
device(config-Ve-10)# ip anycast-address 2.2.2.2/24
```

To confirm the configuration in the running configuration:

```
device# show running-config interface ve 10
!
ip snycast-address 2.2.2.2/24
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip arp inspection

Enables Dynamic ARP Inspection (DAI) on a VLAN.

Syntax

ip arp inspection

no ip arp inspection

Command Default

DAI is disabled.

Modes

VLAN configuration mode

Usage Guidelines

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

The **no** form of the command disables Dynamic ARP Inspection.

Examples

The following example applies ARP_ACL_01 to VLAN 200 and enables DAI.

```
device# configure terminal
device(conf)# vlan 200
device(conf-vlan-200)# ip arp inspection filter ARP_ACL_01
device(conf-vlan-200)# ip arp inspection
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip arp inspection filter

Applies an Address Resolution Protocol (ARP) ACL to a VLAN, which is one of the steps implementing Dynamic ARP Inspection (DAI) on a VLAN.

Syntax

ip arp inspection filter *ACL-name*

no ip arp inspection filter

Command Default

No ARP ACL is applied.

Parameters

ACL-name
Specifies which ACL is applied to the VLAN.

Modes

VLAN configuration mode

Usage Guidelines

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

The **no** form of the command removes the current ARP ACL from the VLAN.

Examples

The following example applies an ARP ACL named ARP_ACL_01 to VLAN 200.

```
device# configure terminal
device(conf)# vlan 200
device(conf-vlan-200)# ip arp inspection filter ARP_ACL_01
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip arp inspection trust

Configures an interface as trusted for all VLANs configured on it.

Syntax

ip arp inspection trust

no ip arp inspection trust

Command Default

The interface is untrusted.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is supported only on Layer 2 physical or port-channel interfaces.

On trusted interfaces, all incoming ARP packets are accepted.

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

The **no** form of this command configures the interface as untrusted.

Examples

The following example configures an Ethernet interface as trusted.

```
device# configure terminal
device(conf)# interface ethernet 0/1
device(conf-if-eth-0/1)# ip arp inspection trust
```

The following example configures a port-channel interface as untrusted.

```
device# configure terminal
device(conf)# interface port-channel 171
device(config-Port-channel-171)# no ip arp inspection trust
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip arp learn-any

Enables address-resolution protocol (ARP) learning from any ARP request.

Syntax

ip arp learn-any

no ip arp learn-any

Command Default

Default ARP learning

Modes

VE configuration mode

Usage Guidelines

This command is effective only on a Layer 3 interface.

This command enables learning from any ARP request (not necessarily targeted to my ip address).

To reset default ARP learning, use the **no** form of this command.

Examples

The following example enables learn-any on VE 100.

```
device# configure terminal
device(config)# interface ve 100
device(config-if-Ve-100)# ip arp learn-any
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip arp-aging-timeout

Sets how long a dynamic Address Resolution Protocol (ARP) entry stays in the ARP cache. The aging timer is reset each time an ARP reply is received.

Syntax

ip arp-aging-timeout *value*

no ip arp-aging-timeout

Command Default

ARP aging timeout is globally enabled and set to 25 minutes.

Parameters

value

Specifies how long an ARP entry stays in the ARP cache. Values range from 0 through 240 minutes.

Modes

Interface subtype configuration mode

Usage Guidelines

When the device places an entry in the ARP cache, the device also starts an aging timer for the entry. The aging timer ensures that the ARP cache does not retain learned entries that are no longer valid. An entry can become invalid when the device with the MAC address of the entry is no longer on the network.

The aging timer is reset each time an ARP reply is received.

Aging out affects dynamic (learned) entries only. Static entries do not age out.

You can modify the ARP aging timeout only at the interface level, but not at the global level.

To prevent entries from aging out, enter **ip arp-aging-timeout 0**.

The **no** form of the command restores the default aging timeout of 25 minutes.

Examples

The following command sets the ARP aging timeout to 100 minutes on an interface.

```
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# ip arp-aging-timeout 100
```

The following command restores the ARP aging timeout to the default value of 25 minutes on an interface.

```
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# no ip arp-aging-timeout
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip dhcp relay address

Configures the IP DHCP Relay on a Layer 3 interface.

Syntax

ip dhcp relay address *ip-addr* [**use-vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

use-vrf

Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

vrf-name

VRF name.

Modes

Interface configuration mode

Usage Guidelines

This command uses the IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

Enter the command while in interface configuration mode for a VE or Ethernet interface where you want to configure the IP DHCP Relay. Configure up to sixteen DHCP server IP addresses per interface.

Use the **no** version of this command to remove the IP DHCP relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

Examples

To configure an IP DHCP Relay address on a Ve interface:

```
device# config
device(config)# interface ve 100
device(config-Ve-100)# ip dhcp relay address 3.1.2.255 use-vrf blue
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip dhcp relay gateway address

Configures the IP DHCP Relay on a Layer 3 gateway interface.

Syntax

ip dhcp relay gateway address *ip-addr*

no ip dhcp relay gateway address *ip-addr*

Parameters

ip-addr

IPv4 gateway address of the DHCP server where the DHCP client requests are to be forwarded.

Modes

Interface configuration mode

Usage Guidelines

Use this command to configure the IP DHCP Relay on the switch Layer 3 gateway interface using the IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

Use the **no**version of this command to remove the IP DHCP Relay from the interface.

Examples

To configure an IP DHCP Relay address on an interface:

```
device(config)# interface ethernet 1/4

device(config-if-eth-1/4)# ip dhcp relay gateway 10.50.22.26
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip dns

Configures the Domain Name System (DNS) domain name and the primary and secondary name server IP addresses.

Syntax

ip dns { **domain-name** *domain-name* | **name-server** *ip-address-of-name-server* }

no ip dns { **domain-name** *domain-name* | **name-server** *ip_address_of_name_server* }

Parameters

domain-name *domain-name*
Specifies the DNS domain name.

name-server *ip-address-of-name-server*
Specifies the IP address of the name server. IPv6 and IPv4 addresses are supported.

Modes

Global configuration mode

Usage Guidelines

- Your first run of **ip dns name-server** specifies the default IP gateway address. Your second run of **ip dns name-server** specifies the secondary IP gateway address.
- Name servers can only be entered or removed one at a time. The newly entered name server will append to the existing name server.
- The **no** form of the command with the domain-name parameter disables IP directed broadcasts for a specific domain.
- The **no** form of the command with the name-server parameter deletes a name server definition.

Examples

The following example configures the DNS domain name and the primary name server IP address.

```
device(config)# ip dns domain-name mycompany.com
device(config)# ip dns name-server  10.70.20.1
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip icmp rate-limiting

Limits the rate at which IPv4 Internet Control Message Protocol (ICMP) messages are sent on a network.

Syntax

ip icmp rate-limiting *milliseconds*

no ip icmp rate-limiting

Command Default

This command is enabled on the management port, but is disabled on the front-end ports.

Parameters

milliseconds

Time interval per ICMP packet in milliseconds. The range is from 0 through 4294967295. The default is 1000.

Modes

Interface configuration mode

Usage Guidelines

This is an interface-specific configuration.

The **no** form of the command will revert to the default setting. Set the interval to 0 to disable IPv4 ICMP rate-limiting.

Examples

The following example enables IPv4 ICMP rate-limiting on an Ethernet interface.

```
device(config)# interface ethernet 3/5
device(conf-int-eth-3/5)# ip icmp rate-limiting 10000
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip icmp redirect

Enables IPv4 Internet Control Message Protocol (ICMP) Redirect messages, which request that packets be sent on an alternative route.

Syntax

ip icmp redirect

no ip icmp redirect

Command Default

This command is enabled on both the management port and on the front-end ports.

Modes

Interface configuration mode

Usage Guidelines

This is an interface-specific configuration.

The **no** form of the command disables IPv4 ICMP Redirect messages.

Examples

The following example enables IPv4 ICMP Redirect messages on an Ethernet interface.

```
device(config)# interface ethernet 2/5
device(conf-int-eth-2/5)# ip icmp redirect
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp immediate-leave

Removes a group from the IGMP table immediately following receipt of a Leave Group request.

Syntax

ip igmp immediate-leave

no ip igmp immediate-leave

Command Default

This command is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

This command treats an interface as if it had one multicast client, so that the receipt of a Leave Group request on the interface causes the group to be removed immediately from the multicast database.

Enter the **no** form of this command to restore the default behavior.

Examples

To configure an Ethernet interface to remove a group from the IGMP table immediately following receipt of a Leave Group request:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp immediate-leave
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp last-member-query-interval

Sets the IGMP last-member query interval for an interface.

Syntax

ip igmp last-member-query-interval *milliseconds*

no ip igmp last-member-query-interval

Command Default

See Parameters.

Parameters

milliseconds

Response time in milliseconds. Range is from 100 through 25500 milliseconds. The default is 1000.

Modes

Interface subtype configuration mode

Usage Guidelines

The last-member query interval is the time in seconds that the IGMP router waits to receive a response to a group-specific query message, including messages sent in response to a host-leave message.

Enter the **no** form of this command to restore the default.

Examples

To set the last-member query interval to 1500 milliseconds on an interface:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp last-member-query-interval 1500
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp query-interval

Sets the IGMP query interval for an interface.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval *seconds*

Command Default

See Parameters.

Parameters

seconds

Response time in seconds. Range is from 1 through 18000 seconds. The default is 125.

Modes

Interface subtype configuration mode

Usage Guidelines

The query interval is the amount of time between IGMP query messages sent by the device.

Enter the **no** form of this command to restore the default.

Examples

To set the query interval to 500 seconds on an interface:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp query-interval 500
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp query-max-response-time

Sets the maximum response time for IGMP queries for an interface.

Syntax

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Command Default

See Parameters.

Parameters

seconds

Response time in seconds. Range is from 1 through 25 seconds. The default is 10.

Modes

Interface subtype configuration mode

Usage Guidelines

When a host receives the query packet, it starts counting to a random value, less than the maximum response time. When this timer expires, the switch (host) replies with a report, provided that no other host from the same group has responded yet.

Enter the **no** form of this command to restore the default.

Examples

To set the maximum response time to 20 seconds:

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp query-max-response-time 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp router-alert-check-disable

Disables the snooping check for the presence of the router alert option.

Syntax

ip igmp router-alert-check-disable

no ip igmp router-alert-check-disable

Modes

Global configuration mode

Usage Guidelines

By default, IGMP snooping checks for the presence of the router alert option in the IP packet header of the IGMP message. Packets that do not include this option are dropped.

Examples

The following example disables the snooping router alert check globally.

```
device(config)# ip igmp router-alert-check-disable
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp snooping enable

Enables Internet Group Management Protocol (IGMP) snooping.

Syntax

ip igmp snooping enable

no ip igmp snooping enable

Modes

VLAN configuration mode

Usage Guidelines

IGMP snooping allows a network device to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

Enter **no ip igmp snooping enable** to disable snooping for a specific VLAN.

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp snooping fast-leave

Enables Internet Group Management Protocol (IGMP) snooping fast-leave processing for a VLAN. This allows the removal of an interface from the forwarding table without sending out group-specific queries to the interface.

Syntax

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Command Default

This command is disabled.

Modes

VLAN configuration mode.

Usage Guidelines

Enter **no ip igmp snooping fast-leave** to disable this function.

Examples

To enable snooping fast-leave for a specific VLAN:

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping fast-leave
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp snooping last-member-query-interval

Sets the IGMP snooping last member query interval value in milliseconds.

Syntax

ip igmp snooping last-member-query-interval *value*

no ip igmp snooping last-member-query-interval *value*

Command Default

The default is 1000 ms.

Parameters

value

Sets the value in milliseconds. The range is 100 to 25500 milliseconds.

Modes

VLAN configuration mode

Usage Guidelines

When a leave is received, a group-specific query is sent. Last member query interval configuration controls the time interval between last member queries sent.

Examples

The following example sets the IGMP snooping last member query interval.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping last-member-query-interval 2000
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp snooping mrouter interface

Configures a VLAN port member to be a multicast router interface.

Syntax

ip igmp snooping mrouter interface { **ethernet** *slot/port* | **port-channel** *interface number* }

no ip igmp snooping mrouter interface { **ethernet** *slot/port* | **port-channel** *interface number* }

Parameters

ethernet *slot/port*
Specifies a valid port number.

port-channel *number*
Specifies the interface is a port-channel. Valid values range from 1 through 6144.

Modes

VLAN configuration mode

Usage Guidelines

A multicast router interface faces toward a multicast router or other Internet Group Management Protocol (IGMP) querier.

The **no** form of this command removes the configured mrouter.

Examples

The following example configures a VLAN port member to be a multicast router interface.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping mrouter interface ethernet 1/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp snooping querier enable

Activates or deactivates the Internet Group Management Protocol (IGMP) snooping querier on a VLAN.

Syntax

ip igmp snooping querier enable

no ip igmp snooping querier enable

Command Default

IGMP snooping querier is disabled.

Modes

VLAN configuration mode

Usage Guidelines

Enter **no ip igmp snooping querier enable** to disable the IGMP snooping querier.

Examples

To enable the IGMP snooping querier on the VLAN:

```
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping querier enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp snooping query-interval

Sets the IGMP snooping query interval in seconds.

Syntax

ip igmp snooping query-interval *seconds*

no ip igmp snooping query-interval *seconds*

Command Default

The default is 125 seconds.

Parameters

seconds

Sets the IGMP snooping query interval in seconds. The range is 1-18000 seconds.

Modes

VLAN configuration mode

Usage Guidelines

The **ip igmp snooping query-interval** command allows you to modify the query interval, which specifies how often the SLX-OS device enabled for active IGMP snooping sends group membership queries.

Examples

The following example sets the IGMP snooping query interval.

```
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping query-interval 200
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp snooping query-max-response-time

Sets the IGMP snooping query maximum response time.

Syntax

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-response-time *seconds*

Command Default

The default is 10 seconds.

Parameters

seconds

Specifies the IGMP snooping query maximum response time in seconds. The range is 1 to 25 seconds.

Modes

VLAN configuration mode

Usage Guidelines

The IGMP snooping query maximum response time is the length of time in seconds that the device will wait for an IGMP (V1 or V2) response from an interface before concluding that the group member on that interface is down and removing it from the group.

Examples

The following example sets the IGMP snooping query max response time.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping query-max-response-time 15
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp snooping static-group

Configures an interface in a VLAN as a static member of a multicast group.

Syntax

ip igmp snooping static-group { *ip-address* } {**interface** *ethernet/port-channel* }

ip igmp snooping static-group { *ip-address* } {**interface** *ethernet/port-channel* }

Parameters

ip-address

Specifies the multicast address to be joined in the A.B.C.D format.

interface

Specifies the interface.

ethernet/port-channel

Specifies the interface type.

Modes

VLAN configuration mode

Usage Guidelines

A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive IGMP membership reports. If clients cannot send reports, you can configure a static group which applies to specific ports. The static group allows packets to be forwarded to the static group ports even though they have no client membership reports.

Examples

The following example sets the IGMP snooping static-group.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ip igmp snooping static-group 225.0.0.1 interface ethernet 6/15
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp ssm-map

Enables the IGMPv2 Source Specific Multicast mapping.

Syntax

ip igmp ssm-map [*ASCII string* | **enable** *source-address*]

no ip igmp ssm-map [*ASCII string* | **enable** *source-address*]

Parameters

ASCII string
Specifies the prefix list name.

enable*source-address*
Specifies the source address.

Modes

Global configuration mode

Router PIM configuration mode

Usage Guidelines

A prefix list is used for SSM mapping with permit clauses.

Use the **no** form of this command to disable SSM mapping.

Examples

The following example enables the SSM mapping for IGMPv2 and configures an SSM map at the global level.

```
device(config)# ip igmp ssm-map enable
device(config)# ip igmp ssm-map ssm-map-230-to-232 203.0.0.10
device(config)# ip igmp ssm-map ssm-map-233-to-234 204.0.0.10
```

The following example enables the SSM range configuration at the router PIM level.

```
device(config)# router pim
    device(config-pim-router)# ssm-enable range PL_ssm_range -230-to-234
```

The following example shows a prefix list configuration for the SSM range.

```
device(config)# ip prefix-list PL_ssm_range  seq 5 permit 230.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 231.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 232.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 233.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 234.0.0.0/8
```

The following example shows a prefix list configuration for an SSM map.

```
device(config)# ip prefix-list ssm-map-230-to-232 seq 5 permit 230.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 10 permit 231.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 15 permit 232.0.0.0/8

device(config)# ip prefix-list ssm-map-233-to-234 seq 5 permit 233.0.0.0/8
device(config)# ip prefix-list ssm-map-233-to-234 seq 10 permit 234.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 15 permit 232.0.0.0/8
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp static-group

Configures the IGMP static group membership entries for a specific interface.

Syntax

ip igmp static-group *A.B.C.D*

no ip igmp static-group *A.B.C.D*

Parameters

A.B.C.D

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses to be included in the multicast group.

Modes

Interface subtype configuration mode

Usage Guidelines

The **ip igmp static-group** command creates IGMP static group membership to test multicast forwarding without a receiver host. Traffic is forwarded to an interface without the need to receive membership reports from host members. Packets to the group are fast-switched out of a specific interface. Static group membership entries are automatically added to the IGMP cache and the PIM mcache table.

Examples

To create a static multicast group for an interface:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp static-group 225.0.0.10 interface ethernet 6/15
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip igmp version

Specifies the IGMP version on a device.

Syntax

ip igmp version *version-number*

no ip igmp version *version-number*

Command Default

IGMP Version 2 is enabled.

Parameters

version-number

Specifies the version number: 1, 2, or 3. Version 2 is the default.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command restores the default; IGMP Version 2 is enabled.

Examples

The following example, in interface configuration mode, enables IGMP Version 3 for a physical port.

```
device# configure terminal
device(config)# interface ethernet 1/1/5
device(config-if-1/1/5)# ip igmp version 3
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip interface loopback (overlay gateway)

Sets the loopback port number for the VXLAN overlay gateway.

Syntax

ip interface loopback *loopback_id*

no ip interface loopback *loopback_id*

Parameters

loopback_id

Specifies a loopback interface. Range is from 1 through 255.

Modes

Overlay gateway configuration mode

Usage Guidelines

Use the **no** form of this command to delete the interface from the gateway.

Examples

The following example configures a loopback interface to the overlay gateway instance.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# ip interface loopback 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip mtu

Sets the IP maximum transmission unit (MTU) globally or on an interface.

Syntax

ip mtu *size*

no ip mtu

Command Default

The default IP MTU size is 1500 bytes.

Parameters

size

Specifies the size of the IP MTU globally or the interface. Enter an integer from 1300 through 9194 bytes.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of the command reverts the MTU size to the default value.

Using the **no** form of this command in global configuration mode resets the default value on all interfaces except the interfaces that you manually configured with MTU values.

When you change the IP MTU size globally, the change is applied to all Ethernet and VE interfaces on the device. However, it does not change a configured interface MTU value. The configured interface value takes precedence over the configured global MTU value.

The **show running-config** command displays the the MTU size when it is not the default value. If you change the global MTU size and do not change the interface MTU size, the **show running-config** command does not display the global MTU value at the interface level.

If the interface is part of a VE, change the IPv4 MTU only at the VE interface and not at the physical port. All member ports of a VE inherit the VE-interface IPv4 MTU value.

Examples

The following example sets the IP MTU to 2000 bytes on the specified Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 2/9
device(conf-if-eth-2/9)# ip mtu 2000
```

The following example changes the IP MTU for a VE.

```
device# configure terminal
device(config)# interface ve 103
device(config-vif-103)# ip mtu 2000
```

The following example changes the IP MTU globally.

```
device(config)# ip mtu 2000
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf active

Sets a specific OSPF interface to active.

Syntax

ip ospf active

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **ip ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPF control packets.

Examples

The following example sets a specific OSPFv2 Ethernet interface to active.

```
device# configure termnial
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf active
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf area

Enables OSPFv2 on an interface.

Syntax

ip ospf area *area-id* | *ip-addr*

no ip ospf area

Command Default

Disabled.

Parameters

area-id

Area ID in decimal format. Valid values range from 1 through 2147483647.

ip-addr

Area ID in IP address format.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command disables OSPFv2 on the interface.

Examples

The following example enables a configured OSPFv2 area named 1 on a specific OSPFv2 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf area 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf auth-change-wait-time

Configures authentication-change hold time.

Syntax

ip ospf auth-change-wait-time *wait-time*

no ip ospf auth-change-wait-time

Command Default

Wait time is 300 seconds

Parameters

wait-time

Time before an authentication change takes place. Valid values range from 0 to 14400 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the authentication change hold time for the interface to which you are connected.

OSPFv2 provides graceful authentication change for the following types of authentication changes:

Changing authentication methods from one of the following to another of the following:

- Simple text password
- MD5 authentication
- No authentication

Configuring a new simple text password or MD5 authentication key.

Changing an existing simple text password or MD5 authentication key

The **no** form of the command resets the wait time to the default of 300 seconds.

Examples

The following example sets the wait time to 400 seconds on a specific OSPF virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf auth-change-wait-time 400
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf authentication-key

Configures simple password-based authentication for OSPF.

Syntax

ip ospf authentication-key *password*

no ip ospf authentication-key

Command Default

Authentication is disabled.

Parameters

password

OSPF processes *password* as a plain text password.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset simple password-based authentication on the OSPFv2 interface to which you are connected. The **no** form of the command disables OSPFv2 authentication.

Examples

The following example configures an authentication key for an OSPF virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf authentication-key morningadmin
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific OSPFv2 interface.

Syntax

ip ospf bfd

no ip ospf bfd

Modes

Interface subtype configuration mode

Usage Guidelines

BFD sessions are initiated only if BFD is also enabled globally using the **bfd** command in OSPF router configuration mode. If BFD is disabled using the **no bfd** command in OSPF router configuration mode, BFD sessions on specific OSPFv2 interfaces are deregistered.

The **no** form of the command removes all BFD sessions from a specified interface.

Examples

The following example enables BFD on an OSPF Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# ip ospf bfd
```

The following example disables BFD on an OSPF virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 24
device(config-if-ve-24)# no ip ospf bfd
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf cost

Configures cost for a specific interface.

Syntax

ip ospf cost *value*

no ip ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPFv2 cost on the interface. If the cost is not configured with this command, OSPFv2 calculates the value from the reference and interface bandwidths.

The **no** form of the command disables the configured cost.

Examples

The following example sets the cost to 520 on a specific Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ip ospf cost 520
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf database-filter

Configures filters for different types of outgoing Link State Advertisements (LSAs).

Syntax

ip ospf database-filter { **all-external** | **all-summary-external** { **allow-default-and-type-4** | **allow-default-out** | **out** } }

ip ospf database-filter all-out

no ip ospf database-filter all-external

no ip ospf database-filter all-out

no ip ospf database-filter all-summary-external

Command Default

All filters are disabled.

Parameters

all-external
Blocks all external LSAs.

all-summary-external
Blocks all summary (Type 3) and external (type 5) LSAs.

allow-default-and-type-4
Allows default-route LSAs and Type 4 LSAs, but block all other LSAs.

allow-default-out
Allows default-route LSAs, but block all other LSAs.

out
Filters outgoing LSAs.

all-out
Blocks all LSAs.

Modes

Interface subtype configuration mode

Usage Guidelines

By default, the device floods all outbound LSAs on all the OSPF interfaces within an area. You can configure a filter to block outbound LSAs on an OSPF interface. This feature is particularly useful when you want to block LSAs from some, but not all, of the interfaces attached to the area. When enabled, this command blocks the specified outgoing LSAs on the interface. Some cases where you might want to enable filters are:

- To control the information being advertised to the network.
- To use a passive router for debugging only.

The **no** form of the command disables configurations.

NOTE
You cannot block LSAs on virtual links.

Examples

The following example applies a filter to block flooding of all LSAs on a specific OSPF Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf database-filter all-out
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf dead-interval

Configures the neighbor dead interval, which is the number of seconds that a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ip ospf dead-interval *interval*

no ip ospf dead-interval

Command Default

The specified time period is 40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 65535 seconds. The default is 40.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to a value that is one fourth that of the new dead interval, unless the hello interval is also explicitly configured using the **ip ospf hello-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The **running-config** command displays only explicitly configured values of the hello interval, which means that a value that was automatically changed as the result of a dead-interval change is not displayed.

The **no** form of the command restores the default value.

Examples

The following example sets the dead interval to 200 on a specific OSPFv2 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf dead-interval 200
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf hello-interval

Configures the hello interval, which is the length of time between the transmission of hello packets that this interface sends to neighbor routers.

Syntax

ip ospf hello-interval *interval*

no ip ospf hello-interval

Command Default

The default value is 10 seconds.

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the hello interval, the dead interval is automatically changed to a value that is four times that of the new hello interval, unless the dead interval is also explicitly configured using the **ip ospf dead-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The **running-config** command displays only explicitly configured values of the dead interval, which means that a value that was automatically changed as the result of a hello-interval change is not displayed.

The **no** form of the command restores the default value.

Examples

The following example sets the hello interval to 50 on a specific OSPFv2 virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf hello-interval 50
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf ldp-sync

Enables Label Distribution Protocol (LDP) synchronization with OSPF and configures the hold down time interval for an interface.

Syntax

ip ospf ldp-sync { **disable** | **enable** }

no ip ospf ldp-sync enable

Command Default

Disabled.

Parameters

disable
: Disables LDP synchronization.

enable
: Enables LDP synchronization.

Modes

Interface subtype configuration mode

Examples

The following example enables LDP synchronization with OSPF for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf ldp-sync enable
```

The following example disables LDP synchronization with OSPF for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Looback-1)# ip ospf ldp-sync disable
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf md5-authentication

Configures MD5 password and authentication change hold time.

Syntax

ip ospf md5-authentication { **key-activation-wait-time** *wait-time* | **key-id** *id* **key** *password* }

no ip ospf md5-authentication key-id

Command Default

No authentication.

Parameters

key-activation-wait-time *wait-time*

Sets the time that OSPFv2 waits before activating a new MD5 key. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends use the newly configured MD5 Key. OSPFv2 packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation. Valid values range from 0 to 14400 seconds.

key-id

Sets MD5 key.

id

Identifies the MD5 key ID. Valid values range from 1 and 255.

key *password*

Specifies the MD5 authentication ID and sets a password.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the MD5 password and/or authentication change hold time on the interface to which you are connected.

By default, the authentication key is encrypted. If you want the authentication key to be in clear text, insert a 0 between authentication-key and string. The software adds a prefix to the authentication key string in the configuration. For example, the following portion of the code has the encrypted code "2".

Enter **no ip ospf md5-authentication key-id** to disable this configuration.

Examples

The following example sets the time that OSPFv2 waits before activating a new MD5 key to 240 seconds on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf md5-authentication key-activation-wait-time 240
```

The following example sets the MD5 key ID to 22 and a password “myospfpassword” on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf md5-authentication key-id 22 key myospfpassword
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

Command Default

Enabled

Modes

Interface subtype configuration mode

Usage Guidelines

In default operation, the IP MTU on both sides of an OSPFv2 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The **no** no form of the command disables MTU-match checking on a specific interface.

Examples

The following example disables MTU-match checking on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no ip ospf mtu-ignore
```

The following example enables MTU-match checking on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf mtu-ignore
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf network

Configures the network type for the interface. Point-to-point can support unnumbered links, which requires less processing by OSPF.

Syntax

ip ospf network { **broadcast** | **non-broadcast** | **point-to-point** }

no ip ospf network

Command Default

Network type is broadcast.

Parameters

broadcast
Network type is broadcast.

non-broadcast
Network type is non-broadcast. An interface can be configured to send OSPF traffic to its neighbor as unicast packets rather than multicast packets.

point-to-point
Network type is point-to-point.

Modes

Interface subtype configuration mode

Usage Guidelines

On a non-broadcast interface, the devices at either end of the interface must configure non-broadcast interface type and the neighbor IP address. There is no restriction on the number of devices sharing a non-broadcast interface.

To configure an OSPF interface as a non-broadcast interface, the feature must be enabled on a physical interface or a VE, following the **ip ospf area** statement, and then specify the IP address of the neighbor in the OSPF configuration. The non-broadcast interface configuration must be done on the OSPF devices at either end of the link.

The **no** form of the command removes the network-type configuration.

Examples

The following example configures an OSPFv2 point-to-point link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf network point-to-point
```

The following example configures an OSPFv2 broadcast link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf network broadcast
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf passive

Sets a specific OSPFv2interface to passive.

Syntax

ip ospf passive

no ip ospf passive

Command Default

All OSPF interfaces are active.

Modes

Interface subtype configuration mode

Usage Guidelines

Passive interfaces accept and process all OSPF protocol traffic, but they do not send any traffic.

You might want to set an interface to passive mode if:

- You are planning to use the router mostly for debugging purposes.
- The router is a stub and does not route traffic.

The **no** form of the command sets an interface back to active.

Examples

The following example sets a specific OSPFv2 Ethernet interface to passive.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf passive
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf priority

Configures priority for designated router (DR) election.

Syntax

ip ospf priority *value*

no ip ospf priority

Command Default

The default value is 1.

Parameters

value

Priority value. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

The OSPFv2 router assigned the highest priority becomes the designated router, and the OSPFv2 router with the second-highest priority becomes the backup router.

The **no** form of the command restores the default value.

Examples

The following example sets a priority of 10 for the OSPFv2 router that is connected to an OSPFv2 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf priority 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

Syntax

ip ospf retransmit-interval *interval*

no ip ospf retransmit-interval

Command Default

The interval is 5 seconds.

Parameters

interval

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command resets the retransmit interval to its default.

Examples

The following example sets the retransmit interval to 8 for all OSPFv2 devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf retransmit-interval 8
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv2 to send link-state update packets on the interface to which you are connected.

Syntax

ip ospf transmit-delay *value*

no ip ospf transmit-delay

Command Default

The transmit delay is set to 1 second.

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command restores the default value.

Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf transmit-delay 25
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip pim dr-priority

Configures the designated router (DR) priority on IPv4 interfaces.

Syntax

ip pim dr-priority *priority-value*

no ip pim dr-priority *priority-value*

Command Default

The default DR priority value is 1.

Parameters

priority-value

Specifies the DR priority value as an integer. The range is 0 through 65535.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command restores the default DR priority value, 1.

You must enable PIM globally before you enable it on an interface.

You can configure the **ip pim dr-priority** command in either Dense mode (DM) or Sparse mode (SM).

If more than one device has the same DR priority on a subnet (as in the case of default DR priority on all), the device with the numerically highest IP address on that subnet is elected as the DR.

The DR priority information is used in the DR election only if all the PIM devices connected to the subnet support the DR priority option. If at least one PIM device on the subnet does not support this option, the DR election falls back to the backwards compatibility mode in which the device with the numerically highest IP address on the subnet is declared the DR regardless of the DR priority values.

Examples

This example configures a DR priority value of 50.

```
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip pim dr-priority 50
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip pim snooping enable

Enables IP PIM snooping on a VLAN.

Syntax

ip pim snooping enable

no ip pim snooping enable

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command disables PIM snooping on the VLAN.

Use this command to enable Layer 2 PIM snooping on a VLAN. You must enable IGMP snooping on the interface before enabling PIM snooping.

Examples

The following example enables PIM snooping on a VLAN.

```
device(config)# vlan 1
device(config-vlan-1)# ip pim snooping enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip pim-sparse

Enables or disables Protocol Independent Multicast Sparse Mode on port channels, physical or VE interfaces.

Syntax

ip pim-sparse

no ip pim-sparse

Command Default

Protocol Independent Multicast (PIM) is not enabled on an interface.

Modes

Interface subtype configuration mode

Usage Guidelines

PIM must be enabled on the device before enabling PIM-sparse. PIM-sparse can be enabled on interfaces

Enter **no ip pim-sparse** to disable this feature.

Examples

To enable PIM Sparse Mode on a virtual Ethernet (VE) interface:

```
device(config)# int ve 1
device(config-if-Ve-1)# ip pim-sparse
```

To enable PIM Sparse Mode on a router port:

```
device(config)# int eth 1/1
device(config-if-eth-1/1)# ip pim-sparse
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip pim ttl-threshold

Sets the IP PIM time to live (TTL) threshold.

Syntax

ip pim ttl-threshold *value*

no ip pim ttl-threshold

Command Default

The default value is 1.

Parameters

priority value

Specifies the TTL threshold value. The range is 1 to 64.

Modes

Interface configuration mode

Usage Guidelines

The TTL threshold defines the minimum value required in a packet for it to be forwarded out of the interface after the TTL has been decremented.

For example, if the TTL for an interface is set at 10, only those packets that enter with a TTL value of 11 or more are forwarded through the TTL-10 interface. With a default TTL threshold of 1, only packets ingressing with a TTL of 2 or greater are forwarded. The TTL threshold only applies to routed interfaces and is ignored by switched interfaces. Possible TTL values are 1 to 64. The default TTL value is 1.

The **no** form of the command restores the default TTL threshold 1.

Examples

The following example sets the TTL value.

```
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# ip pim ttl-threshold 50
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip port (Telemetry)

Designates the IPv4 port used for telemetry collection.

Syntax

ip { *ipv4_address* **port** *port_number* } [**transport** [**tcp** | **ssl**]]

no ip { *ipv4_address* **port** *port_number* }

Command Default

The default transport protocol is TCP.

Parameters

ipv4_address
The IPv4 address for the collector

port *port_number*
The

transport
Designates the transprt protocol. The default protocol is TCP.

tcp
Standard TCP protocol.

ssl
For secure transport use the SSL transport protocol

Modes

Telemetry collector configuration mode

Usage Guidelines

Use the **no ip** command to remove the port designation from the telemetry collector.

.

Examples

Example configuring the telemetry for secure transport.

```
device# configure terminal
Entering configuration mode terminal
device(config)# telemetry collector collector_1
device(config-telemetry-collector_collector_1)# ip 10.168.112.10 port 1 transport ssl
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip policy route-map

Enables policy-based routing (PBR).

Syntax

ip policy route-map *map-name*

no ip policy route-map *map-name*

Command Default

PBR is not enabled.

Parameters

map-name

Specifies the name of the route map.

Modes

Interface configuration mode

Virtual interface configuration mode

Usage Guidelines

The **no** form of the command disables PBR.

Examples

The following example enables PBR on a specific interface.

```
device# configure terminal
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# match ip address acl 99
device(config-route-map-test-route/permit/99)# set ip next-hop 192.168.3.1
device(config-route-map-test-route/permit/99)# exit
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip policy route-map test-route
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip proxy-arp

Enables Proxy Address Resolution Protocol (APR) on an interface.

Syntax

ip proxy-arp

no ip proxy-arp

Command Default

Proxy ARP is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Proxy ARP enables a device to answer ARP requests from devices in one network on behalf of devices in another network. Because ARP requests are MAC-layer broadcasts, they reach only the devices that are directly connected to the sender of the ARP request. Therefore, ARP requests do not cross routers.

The **no** form of the command disables Proxy ARP on an interface.

Examples

The following example enables Proxy ARP on a specified interface.

```
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# ip proxy-arp
```

The following example disables Proxy ARP on a specified interface.

```
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# no ip proxy-arp
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip receive access-group

Applies an IPv4 access control list (ACL) at global configuration level. Such *receive-path ACLs* filter incoming route-processor traffic according to rules that you create, but do not filter data-path traffic.

Syntax

ip receive access-group *acl-name*

no ip receive access-group *acl-name*

Command Default

No receive-path ACLs are applied.

Parameters

acl-name
Specifies the name of the standard or extended IP access list.

Modes

Global configuration mode

Usage Guidelines

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny/hard-drop rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL—from an interface-subtype configuration mode—you use the { **ip** | **ipv6** | **mac** } **access-group** command.
- To apply a receive-path ACL—from global configuration mode—you use the { **ip** | **ipv6** } **receive access-group** command.

You can apply a maximum of two receive-path ACLs to a device, as follows:

- One IPv4 receive-path ACL
- One IPv6 receive-path ACL

To remove a receive-path ACL, enter the **no** form of this command.

Examples

The following example creates an IPv4 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ip access-list extended ipv4-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20.0.0.1 count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq bgp count

device(conf-ipacl-ext)# exit
device(config)# ip receive access-group ipv4-receive-acl-example
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip route

Adds a static route to the IP routing table.

Syntax

ip route *dest-ip-addr* [**next-hop-vrf** *next-vrf-name*] *next-hop-address* [*metric*] [**distance** *distance*] [**tag** *tag-number*]

ip route *dest-ip-addr* { **ethernet** *slot/port* | **ve** *ve-number*} [*metric*] [**distance** *distance*] [**tag** *tag-number*]

ip route *dest-ip-addr* **null 0** [*metric*] [**distance** *distance*] [**tag** *tag-number*]

no ip route *dest-ip-addr* [**next-hop-vrf** *next-vrf-name*] *next-hop-address* [*metric*] [**distance** *distance*] [**tag** *tag-number*]

no ip route *dest-ip-addr* { **ethernet** *slot/port* | **ve** *ve-number*} [*metric*] [**distance** *distance*] [**tag** *tag-number*]

no ip route *dest-ip-addr* **null 0** [*metric*] [**distance** *distance*] [**tag** *tag-number*]

Parameters

next-hop-vrf *vrf-name*
Specifies the name of the non-default VRF to be used for as the next-hop gateway.

dest-ip-addr
Specifies the destination IPv4 address and mask in the format A.B.C.D/L (where "L" is the prefix length of the mask).

next-hop-addr
Specifies the IPv4 address of the next hop.

ethernet *slot/port*
Specifies the destination Ethernet port.

next-hop-vrf *next-vrf-name*
VRF name of next hop.

ve *vlan-id*
Specifies the outgoing interface type as VE.

null 0
Configures the Layer 3 switch to drop IP packets to a specific network or host address by configuring a "null" (sometimes called "null0") static route for the address.

metric
Specifies the cost metric of the route. Valid values range from 1 through 16. The default is 1.

distance *distance*
Specifies the administrative distance of the route. When comparing otherwise equal routes to a destination, an SLX-OS device prefers lower administrative distances over higher ones. Valid values range from 1 through 254. The default is 1.

tag *tag-number*
Specifies the tag value of the route to use for route filtering with a route map. Valid values range from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command followed by the route identifier removes a static route.

If you do not want to specify a next-hop IP address, you can instead specify a physical or virtual interface on the SLX-OS device. If you specify an Ethernet port, the device forwards packets destined for the static route's destination network to the specified interface. Conceptually, this feature makes the destination network like a directly connected network, associated with an SLX-OS device interface.

The port or virtual interface you use for the static route's next hop must have at least one IP address configured on it. The address does not need to be in the same subnet as the destination network.

For a default route, use the following as the destination IP address 0.0.0.0/0.

You can create a null route for traffic for traffic that should not be forwarded. To create a null route, use the key phrase **null 0** as the next hop.

Examples

The following example configures a static route to 10.95.7.0 addresses, using 10.95.6.157 as the next-hop gateway.

```
device(config)# ip route 10.95.7.0/24 10.95.6.157
```

The following example configures a default route to next-hop IP address 10.24.4.1.

```
device(config)# ip route 0.0.0.0/0 10.24.4.1
```

The following example configures a static route with an Ethernet interface as the destination.

```
device(config)# ip route 192.128.2.69/24 ethernet 4/1
```

The following example configures a null static route to drop packets destined for network 10.157.22.x.

```
device(config)# ip route 10.157.22.0/24 null 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip router-id

Changes the router ID that is already in configured.

Syntax

ip router-id *A.B.C.D*

no ip router-id *A.B.C.D*

Parameters

A.B.C.D

Specifies the IPv4 address that you want as the router ID.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Though a device has IP addresses assigned to various interfaces, some routing protocols identify the device by the router ID rather than the IP addresses assigned to the interfaces connected by the protocol.

The **no** form of the command removes the configured router ID and restores the default router ID.

Examples

The following example specifies the router ID as 192.158.1.2.

```
device# configure terminal
device(config)# ip router-id 192.158.1.2
```

History

Release version	Command history
18x.1.00	This command was introduced.

ip vrrp-extended auth-type

Configures the type of authentication used on a Virtual Router Redundancy Protocol Extended (VRRP-E) interface.

Syntax

ip vrrp-extended auth-type md5-auth *auth-text*

no ip vrrp-extended auth-type md5-auth

Command Default

No authentication is configured for a VRRP-E interface.

Parameters

auth-type
Authentication type used to verify the *password*.

md5-auth *auth-text*
Configures MD5 authentication on the interface. The maximum length of the text string is 64 characters.

Modes

Virtual Ethernet (VE) interface configuration mode

Usage Guidelines

This configuration is for VE interfaces only.

If the **md5-auth** option is configured, syslog and SNMP traps are generated if a packet is being dropped due to MD5 authentication failure. Using MD5 authentication implies that the software does not need to run checksum verification on the receiving device and can rely on the authentication code (message digest 5 algorithm) to verify the integrity of the VRRP-E message header.

The **no** form of this command removes the VRRP-E authentication from the interface.

Examples

The following example configures MD5 authentication on VE interface 20.

```
device(config)# protocol vrrp-extended
device(config)# interface ve 20
device(config-if-Ve-20)# ip vrrp-extended auth-type md5-auth lyk28d3j
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 access-group

Applies rules specified in an IPv6 access control list (ACL) to traffic entering an interface.

Syntax

ipv6 access-group *ACLname* **in**

no ipv6 access-group *ACLname* **in**

Parameters

ACLname
Specifies the name of the standard or extended IPv6 access list.

in
Applies the ACL to incoming switched and routed traffic.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to apply an IPv6 ACL to one of the following interface types:

- User interfaces
  - (Ingress only) Logical interfaces (LAGs)
  - Logical interfaces (LAGs)
  - Virtual Ethernet (VE) (attached to a VLAN or to a bridge domain)
- All supported management interfaces

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

You can apply a maximum of two ACLs to a management interface, as follows:

- One ingress IPv4 ACL
- One ingress IPv6 ACL

You can apply an ACL to multiple interfaces.

To remove an ACL from an interface, enter the **no** form of this command.

Examples

The following example applies an IPv6 ACL on an Ethernet interface to incoming traffic.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# ipv6 access-group ipv6_acl_7 in
```

The following example removes an IPv6 ACL from an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no ipv6 access-group ipv6_acl_7 in
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 access-list

Creates a standard or extended IPv6 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

ipv6 access-list { **standard** | **extended** } *ACLname*

no ipv6 access-list { **standard** | **extended** } *ACLname*

Parameters

standard | **extended**

Specifies one of the following types of access lists:

standard

Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

extended

Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

ACLname

Specifies an ACL name unique among all ACLs (Layer 2 and Layer 3). The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a–z, A–Z or 0–9. You can also use underscore (_) or hyphen (-) in an ACL name, but not as the first character.

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after:

- Applied to an interface, using the **{ ip | ipv6 | mac } access-group** command.
- Applied at device-level, using the **{ ip | ipv6 } receive access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

Examples

The following example creates an IPv6 standard ACL:

```
device# configure
device(config)# ipv6 access-list standard stdV6ACL1
```

The following example creates an IPv6 extended ACL:

```
device# configure
device(config)# ipv6 access-list extended ipv6_acl_1
```

The following example creates rules on an IPv6 standard ACL:

```
device# configure
device(config)# ipv6 access-list standard stdV6ACL1
device(conf-ipv6-std)# seq 10 permit 2001:db8:85a3:0:0:8a2e:370:7334
device(conf-ipv6-std)# seq 11 deny any
```

The following example deletes an IPv6 ACL:

```
device# configure
device(config)# no ipv6 access-list standard stdV6ACL1
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 address

Configure an IPv6 address for an interface.

Syntax

ipv6 address *pv6-prefix//prefix-length* [**secondary**] [**anycast** | **eui-64**]

no ipv6 address *pv6-prefix//prefix-length* [**secondary**] [**anycast** | **eui-64**]

ipv6 address *ipv6-address* **link-local**

no ipv6 address *ipv6-address* **link-local**

Parameters

ipv6-address
Specifies the IPv6 address.

ipv6-prefix
Specifies the IPv6 prefix address in this format: X:X::X:X/M.

prefix-length
A decimal value specifying the length of the IPv6 prefix.

secondary
Specifies that the address is a secondary address. A maximum of 256 secondary addresses can be configured.

anycast
Configures an address as an anycast address.

eui-64
Configures the global address with an EUI-64 interface ID in the low-order 64 bits. The interface ID is automatically constructed in IEEE EUI-64 format using the interface's MAC address.

Modes

Interface configuration mode

Usage Guidelines

A secondary address cannot be configured on an interface unless the primary address is configured first.

The primary address cannot be deleted on an interface unless the secondary addresses are deleted first.

This command is not supported on loopback or management interfaces.

Examples

This example shows how to configure a primary, secondary global, or unique local IPv6 unicast address, including a manually configured interface ID:

```
device(config)# configure terminal
device(config)# interface ethernet 3/1
device(conf-if-eth-2/3)# ipv6 address 2001:db8:12d:1300:240z:d0ff:fe48:4672/64
```

This example shows how to remove the IPv6 unicast address, including a manually configured interface ID from an interface:

```
device(conf-if-eth-2/3)# no ipv6 address 2001:db8:12d:1300:240z:d0ff:fe48:4672/64
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 anycast-address

Configures an anycast-gateway IPv6 address on an interface, which uses the gateway IPv6 address for the host.

Syntax

ipv6 anycast-address { *IPv6-address*/ *mask* }

no ipv6 anycast-address

Command Default

No address is configured.

Parameters

IPv6-address / *mask*
IPv6 address and mask.

Modes

interface configuration mode on a virtual Ethernet (VE) interface.

Usage Guidelines

An IPv4 and IPv6 anycast MAC address cannot be configured as the same MAC address.

Use the **no** form of this command to delete the configured IPv6 anycast address from the interface.

Examples

To configure an IPv6 address and mask on a virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# interface ve 10
device(config-Ve-10)# ipv6 anycast-address fe80::1234/64
```

To confirm the configuration in the running configuration:

```
device# show running-config interface ve 10
!
ipv6 snycast-address fe80::1234/64
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 dhcp relay address

Configures the IPv6 DHCP Relay address on a Layer 3 interface.

Syntax

ipv6 dhcp relay address *ipv6-addr* [**interface** *interface-type interface-name*] [**use-vrf** *vrf-name*]

no ipv6 dhcp relay address *ipv6-addr* [**interface** *interface-type interface-name*] [**use-vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of the DHCP server where the DHCP client requests are to be forwarded.

interface
This parameter specifies the outgoing interface, used when the relay address is a link-local or multicast address

interface-type
The type of interface - Ethernet or VE.

interface-name
The interface name or Ve ID.

use-vrf
Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

vrf-name
VRF name.

Modes

Interface subtype configuration mode

Usage Guidelines

This command uses the IPv6 address of the DHCP server where the DHCP client requests are to be forwarded. You can configure the address on a virtual Ethernet (VE) or an Ethernet interface. You can configure up to 16 relay destination addresses on an interface.

Enter the command while in interface subtype configuration mode for a VE or Ethernet interface where you want to configure the IPv6 DHCP Relay. Use the **no** version of this command to remove the IPv6 DHCP Relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

If the relay address is a link local address or a multicast address, an outgoing interface must be configured for IPv6 relay to function. In instances where the server address is relayed to a different VRF compared to a client connected interface VRF, in addition to the relay address, you must also specify the user-vrf, otherwise IPv6 relay may not function correctly. IPv6 route leaking is also required for IPv6 reachability.

The **no** form of the command deletes the IPv6 DHCP Relay address from the interface.

Examples

To configure an IPv6 DHCP Relay address on a Ve interface:

To configure an IPv6 DHCP Relay address on an interface:

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 dns

Configures the DNS domain name and the primary and secondary name-server IPv6 addresses.

Syntax

ipv6 dns { **domain-name** *domain_name* | **name-server** *name_server* }

no ipv6 dns { **domain-name** *domain_name* | **name-server** *name_server* }

Parameters

domain-name *domain_name*
Specifies the DNS domain name.

name-server *name_server*
Specifies the IPv6 address of the primary and secondary name servers. Both the IPv6 and IPv4 addresses are supported.

Modes

Global configuration mode

Usage Guidelines

Your first run of **ipv6 dns name-server** specifies the default IP gateway address. Your second run of **ipv6 dns name-server** specifies the secondary IP gateway address.

Name servers can only be entered or removed one at a time. The newly entered name server will append to the existing name server.

To disable IP directed broadcasts for a specific domain, enter **no ipv6 dns domain-name** *domain_name*.

To delete a name-server definition, enter **no ipv6 dns name-server** *ipv6_address_of_name_server*.

Examples

The following example configures DNS.

```
device(config)# ipv6 dns domain-name mycompany.com
device(config)# ipv6 dns name-server 2001:db8:12d:1300:240z:d0ff:fe48:4672
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 icmpv6 rate-limiting

Limits the rate at which IPv6 Internet Control Message Protocol version 6 (ICMPv6) messages are sent on a network.

Syntax

ipv6 icmpv6 rate-limiting *milliseconds*

no ipv6 icmpv6 rate-limiting

Command Default

This command is enabled on the management port and on the front-end ports.

Parameters

milliseconds

Time interval per ICMP packet. The range is from 1 through 4294967295 milliseconds. The default is 1000 milliseconds.

Modes

Interface configuration mode

Usage Guidelines

This is an interface-specific configuration.

The **no** form of this command reverts the rate limiting to the default settings.

Set the rate limiting to 0 to disable icmpv6 rate limiting.

Examples

The following example enables IPv6 ICMP rate-limiting on an Ethernet interface.

```
device(config)# interface ethernet 3/5
device(conf-int-eth-3/5)# ipv6 icmpv6 rate-limiting
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 mtu

Sets the IPv6 maximum transmission unit (MTU) on a specified interface.

Syntax

ipv6 mtu *size*

no ipv6 mtu

Command Default

IPv6 MTU size is 1500 bytes.

Parameters

size

Specifies the size of an interface IPv6 MTU. The range is from 1300 through 9216 bytes.

Modes

Interface configuration mode

Usage Guidelines

If the interface is part of a VE, change the IPv6 MTU only at the VE interface and not at the physical port. All member ports of a VE inherit the VE-interface IPv6 MTU value.

Use the **no ipv6 mtu** command to revert the IPv6 MTU size to the default value.

Examples

On a specified Ethernet interface, the following example sets the IPv6 MTU to 2000 bytes.

```
device# configure terminal
device(config)# interface ethernet 2/9
device(conf-if-eth-2/9)# ipv6 mtu 2000
```

The following example changes the IPv6 MTU for a VE.

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 nd cache expire

Configures the time interval after which the Neighbor Discovery cache is deleted or refreshed.

Syntax

ipv6 nd cache expire *seconds*

no ipv6 nd cache expire *seconds*

Command Default

Default expiration time is 1500 seconds.

Parameters

seconds

Specifies how long an entry stays in the Neighbor Discovery cache. The range is from 30 through 14400 seconds. The default is 1500.

Modes

Interface subtype configuration mode

Usage Guidelines

Cache entries expire and are deleted if they remain in a "stale" state as defined by *seconds*.

You can modify the ND expiration time only at the interface level, but not at the global level.

The **no** form of this command restores the default aging timeout of 1500 seconds.

Examples

The following example sets the Neighbor Discovery expiration time to 2500 seconds on an Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/2
conf-if-eth-0/2)# ipv6 nd cache expire 2500
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf active

Sets a specific OSPFv3 interface to active.

Syntax

ipv6 ospf active

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **ipv6 ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPFv3 control packets.

Examples

The following example sets a specific OSPFv3 Ethernet interface to active.

```
device# configure termnial
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf active
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf area

Enables OSPFv3 on an interface.

Syntax

ipv6 ospf area *area-id* | *ip-addr*

no ipv6 ospf area

Command Default

OSPFv3 is disabled.

Parameters

area-id

Area ID in dotted decimal or decimal format.

ip-addr

Area ID in IP address format.

Modes

Interface subtype configuration mode

Usage Guidelines

This command enables an OSPFv3 area on the interface to which you are connected.

The **no** form of the command disables OSPFv3 on this interface.

Examples

The following example enables a configured OSPFv3 area named 0 on a specific OSPFv3 Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf authentication ipsec

Specifies IP security (IPsec) as the authentication type for an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec key-add-remove-interval *interval*

no ipv6 ospf authentication ipsec key-add-remove-interval *interval*

Command Default

Disabled.

Parameters

key-add-remove-interval *interval*

Specifies the OSPFv3 authentication key add-remove interval. Valid values range from decimal numbers 0 through 14400. The default is 300.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command removes IPsec authentication from the interface.

Examples

The following example enables IPsec on a specified OSPFv3 Looback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
device(config-Loopback-1)# ipv6 ospf authentication ipsec
```

The following example sets the OSPFv3 authentication key add-remove interval to 480.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
device(config-Loopback-1)# ipv6 ospf authentication ipsec key-add-remove-interval 480
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf authentication ipsec disable

Disables IP security (IPsec) services on an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec disable

no ipv6 ospf authentication ipsec disable

Command Default

Authentication is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to disable IPsec if it is enabled on the interface. Packets that are sent out will not be IPSec encapsulated and the received packets which are IPSec encapsulated will be dropped.

The **no** form of the command re-enables IPSec on the interface if IPsec is already configured on the interface.

Examples

The following example disables IPsec on a specific OSPFv3 interface where IPsec is already enabled.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf authentication ipsec disable
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf authentication spi

Specifies the security policy index (SPI) value for an OSPFv3 interface.

Syntax

ipv6 ospf authentication spi *spi* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** *key* }

no ipv6 ospf authentication spi

Command Default

Disabled.

Parameters

spi
SPI value. Valid values range from decimal numbers 512 through 4294967295.

ah
Specifies Authentication Header (ah) as the protocol to provide packet-level security.

esp
Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null
Specifies that the ESP payload is not encrypted.

hmac-md5
Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPFv3 interface.

hmac-sha1
Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPFv3 interface.

key
Number used in the calculation of the message digest.

key
The 40 hexadecimal character key.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 ospf authentication spi** *spi* to remove the SPI value from the interface.

Examples

The following example enables ESP and HMAC-SHA-1 on a specified OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf area 0
device(conf-if-eth-1/1)# ipv6 ospf authentication spi 512 esp null hmac-sha1 key
abcef12345678901234fedcba098765432109876
```

The following example enables HA and HMAC-MD5 on a specified OSPFv3 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf area 0
device(config-if-Ve-1# ipv6 ospf authentication spi 750 ha hmac-md5 key
abcef12345678901234fedcba098765432109876
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific OSPFv3 interface.

Syntax

ipv6 ospf bfd

no ipv6 ospf bfd

Modes

Interface subtype configuration mode

Usage Guidelines

BFD sessions are initiated only if BFD is also enabled globally using the **bfd** command in OSPFv3 router configuration mode. If BFD is disabled using the **no bfd** command in OSPFv3 router configuration mode, BFD sessions on specific interfaces are deregistered.

The **no** form of the command removes all BFD sessions from a specified interface.

Examples

The following example enables BFD on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# ipv6 ospf bfd
```

The following example disables BFD on an OSPFv3 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 24
device(config-if-Ve-24)# no ipv6 ospf bfd
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf cost

Configures cost for a specific OSPFv3 interface.

Syntax

ipv6 ospf cost *value*

no ipv6 ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPFv3 cost on the interface. If the cost is not configured with this command, OSPFv3 calculates the value from the reference and interface bandwidths.

For more information, refer to the **auto-cost reference-bandwidth** command.

The **no** form of the command disables the configured cost.

Examples

The following example sets the cost to 620 on a specific OSPFv3 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf cost 620
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf dead-interval

Specifies the time period for which a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ipv6 ospf dead-interval *interval*

no ipv6 ospf dead-interval

Command Default

The specified time period is 40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 65535 seconds. The default is 40.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to a value that is one fourth that of the new dead interval, unless the hello interval is also explicitly configured using the **ipv6 ospf hello-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The **running-config** command displays only explicitly configured values of the hello interval, which means that a value that was automatically changed as the result of a dead-interval change is not displayed.

The **no** form of the command restores the default value.

Examples

The following example sets the dead interval to 80 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf dead-interval 80
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf hello-interval

Sets the length of time between the transmission of hello packets that an interface sends to neighbor routers.

Syntax

ipv6 ospf hello-interval *interval*

no ipv6 ospf hello-interval

Command Default

The length of time between the transmission of hello packets is set to 10 seconds.

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535 seconds. The default is 10.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the hello interval, the dead interval is automatically changed to a value that is four times that of the new hello interval, unless the dead interval is also explicitly configured using the **ipv6 ospf dead-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The **running-config** command displays only explicitly configured values of the dead interval, which means that a value that was automatically changed as the result of a hello interval change is not displayed.

The **no** form of the command restores the default value.

Examples

The following example sets the hello interval to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf hello-interval 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf hello-jitter

Sets the allowed jitter between HELLO packets.

Syntax

ipv6 ospf hello-jitter *interval*

no ipv6 ospf hello-jitter

Command Default

10%

Parameters

jitter

Allowed interval between hello packets.Valid values range from 1 through 50 percent (%).

Modes

Interface subtype configuration mode

Usage Guidelines

The hello interval can vary from the configured hello-interval to a maximum of percentage value of configured jitter.

Examples

The following example sets the hello jitter to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf hello-jitter 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf instance

Specifies the number of OSPFv3 instances running on an interface.

Syntax

ipv6 ospf instance *instanceID*

no ipv6 ospf instance

Parameters

instanceID

Instance identification number. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command restores the default value.

Examples

The following example sets the number of IPv6 OSPF instances to 35 on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf instance 35
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Command Default

Enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

In default operation, the IP MTU on both sides of an OSPFv3 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The **no** no form of the command disables MTU-match checking on a specific interface.

Examples

The following example disables MTU-match checking on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no ipv6 ospf mtu-ignore
```

The following example disables MTU-match checking on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf mtu-ignore
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf network

Configures network type.

Syntax

ipv6 ospf network { **broadcast** | **point-to-point** }

no ipv6 ospf network

Command Default

Network type is broadcast.

Parameters

broadcast

Network type is broadcast, such as Ethernet.

point-to-point

Network type is point-to-point.

Modes

Interface subtype configuration mode

Usage Guidelines

Point-to-point can support unnumbered links, which requires less processing by OSPFv3.

The **no** form of the command removes the network-type configuration.

NOTE

The network type non-broadcast is not supported at this time.

Examples

The following example configures an OSPFv3 point-to-point link on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf network point-to-point
```

The following example configures an OSPFv3 broadcast link on a specific OSPFv3 Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf network broadcast
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf passive

Sets a specific OSPFv3 interface to passive.

Syntax

ipv6 ospf passive

no ipv6 ospf passive

Modes

Interface subtype configuration mode

Usage Guidelines

The **ipv6 ospf passive** command disables transmission of OSPFv3 control packets on that interface. OSPFv3 control packets received on a passive interface are discarded.

The **no** form of the command sets an interface back to active.

Examples

The following example sets a specific OSPFv3 virtual Ethernet (VE) interface to passive.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf passive
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf priority

Configures priority for designated router (DR) election and backup designated routers (BDRs) on the interface you are connected to.

Syntax

ipv6 ospf priority *value*

no ipv6 ospf priority

Command Default

The value is set to 1.

Parameters

value

Priority value. Valid values range from 0 through 255. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

The OSPFv3 router assigned the highest priority becomes the designated router, and the OSPFv3 router with the second-highest priority becomes the backup router.

The **no** form of the command restores the default value.

Examples

The following example sets a priority of 4 for the OSPFv3 router that is connected to an OSPFv3 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf priority 4
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

Syntax

ipv6 ospf retransmit-interval *interval*

no ipv6 ospf retransmit-interval

Command Default

The interval is 5 seconds.

Parameters

interval

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds. The default is 5.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command resets the retransmit interval to its default.

Examples

The following example sets the retransmit interval to 8 for all OSPFv3 devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf retransmit-interval 8
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf suppress-linklsa

Suppresses link LSA advertisements.

Syntax

ipv6 ospf suppress-linklsa

no ipv6 ospf suppress-linklsa

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command restores the defaults where link LSA advertisements are not suppressed.

Examples

The following example suppresses link LSAs from being advertised on devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf suppress-linklsa
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv3 to send link-state update packets on the interface to which you are connected.

Syntax

ipv6 ospf transmit-delay *value*

no ipv6 ospf transmit-delay

Command Default

The transmit delay is set to 1 second.

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command restores the default value.

Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf transmit-delay 25
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 prefix-list

Configures an IPv6 prefix list for basic traffic filtering

Syntax

ipv6 prefix-list *name* **deny** *ipv6-prefix/prefix-length* [**ge** *ge-value*] [**le** *le-value*]

ipv6 prefix-list *name* **permit** *ipv6-prefix/prefix-length* [**ge** *ge-value*] [**le** *le-value*]

ipv6 prefix-list *name* **seq** *instance-number* {**deny ge** *ge-value* **le** *le-value* | **permit ge** *ge-value* **le** *le-value* }

no ipv6 prefix-list *name*

Parameters

name
Specifies the prefix list name.

deny *ip-prefix/prefix-length*
Denies a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length, unless you use the **ge** *ge-value* or **le** *le-value* parameters.

ge *ge-value*
Specifies minimum prefix length to be matched. The range is from *ge-value* to 128.

le *le-value*
Specifies maximum prefix length to be matched. The range is from the *le-value* to the *prefix-length* parameter.

permit *ip-prefix/prefix-length*
Permits a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length, unless you use the **ge** *ge-value* or **le** *le-value* parameters.

seq
Specifies an IPv6 prefix list sequence number of entry.

instance
Specifies an IPv6 prefix list instance number.

Modes

Global configuration mode

Usage Guidelines

An IPv6 prefix list is composed of one or more conditional statements that execute a permit or deny action if a route matches a specified prefix. In prefix lists with multiple statements, you can specify a sequence number for each statement. The specified sequence number determines the order in which the statement appears in the prefix.

You can configure an IPv6 prefix list on a global basis, then use it as input to other commands or processes, such as route aggregation, route redistribution, route distribution, route maps, and so on. When an SLX-OS device interface sends or receives an IPv6 packet, it applies the statements within the IPv6 prefix list in their order of appearance to the packet. As soon as a match occurs, the device takes the specified action (permit or deny the packet) and stops further comparison for that packet.

You can use permit statements in the prefix list to specify the traffic that you want to send to the other feature. If you use deny statements, the traffic specified by the deny statements is not supplied to the other feature. You can configure up to one hundred IPv6 prefix lists.

You must specify the ipv6-prefix parameter in hexadecimal using 16-bit values between colons as documented in RFC 4291. You must specify the prefix-length parameter as a decimal value. A slash mark (/) must follow the ipv6-prefix parameter and precede the prefix-length parameter.

The *ge-value* or *le-value* you specify must meet the following condition for *prefix-length*:

```
ge-value <= le-value <= 128
```

Examples

The following example creates a prefix-list that allows routes with the prefix 2001:db8::/32 .

```
device# configure terminal
device(config)# ipv6 prefix-list route1 permit 2001:db8::/32
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# ipv6 prefix-list route1
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 protocol vrrp

Globally enables IPv6 VRRPv3.

Syntax

ipv6 protocol vrrp

no ipv6 protocol vrrp

Command Default

IPv6 VRRPv3 is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command globally disables VRRPv3.

Examples

To enable IPv6 VRRPv3 globally:

```
device# configure terminal
device(config)# ipv6 protocol vrrp
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 protocol vrrp-extended

Globally enables IPv6 VRRP-Ev3.

Syntax

ipv6 protocol vrrp-extended

no ipv6 protocol vrrp-extended

Command Default

IPv6 VRRP-Ev3 is disabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command globally disables IPv6 VRRP-Ev3.

Examples

To enable IPv6 VRRP-Ev3 globally:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 receive access-group

Applies an IPv6 access control list (ACL) at global configuration level. Such *receive-path ACLs* filter incoming route-processor traffic according to rules that you create, but do not filter data-path traffic.

Syntax

ipv6 receive access-group *acl-name*

no ipv6 receive access-group *acl-name*

Command Default

No receive-path ACLs are applied.

Parameters

acl-name
Specifies the name of the standard or extended IP access list.

Modes

Global configuration mode

Usage Guidelines

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL, from an interface-subtype configuration mode you use the { **ip** | **ipv6** | **mac** } **access-group** command.
- To apply a receive-path ACL, from global configuration mode you use the { **ip** | **ipv6** } **receive access-group** command.

You can apply a maximum of two receive-path ACLs to a device, as follows:

- One IPv4 receive-path ACL
- One IPv6 receive-path ACL

To remove a receive-path ACL, enter the **no** form of this command.

Examples

The following example creates an IPv6 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ipv6 access-list extended ipv6-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10::1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20::1 count
device(conf-ipacl-ext)# permit tcp host 10::2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10::2 any eq bgp count

device(conf-ipacl-ext)# exit
device(config)# ipv6 receive access-group ipv6-receive-acl-example
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 route

Configures an IPv6 static route.

Syntax

ipv6 route *dest-ipv6-prefix*/*prefix-length next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

ipv6 route *dest-ipv6-prefix*/*prefix-length link-local-next-hop-ipv6-address* [**ve** *ve-id*] [*metric*] [**distance** *number*] [**tag** *tag-number*]

ipv6 route *dest-ipv6-prefix*/*prefix-length link-local-next-hop-ipv6-address* [**ethernet** *slot/port*] [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length next-hop-ipv6-address*

no ipv6 route *dest-ipv6-prefix*/*prefix-length link-local-next-hop-ipv6-address* [**ve** *ve-id*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length link-local-next-hop-ipv6-address* [**ethernet** *slot/port*]

Command Default

No IPv6 static route is configured by default.

Parameters

dest-ipv6-prefix
Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
A decimal value specifying the length of the IPv6 address prefix.

next-hop-ipv6-address
IPv6 address of the next-hop gateway.

link-local-next-hop-ipv6-address
IPv6 address of the link-local next-hop gateway.

ethernet *slot/port*
Specifies the Ethernet slot and port.

ve *ve-id*
Specifies the virtual Ethernet (VE) interface.

metric
Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance *number*
Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route,

configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

tag

Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

tag-number

A number from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Use the **no** form of the command with the same parameters to remove the IPv6 static route.

Examples

The following example creates an IPv6 static route for a destination network with the prefix 2001:DB8::0/32 and a next-hop gateway with the global address 2001:DB8:0:ee44::1.

```
device# configure terminal
device(config)# ipv6 route 2001:DB8::0/32 2001:DB8:0:ee44::1
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 route next-hop-vrf

Configures an IPv6 static route through a named VRF.

Syntax

ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address*

Command Default

No IPv6 static route is configured by default.

Parameters

dest-ipv6-prefix
Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
A decimal value specifying the length of the IPv6 address prefix.

next-hop-ipv6-address
IPv6 address of the next-hop gateway.

next-hop-vrf *vrf_name next-hop-ipv6-address*
Specifies a VRF instance and a next-hop IPv6 address.

metric
Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance *number*
Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

tag
Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

tag-number
A number from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Use the **no** form of the command with the same parameters to remove the IPv6 static route.

Related commands:

- **ipv6 route**
- **ipv6 route null**

Examples

The following example creates an IPv6 static route to IPv6 2001:DB8::0/32 destinations through the VRF named "partners" and the next-hop router with the IPv6 address 2001:DB8:0:ee44::1.

```
device# configure terminal
device(config)# ipv6 route 2001:DB8::0/32 next-hop-vrf partners 2001:DB8:0:ee44::1
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 route null

Configures an IPv6 null route for discarding traffic.

Syntax

ipv6 route *dest-ipv6-prefix*/*prefix-length* **null 0** [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length* **null 0**

Command Default

No IPv6 static route is configured by default.

Parameters

dest-ipv6-prefix
Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
A decimal value specifying the length of the IPv6 address prefix.

next-hop-ipv6-address
IPv6 address of the next-hop gateway.

null 0
Causes packets to the selected destination to be dropped by shunting them to the "null 0" interface. (This is the only available option.)

ethernet *slot/port*
Specifies the Ethernet slot and port.

metric
Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance *number*
Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

tag
Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

tag-number
A number from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Use the **no** form of the command with the same parameters to remove the null route.

Related commands:

- **ipv6 route**
- **ipv6 route next-hop-vrf**

Examples

The following example creates a primary route to all 2001 : DB8 : : 0/32 destinations through virtual interface (ve) 3. The primary route has the default cost metric of 1. The example aslo creates an alternative null route (with a cost metric of 2) to drop packets when the primary route is not available.

```
device# configure terminal
device(config)# ipv6 route 2001 : DB8 : : 0/32 fe80::1 ve 3
device(config)# ipv6 route 2001 : DB8 : : 0/32 null 0 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 router ospf

Enables and configures the Open Shortest Path First version 3 (OSPFv3) routing protocol.

Syntax

ipv6 router ospf [**vrf** *name*]

no ipv6 router ospf

Command Default

Disabled.

Parameters

vrf *name*

Specifies a nondefault VRF.

Modes

Global configuration mode

Usage Guidelines

If you save the configuration to the startup-config file after disabling OSPFv3, all OSPFv3 configuration information is removed from the startup-config file.

Use this command to enable the OSPFv3 routing protocol and enter OSPFv3 router or OSPFv3 router VRFconfiguration mode. OSPFv3 maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

The **no** form of the command deletes all current OSPFv3 configurations and blocks any further OSPFv3 configuration.

Examples

The following example enables OSPFv3 on a default VRF and enters OSPFv3 router configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 vrrp-extended auth-type

Configures the type of authentication used on a Virtual Router Redundancy Protocol Extended (VRRP-E) interface.

Syntax

ipv6 vrrp-extended auth-type md5-auth *auth-text*

no ipv6 vrrp-extended auth-type md5-auth

Command Default

No authentication is configured for a VRRP-E interface.

Parameters

md5-auth *auth-text*

Configures MD5 authentication on the interface. The maximum length of the text string is 64 characters.

Modes

Virtual Ethernet (VE) interface configuration mode

Usage Guidelines

This configuration is for VE interfaces only.

If the **md5-auth** option is configured, syslog and SNMP traps are generated if a packet is being dropped due to MD5 authentication failure. Using MD5 authentication implies that the software does not need to run checksum verification on the receiving device and can rely on the authentication code (message digest 5 algorithm) to verify the integrity of the VRRP-E message header.

The **no** form of this command removes the VRRP-E authentication from the interface.

Examples

The following example configures MD5 authentication on VE interface 20.

```
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 20
device(config-if-Ve-20)# ipv6 vrrp-extended auth-type md5-auth lyk28d3j
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 vrrp-extended-group

Configures an IPv6 VRRP-Ev3 group and enters into the VRRP-E configuration mode.

Syntax

ipv6 vrrp-extended-group *group-ID*

no ipv6 vrrp-extended-group *group-ID*

Parameters

group-ID

A number from 1 through 255 that you assign to the VRRP-Ev3 group.

Modes

Virtual Ethernet (VE) interface configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-extended-group** *group-ID* to remove the specific IPv6 VRRP-Ev3 group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

This configuration is for virtual Ethernet (VE) interfaces only. IPv6 VRRP-Ev3 must be enabled on the device before the IPv6 VRRP-E group is configured.

Examples

The following example shows how to assign the VE interface with a VLAN number of 2019 to the VRRP-Ev3 group with the ID of 19.

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 2019
device(config-Ve-2019)# ipv6 address 2001:2019:8192::122/64
device(config-Ve-2019)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-19)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 vrrp-group

Configures an IPv6 VRRPv3 group and enters into the virtual router configuration mode.

Syntax

ipv6 vrrp-group *group-ID*

no ipv6 vrrp-group *group-ID*

Parameters

group-ID

A value from 1 through 255 that you assign to the VRRPv3 group.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-group** *group-ID* to remove a specific IPv6 VRRPv3 group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

IPv6 VRRPv3 must be enabled on the device before the IPv6 VRRP group is configured.

Examples

The following example shows how to assign an Ethernet interface to the VRRPv3 group with the ID of 18.

```
device# configure terminal
device(config)# ipv6 protocol vrrp
device(config)# interface ethernet 1/6
device(config-if-eth-1/6)# ipv6 address 2001:2019:8192::125/64
device(config-if-eth-1/6)# ipv6 vrrp-group 18
device(config-vrrp-group-18)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

ipv6 vrrp-suppress-interface-ra

Suppresses interface router advertisement (RA) when VRRPv3 is configured on an interface.

Syntax

ipv6 vrrp-suppress-interface-ra

no ipv6 vrrp-suppress-interface-ra

Command Default

Interface RA is enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-suppress-interface-ra** to remove the suppression of interface RA.

Router advertisements are sent by the VRRP master device and contain the link-local virtual IP address and the virtual MAC address. For network security reasons, if you do not want the MAC addresses of interfaces to be viewed, you can disable RA messages.

Examples

This example suppresses interface RA on a virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# ipv6 protocol vrrp
device(config)# interface ve 2019
device(config-Ve-2019)# ipv6 vrrp-suppress-interface-ra
```

History

Release version	Command history
18x.1.00	This command was introduced.

iterations

For an implementation of an event-handler profile, specifies the number of times an event-handler action is run, when triggered.

Syntax

iterations *num-iterations*

no iterations

Command Default

When the trigger condition occurs, the event-handler actions runs once.

Parameters

num-iterations

Specifies the number of times an event-handler action is run, when triggered. Valid values are any positive integer.

Modes

Event-handler activation mode

Usage Guidelines

The **no** form of this command resets the **iterations** setting to the default 1 iteration.

Examples

The following example specifies 5 iterations.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# iterations 5
```

The following example resets **iterations** to the default value of 1 iteration.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no iterations
```

History

Release version	Command history
17s.1.00	This command was introduced.

Commands K - M

key

Specifies a text string to be used as a shared secret between the device and the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

key *shared_secret*

no key

Command Default

The default value is "sharedsecret".

Parameters

shared_secret

The text string that is used as the shared secret between the device and the RADIUS server. The default string is "sharedsecret". The exclamation mark (!) is supported for RADIUS servers, and you can specify the shared secret string in either double quotation marks or by using the escape character (\); for example, **"secret!key"** or **secret\!key**.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **key** command does not support an empty string.

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure the text string "new#radius*secret" as the shared secret between the device and the RADIUS server.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# key "new#radius*secret"
```

History

Release version	Command history
18x.1.00	This command was introduced.

key-add-remove-interval

Alters the timing of the authentication key add-remove interval.

Syntax

key-add-remove-interval *interval*

no key-add-remove-interval *interval*

Parameters

interval

Specifies the add-remove interval in seconds. Valid values range from 0 through 14400. The default is 300 seconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command resets the add-remove interval to the default value of 300 seconds.

Examples

The following example sets the key add-remove interval to 240 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# key-add-remove-interval 240
```

History

Release version	Command history
18x.1.00	This command was introduced.

key-rollover-interval

Alters the timing of the existing configuration changeover.

Syntax

key-rollover-interval *interval*

no key-rollover-interval *interval*

Parameters

interval

Specifies the key-rollover-interval in seconds. Valid values range from 0 through 14400. The default is 300 seconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

In order to have consistent security parameters, rekeying should be done on all nodes at the same time. Use the **key-rollover-interval** command to facilitate this. The key rollover timer waits for a specified period of time before switching to the new set of keys. Use this command to ensure that all the nodes switch to the new set of keys at the same time.

The **no** form of the command resets the rollover interval to the default value of 300 seconds.

Examples

The following example sets the key rollover interval to 420 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# key-rollover-interval 420
```

The following example re-sets the key rollover interval to the default value.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# no key-rollover-interval 420
```

History

Release version	Command history
18x.1.00	This command was introduced.

keypair

Associates the generated RSA/ECDSA/DSA key pair with a trust point for security protocol exchanges for applications.

Syntax

Associates the generated RSA/ECDSA/DSA key pair with the trust point.

keypair *key_label*

no keypair

Parameters

key_label

Specifies the name of the key pair to associate with the trust point.

Modes

Trust point configuration mode

Usage Guidelines

Use the **no keypair** command to remove the key pair association.

Examples

Typical command usage:

```
device(config)# crypto ca trustpoint t1
device(config-ca-t1)# keypair k1
device(config-ca-t1)# do show running-config crypto
 crypto key label k1 rsa modulus 2048
 crypto ca trustpoint t1
  keypair k1
!
device# show crypto ca trustpoint
trustpoint: t1; key-pair: k1
```

History

Release version	Command history
18x.1.00	This command was introduced.

lacp default-up

Activates an Link Aggregation Control Protocol (LACP) link in the absence of PDUs.

Syntax

lacp default-up

no lacp default-up

Modes

Interface subtype configuration mode

Usage Guidelines

This command forces the port to activate an LACP link if there are no PDUs available on the interface port.

This command is supported on all physical interfaces.

This command is visible only if the interface is a dynamic and standard member of a port-channel.

This command is not supported on static LAGs.

This command is not supported on static or dynamic trunks.

Examples

The following example activates an LACP link in the absence of PDUs on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/11
device(conf-if-eth-0/11)# lacp default-up
```

History

Release version	Command history
17s.1.00	This command was introduced.

lacp port-priority

Configures the Link Aggregation Control Protocol (LACP) port priority of a member port of a port-channel.

Syntax

lacp port-priority *value*

no lacp port-priority

Parameters

value

Specifies the priority. Valid values range from 1 through 65535. A lower number takes priority over a higher number. The default value is 32768.

Modes

Interface subtype configuration mode.

Usage Guidelines

An LACP port priority is configured on each port using LACP. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

A link with higher priority (smaller in value) gets preference over a link with lower priority (greater in value).

The **no** form of the command returns the default value.

Examples

The following example sets the LACP port priority to 1000 for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# lacp port-priority 1000
```

History

Release version	Command history
18x.1.00	This command was introduced.

lacp system-priority

Sets the Link Aggregation Control Protocol (LACP) system priority. The LACP priority determines which system is responsible for resolving conflicts in the choice of aggregation groups.

Syntax

lacp system-priority *value*

no lacp system-priority

Command Default

The default value is 32768.

Parameters

value

Specifies the value of the LACP system priority. Valid values range from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

Lower numerical values have higher priorities.

Enter **no lacp system-priority** to reset the system priority to the default value.

Examples

The following example sets the LACP system priority value to 68.

```
device# configure terminal
device(config)# lacp system-priority 68
```

History

Release version	Command history
18x.1.00	This command was introduced.

lacp timeout

Sets the timeout value used by the Link Aggregation Control Protocol (LACP) to exchange packets on an interface before invalidating a received data unit (DU).

Syntax

lacp timeout { **long** | **short** }

no lacp timeout

Command Default

For standard LAGs, the default value is the **long** timeout.

Parameters

long

Specifies that a long-timeout value of 30 seconds will be used. With this value, the port waits three times this long (90 seconds) before invalidating the information received earlier on this PDU.

short

Specifies that a short-timeout value of one second will be used. With this value, the port waits three times this long (three seconds) before invalidating the information received earlier on this PDU.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set the timeout value based on how frequently you think the switch will receive LACP PDUs from the partner device.

The **no** form of the command restores the default values.

Examples

The following example sets the LACP long-timeout value on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# lacp timeout long
```

History

Release version	Command history
18x.1.00	This command was introduced.

lacp-pdu-forward enable

Configures the device to forward LACP PDUs received on an interface where LACP is not configured, to the VLAN on which the LACP PDUs are received.

Syntax

lacp-pdu-forward enable

no lacp-pdu-forward enable

Command Default

LACP PDUs received on an interface where LACP is not configured are discarded.

Modes

Interface subtype configuration mode

Usage Guidelines

LACP PDUs are forwarded only when they are received on a physical interface or static port channel interface. LACP PDUs cannot be forwarded if they are received on a LACP based dynamic port channel.

LACP PDU forwarding enabled on a static port channel applies to all the member ports.

When LACP is enabled on a port, it overrides LACP PDU forwarding configuration and the PDUs are trapped to CPU.

Enabling and disabling of BPDU drop on a bridge domain does not impact LACP PDU forwarding.

Use the **no** form of the command to disable LACP PDU forwarding.

Examples

The following example configures LACP PDU forwarding on a physical interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# lacp-pdu-forward enable
```

The following example configures LACP PDU forwarding on a static port channel interface.

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)# lacp-pdu-forward enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

lag hash

Configures LAG hashing parameters such as where to start picking headers for key generation, the number of headers to be considered, and so forth.

Syntax

lag hash hdr-count *count*

no lag hash hdr-count *count*

lag hash hdr-start { **fwd** | **term** }

no lag hash hdr-start { **fwd** | **term** }

lag hash srcport

no lag hash srcport

Parameters

hdr-count *count*
Specifies the number of headers to be considered for LAG hashing. Values range from 1 through 3. The default is 3.

hdr-start
Specifies where to start picking headers for the key generation.

fwd
(Default) Start from the inner header, which is used for forwarding the packet.

term
Start from the outer header, which is the header below the forwarding header and is the last terminated header.

srcport
Includes the source port in the hashing configuration. The default is not to include it.

Modes

Global configuration mode

Usage Guidelines

To restore default settings, use the **no** forms of these commands.

Examples

The following example changes the **hdr-count** value to 2.

```
device# configure terminal
device(config)# lag hash hdr-count 2
```

The following example changes the **hdr-start** value to term.

```
device# configure terminal
device(config)# lag hash hdr-start term
```

History

Release version	Command history
18x.1.00	This command was introduced.

ldap-server host

Configures an LDAP-server host.

Syntax

ldap-server host [**use-vrf** *vrf-name*]

ldap-server host { *ipaddr* | *FQDN* } [**port** *portnum*] [**domain** *basedn*] [**timeout** *secs*] [**retries** *num*]

no ldap-server host { *ipaddr* | *FQDN* } [**use-vrf** *vrf-name*]

Command Default

- Timeout: 5 seconds
- Port: 389
- Retries: 5

Parameters

use-vrf *vrf-name*
Specifies a VRF though which to communicate with the LDAP server. See the Usage Guidelines.

ipaddr | *FQDN*
Specifies the IPv4 address or Fully Qualified Domain name of the Active Directory (AD) server. IPv6 is supported for Windows 2008 AD server only. The maximum supported length for the LDAP host name is 40 characters.

port *portnum*
Specifies the TCP port used to connect the AD server for authentication. The port range is from 1024 through 65535.

domain *basedn*
Describes the base domain name of the host.

timeout *secs*
Specifies the wait time for a server to respond. The range is 1 through 60 seconds.

retries *num*
Specifies the number of retries for the server connection. The range is 0 through 100.

Modes

Global configuration mode

Usage Guidelines

Use this command to sets up a connection to the Lightweight Directory Access Protocol (LDAP) server host, or modifies an existing configuration. A maximum of 5 LDAP servers can be configured on a device. Executing "no" on an attribute sets it with its default value.

Enter **no ldap-server host** to delete the server configuration.

Invoking **no** on an attribute sets the attribute with its default value.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

To add an LDAP server on port 3890 with retries set to three:

```
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# domain sec.extreme.com port 3890 retries 3
```

To change the domain in an existing configuration:

```
device(config)# ldap-server host 10.24.65.6

device(config-host-10.24.65.6/mgmt-vrf)# domain security.extreme.com
```

To delete an LDAP server:

```
device(config)# no ldap-server host 10.24.65.6
```

To reset the number of retries to the default value:

```
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# retries
```

Executing **no** on an attribute sets it with its default value.

```
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# no retries
```

Attributes holding default values will not be displayed.

```
device(config-host-10.24.65.6/mgmt-vrf)# do show running-config ldap-server host 10.24.65.6
ldap-server host 10.24.65.6 use-vrf mgmt-vrf
port 3890 retries 3 timeout 8 basedn security.extreme.com
```

History

Release version	Command history
18x.1.00	This command was introduced.

ldap-server maprole

Maps an Active Directory (AD) group to a device role.

Syntax

ldap-server maprole group *group_name* **role** *role_name*

no ldap-server maprole group *group_name*

Parameters

group *group_name*
The name of the AD group.

role *role_name*
The name of the device role.

Modes

Global configuration mode

Usage Guidelines

Enter **no ldap-server maprolegroup** *group_name* without the **role** *role_name* parameter to remove the mapping of the AD group to a role.

Examples

To map the AD group "Administrator" to the device role "admin":

```
device(config)# ldap-server maprole group Administrator role admin
```

To remove the mapping:

```
device(config)# no ldap-server maprole group Administrator
```

History

Release version	Command history
18x.1.00	This command was introduced.

line vty exec-timeout

Sets the recurrent CLI idle timeout period.

Syntax

line vty exec-timeout *timeout*

no line vty exec-timeout

Command Default

If no value is specified, the timeout value is 10 minutes.

Parameters

timeout

Specifies the CLI session timeout period in minutes. The timeout value specifies the amount of time a CLI session can be idle before it logs you out. Valid values range from 0 through 136. The default is 10.

Modes

Global configuration mode

Usage Guidelines

The **line vty exec timeout** command is a recurrent command, applying to all login sessions. The **terminal timeout** command applies only to the current session.

Even if other keys are pressed during the timeout period, the only keystroke that prevents logout is **Enter**.

This command is supported only on the local device.

This command is not available on the standby management module.

To restore the default timeout value of 10 minutes, enter **no line vty exec-timeout**.

Examples

The following example sets the terminal timeout to 60 minutes.

```
device(config)# line vty exec-timeout 60
device(config-line-vty)# exit
device(config)# exit
device# show running-config line vty
line vty
exec-timeout 60
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

link-error-disable

Configures port flap dampening for the interface, including the threshold of link flapping to shut down the port and the time interval in which it remains shut down.

Syntax

link-error-disable *toggle-threshold sampling-time-in-sec wait-time-in-sec*

no link-error-disable

Command Default

Port flap dampening is disabled on the device.

Parameters

toggle-threshold

Specifies the number of times a port link state goes from up to down and down to up before the wait period is activated. The value ranges from 1 through 50.

sampling-time-in-sec

Specifies the amount of time, in seconds, during which the specified toggle threshold can occur before the wait period is activated. Enter an integer from 1 through 65535.

wait-time-in-sec

Specifies the amount of time, in seconds, for which the port remains disabled (down) before it becomes enabled. The value ranges from 0 through 65535. A value of 0 indicates that the port will stay down until an administrative override occurs.

Modes

Interface Ethernet configuration mode

Usage Guidelines

Use the **no** form of the command to disable port flap dampening.

Port flap dampening allows you to configure a wait period before a port, whose link goes down then up, becomes enabled. This feature is available for all front ports on the device.

If the port link state toggles, from down to up or from up to down, for a specified number of times within a specified period, the interface is physically disabled for the specified wait period. Once the wait period expires, the port's link state is re-enabled. However, if the wait period is set to zero (0) seconds, or you want to re-enable the port before the wait period expires, the port must be manually re-enabled. To re-enable the port, reenter the **link-error-disable** command on the disabled port.

Examples

The following example shows the configuration of port flap dampening. The toggle threshold is set to 10 times. The sampling time is set to 3 seconds. The wait time is set to 10 seconds.

```
device# configure terminal
device(config)# interface Ethernet 1/4
device(conf-if-eth-1/4)# link-error-disable 10 3 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

link-fault-signal

Configures RX and TX Link Fault Signaling (LFS) detection globally or on an interface port.

Syntax

link-fault-signal rx { **off** | **on** } **tx** { **off** | **on**

no link-fault-signal

Command Default

Both TX and RX LFS are enabled.

Parameters

rx

Configure RX LFS detection.

off

Disables LFS.

on

Enables LFS.

tx

Configure TX LFS detection.

Modes

Global and interface configuration modes

Usage Guidelines

Use the **no** form of the command to reset RX and TX LFS to their default settings of enabled.

The interface must be in the shutdown state before you disable or enable TX LFS.

LFS is not supported in 1G mode.

When the device detects a local fault, it returns a remote fault to the link partner. When the device detects a remote fault, it returns an idle state.

A port's physical link detection is independent of LFS detection. When either of these link fault signals is detected, the following behaviors occur:

- The link is declared as DOWN and the device should display Protocol Down on the SLX-OS CLI.
- The physical link is not bought down in both of the previous cases. The peer side based on its implementation might display that the link is UP when the device displays that the link is DOWN due to a fault detection.
- The transmit (TX) packets, if any, are dropped at the MAC layer. The receive (RX) packets, if any, are dropped in the software.

- The detected signal is reported as a RASTRACE message and as a RASLOG. The same behavior occurs when the signal is cleared.

You can enable or disable LFS globally and on the interface level for both RX and TX directions:

- If the LFS is enabled for RX, the normal local and remote fault detection and processing described previously occur. If it is disabled for RX, local and remote fault detection are ignored.
- If the LFS is enabled for TX and a local fault occurs, a remote fault (pause frame) is generated to the remote side. If it is disabled for TX, the remote fault is not generated.

The interface configuration overrides the global configuration.

Examples

The following example shows the global and interface configuration of LFS. In this example, the global LFS is disabled for the link fault RX and enabled for link fault TX. The LFS for the interface is enabled for the link fault RX and disabled for the link fault TX, overriding the global configuration.

```
device# configure terminal
device(config)# link-fault-signaling rx off tx on
device(config)# interface Ethernet 2/1
device(conf-if-eth-2/1)# shutdown
device(conf-if-eth-2/1)# link-fault-signaling rx on tx off
device(conf-if-eth-2/1)# no shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

link-oam allow-loopback

Enables an interface to accept remote loopback.

Syntax

link-oam allow-loopback

no link-oam allow-loopback

Command Default

Please refer the usage guidelines.

Modes

Ethernet interface configuration mode

Usage Guidelines

To run this command, link OAM must be configured. By default, loopback is disabled on the interface. The support for this configuration is restricted. The user cannot configure allow-loopback on more than one port per line card. The NO form of the command disables the interface from accepting loopback.

Examples

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-int-eth1/1)# link-oam allow-loopback
```

History

Release version	Command history
18x.1.00	This command was introduced.

link-oam enable

Enables link oam on an ethernet interface and sets the mode to active or passive.

Syntax

link-oam enable [**active** | **passive**]

no link-oam enable

Command Default

Please refer the usage guidelines.

Parameters

active

Configures link-oam in active mode.

passive

Configures link-oam in passive mode.

Modes

Ethernet interface configuration mode

Usage Guidelines

By default, link oam is disabled on the interface. Once this CLI is configured, it cannot be modified. In order to reconfigure, link-oam has to be deconfigured using **no link-oam enable** command.

Examples

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-int-eth1/1)# link-oam enable passive
```

History

Release version	Command history
18x.1.00	This command was introduced.

link-oam remote-failure

Blocks the interface on receipt of a remote failure message, in addition to the syslog generation.

Syntax

link-oam remote-failure {**link-fault** | **dying-gasp** | **critical-event**} **action** *block-interface*

Command Default

Please refer the usage guidelines.

Parameters

link-fault
Blocks the interface on receipt of a link failure message.

dying-gasp
Blocks the interface on receipt of a dying-gasp message.

critical-event
Blocks the interface on receipt of a critical event message.

Modes

Ethernet interface configuration mode

Usage Guidelines

To run this command, the Link OAM must be configured. By default, on receipt of a remote failure message, the device will only log the event through syslog. This command allows block-interface action to be configured for each of the three events that the protocol supports.

Examples

```
device(config-int-eth1/1)# link-oam remote-failure link-fault action block-interface
device(config-int-eth1/1)# link-oam remote-failure dying-gasp action block-interface
```

History

Release version	Command history
18x.1.00	This command was introduced.

link-oam remote-loop-back

Starts and stops the remote loopback on peer that is connected to a local ethernet interface.

Syntax

link-oam remote-loop-back ethernet *slot-number* / *port-number* [**start** | **stop**]

Parameters

slot-number
Specifies the slot number.

port-number
Specifies the port number.

start
Start the remote loopback on peer that is connected to the interface.

stop
Stops the remote loopback on peer that is connected to the interface.

Modes

Exec mode

Examples

```
device# link-oam remote-loop-back ethernet 1/1 start
```

History

Release version	Command history
18x.1.00	This command was introduced.

lldp profile

Applies a Link Layer Discovery Protocol (LLDP) profile to an interface.

Syntax

lldp profile *name*

no lldp profile

Command Default

LLDP profile name.

Parameters

name

Specifies the profile name. Valid profile name length is between 1 and 32 characters.

Modes

Interface subtype configuration mode

Usage Guidelines

You must use the **lldp profile** command to create an LLDP profile before you can apply the profile to the interface. Only one LLDP profile can exist at any time for a particular interface. When this command is not present, the parameters defined in the global LLDP configuration are used.

Enter **no lldp profile** to delete the profile from the interface.

Examples

To apply an LLDP profile called *test* on an specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/9
device(conf-if-eth-0/9)# lldp profile test
```

History

Release version	Command history
18x.1.00	This command was introduced.

load-balance hash

For supported header types, selects the fields used for LAG hashing.

Syntax

load-balance hash ethernet { **da-mac** | **etype** | **sa-mac** | **vlan** }

no load-balance hash ethernet [**da-mac** | **etype** | **sa-mac** | **vlan**]

load-balance hash ip { **dst-ip** | **dst-l4-port** | **protocol** | **src-ip** | **src-l4-port** }

no load-balance hash ip [**dst-ip** | **dst-l4-port** | **protocol** | **src-ip** | **src-l4-port**]

load-balance hash ipv6 { **ipv6-dst-ip** | **ipv6-dst-l4-port** | **ipv6-next-hdr** | **ipv6-src-ip** | **ipv6-src-l4-port** }

no load-balance hash ipv6 [**ipv6-dst-ip** | **ipv6-dst-l4-port** | **ipv6-next-hdr** | **ipv6-src-ip** | **ipv6-src-l4-port**]

Command Default

All header parameters are enabled.

Parameters

ethernet

da-mac
Specifies Layer 2 destination address.

etype
Specifies the **etype** option.

sa-mac
Specifies Layer 2 source address.

vlan
Specifies the **vlan** option.

ip

dst-ip
Specifies destination IP address.

dst-l4-port
Specifies destination Layer 4 port.

protocol
Specifies the IP protocol.

src-ip
Specifies source IP address.

src-l4-port
Specifies source Layer 4 port.

ipv6

ipv6-dst-ip
Specifies destination IPv6 address.

ipv6-dst-l4-port
Specifies IPv6 destination Layer 4 port.

ipv6-next-hdr
Specifies next IPv6 header.

ipv6-src-ip
Specifies source IPv6 address.

ipv6-src-l4-port
Specifies IPv6 source Layer 4 port.

Modes

Global configuration mode

Usage Guidelines

The **no** forms of these commands cancel selection of the relevant protocol headers for LAG hashing.

Examples

The following example specifies Layer 2 destination address.

```
device# configure terminal
device(config)# load-balance hash ethernet da-mac
```

The following example cancels the default enablement of IPv4 headers for hashing. It then enables IPv4 source IP address only.

```
device# configure terminal
device(config)# no load-balance hash ip
device(config)# load-balance hash ip src-ip
```

History

Release version	Command history
18x.1.00	This command was introduced.

local-as

Specifies the BGP autonomous system number (ASN) where the device resides.

Syntax

local-as *num*

no local-as *num*

Command Default

No ASN is specified.

Parameters

num

The local ASN. The range is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

ASNs in the range from 64512 through 65535 are private numbers that are not advertised to the external community.

The **no** form of the command removes the ASN from the device.

Examples

This example assigns a separate local AS number.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 777
```

History

Release version	Command history
18x.1.00	This command was introduced.

log (OSPFv2)

Controls the generation of OSPFv2 logs.

Syntax

log { **adjacency** [**dr-only**] | **all** | **bad-packet** [**checksum**] | **database** | **retransmit** }

no log { **adjacency** [**dr-only**] | **all** | **bad-packet** [**checksum**] | **database** | **retransmit** }

Command Default

Only OSPFv2 messages indicating possible system errors are logged.

Parameters

adjacency

Specifies the logging of essential OSPFv2 neighbor state changes.

dr-only

Specifies the logging of essential OSPF neighbor state changes where the interface state is designated router (DR).

all

Specifies the logging of all syslog messages.

bad-packet

Specifies the logging of bad OSPFv2 packets.

checksum

Specifies all OSPFv2 packets that have checksum errors.

database

Specifies the logging of OSPFv2 LSA-related information.

retransmit

Specifies the logging of OSPFv2 retransmission activities.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of specific events related to OSPFv2. If this command is not enabled only OSPFv2 messages indicating possible system errors are logged.

A limitation with the **dr-only** sub-option is that when a DR/BDR election is underway, OSPF neighbor state changes pertaining to non-DR/BDR routers are not logged. Logging resumes once a DR is elected on that network.

The **no** form of this command restores the default.

Examples

The following example enables the logging of all OSPFv2-related syslog events.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# log all
```

The following example enables the logging of OSPFv2 retransmission activities.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# log retransmit
```

History

Release version	Command history
18x.1.00	This command was introduced.

log (OSPFv3)

Controls the generation of OSPFv3 logs.

Syntax

log { **adjacency** [**dr-only**] | **all** | **bad-packet** [**checksum**] | **database** | **retransmit** }

no log { **adjacency** | **all** | **bad-packet** [**checksum**] | **database** | **retransmit** }

Command Default

Only OSPFv3 messages indicating possible system errors are logged.

Parameters

adjacency
Specifies the logging of essential OSPFv3 neighbor state changes.

dr-only
Specifies the logging only of designated router (DR) interface adjacency changes.

all
Specifies the logging of all syslog messages.

bad-packet
Specifies the logging of bad OSPFv3 packets.

checksum
Specifies all OSPFv3 packets that have checksum errors.

database
Specifies the logging of OSPFv3 LSA-related information.

retransmit
Specifies the logging of OSPFv3 retransmission activities.

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of specific events related to OSPFv3. If this command is not enabled, only OSPFv3 messages indicating possible system errors are logged.

The **no** form of the command restores the default.

Examples

The following example enables the logging of all OSPFv3-related syslog events.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# log all
```

The following example enables the logging of OSPFv3 retransmission activities.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# log retransmit
```

History

Release version	Command history
18x.1.00	This command was introduced.

log-dampening-debug

Logs dampening debug messages.

Syntax

log-dampening-debug

no log-dampening-debug

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

The following example logs dampening debug messages.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# log-dampening-debug
```

History

Release version	Command history
18x.1.00	This command was introduced.

log-shell

Controls the remote logging of SLXVM Linux shell command activities.

Syntax

log-shell { **start** | **status** | **stop** }

Command Default

By default, the device logs the SLXVM Linux shell access and all commands executed at the SLXVM Linux shell locally.

Parameters

start
Restarts remote logging.

status
Checks the remote logging status.

stop
Disables remote logging.

Modes

Privileged EXEC mode

Usage Guidelines

Changes of the **log-shell stop** and **log-shell start** commands are applicable only on new SLXVM Linux shell sessions.

If you configure a remote Syslog server, the same logs can be seen on this server.

When you disable remote logging, local logging of user activities continues.

Examples

The following example disables remote logging.

```
device# log-shell stop
```

The following example restarts remote logging.

```
device# log-shell start
```

History

Release version	Command history
18x.1.00	This command was introduced.

logging auditlog class

Activates audit logging for various categories and classes of actions.

Syntax

logging auditlog class *class*

no logging auditlog class *class*

Command Default

CONFIGURATION, FIRMWARE, and SECURITY audit log classes are enabled.

Parameters

class

Specifies the class name of the audit log. Valid classes are CONFIGURATION, FIRMWARE, and SECURITY.

Modes

Global configuration mode

Usage Guidelines

The total message storage available is 2048 messages.

Enter **no logging auditlog class** *class* to disable the audit logging for the specified class.

Examples

To enable a specific audit log class:

```
device# configure terminal
device(config)# logging auditlog class security
device(config)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

logging raslog console

Sets the severity levels for the RASLog console.

Syntax

logging raslog console *severity*

no logging raslog console *severity*

Command Default

Severity level is INFO.

Parameters

severity

Specifies the minimum severity level of the message to pass through the filter. Valid values consist of one of the following: INFO, WARNING, ERROR, or CRITICAL. Input values are case-sensitive.

Modes

Global configuration mode

Usage Guidelines

The total message storage available is 2048 messages.

Examples

To reset the RASLog severity levels to the default value.

```
device# configure terminal
device(config)# no logging raslog console
2013/11/14-08:42:57, [RAS-3008], 5348, M2 | Active, INFO, VDX8770-4, Logging messages to console has
been reset by user.
```

History

Release version	Command history
18x.1.00	This command was introduced.

logging raslog console stop

Temporarily stops displaying RASLog messages on the console.

Syntax

logging raslog console { **start** | **stop** [*minutes*] }

Command Default

RASlog messages display on the console

Parameters

start

Initiates RASLog messages.

stop *minutes*

Stops RASLog messages for a designated number of minutes.

Modes

Privileged EXEC mode

Usage Guidelines

When stopping or starting RASLog messages, the commands are not configuration commands and therefore are not persistent.

If the command **logging raslog console stop** *minutes* is invoked before the previous time value expires, the latest CLI duration applies.

Examples

To stop RASLog messages for 1 minute:

```
device# logging raslog console stop 1
Logging message have been blocked on console for 1 minutes
```

To start RASLog messages:

```
device# logging raslog console start
```

History

Release version	Command history
18x.1.00	This command was introduced.

logging syslog-client

Configure various parameters used by syslog clients.

Syntax

logging syslog-client localip { CHASSIS_IP }

Parameters

CHASSIS_IP

Uses the Chassis IP address as source IP address in the IP header of syslog messages generated by this device.

Modes

Global configuration mode

Examples

Example command for using the chassis IP as the source IP in the IP header of syslog messages, generated by this device.

```
device# configure terminal
device(config)# logging syslog-client localip CHASSIS_IP
```

History

Release version	Command history
18x.1.00	This command was introduced.

logging syslog-facility local

Configures the syslog facility.

Syntax

logging syslog-facility local *log_level*

Command Default

Syslog level is LOG_LOCAL7.

Parameters

log_level

Specifies the syslog facility level. Valid log levels include the following: LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4, LOG_LOCAL5, LOG_LOCAL6, LOG_LOCAL7

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the log level for all error log entries to forward to one or more specified syslog servers. You can configure up to four syslog servers.

Examples

To configure the syslog facility level:

```
device# configure terminal
device(config)# logging syslog-facility local LOG_LOCAL5
```

History

Release version	Command history
18x.1.00	This command was introduced.

logging syslog-server

Configures a switch to forward system messages to specified syslog servers.

Syntax

logging syslog-server *ip_address* [**secure**] [**port** *port-num*] [**use-vrf** *vrf-name*]

no logging syslog-server *ip_address* [**secure**] [**port** *port-num*] [**use-vrf** *vrf-name*]

Parameters

ip_address
Specifies the IP address of the syslog server in IPv4 or IPv6 format.

secure
Configures a secure default (port 514) or specified nondefault syslog server port. A secure port number with default values is not shown in the SLX-OS database.

port *port-num*
Specifies a nondefault port. The port range is from 1 through 65535.

use-vrf *vrf-name*
Specifies a VRF through which to communicate with the server. See the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure a switch to forward all error log entries to the one or more specified servers. You can configure up to four servers.

A secure port number with default values is not shown in the database.

The **certutil import syslogca** command is required for secure syslog to be fully functional.

You can configure up to four syslog servers; this includes all VRFs. You must execute the command for each server.

Use the **no logging syslog-server** command with the optional **use-vrf** keyword to remove the specified IP address VRF.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

To configure a server IPv4 address to which system messages are sent on a user-specified VRF:

```
device# configure terminal
device(config)# logging syslog-server 192.168.163.233 use-vrf myvrf
device(config-syslog-server-192.168.163.233/myvrf)#
```

To configure a server IPv4 address and specify a VRF with a secure nondefault port, and confirm the configuration:

```
device# configure terminal
device(config)# logging syslog-server 192.168.163.233 use-vrf myvrf secure port 1999
device(config-syslog-server-192.168.163.233/myvrf)# do show running-config logging syslog-server
logging syslog-server 192.168.163.233 use-vrf myvrf
secure port 1999
```

To remove a configured syslog server:

```
device# configure terminal
device(config)# no logging syslog-server 192.168.163.233
```

To remove a syslog nondefault server port and confirm the configuration:

```
device# configure terminal
device(config)# no logging syslog-server 10.17.17.203 secure port 1999
device(config)# do show running-config logging syslog-server
logging syslog-server 10.17.17.203
secure
```

History

Release version	Command history
18x.1.00	This command was introduced.

logical-interface

Configures a logical interface on a physical port or a port-channel (LAG) on an edge port, entering LIF configuration mode, and optionally binds the interface to a bridge domain (BD).

Syntax

logical-interface { **ethernet** *slot/port.service_instance* | **port-channel** *num.service_instance* }

no logical-interface { **ethernet** *slot/port.service_instance* | **port-channel** *num.service_instance* }

Command Default

See the Usage Guidelines.

Parameters

ethernet *slot/port*
: Specifies an Ethernet interface.

port-channel *num*
: Specifies a port-channel interface.

service_instance
: Specifies a service instance ID. Range is from 1 through 12288.

Modes

Interface subtype configuration mode

Bridge domain configuration mode

Usage Guidelines

The following are some common rules to consider in configuring logical interfaces:

- This command is applicable to an edge port only.
- This command by itself does not create the LIF as it requires more classifications as to what VLAN(s) should be specified and whether the classifying VLAN is untagged or tagged.
- By default, when the LIF is created it is enabled. it is also "tagged" unless it is explicitly configured with the "untagged" option.
- The user must specify a service instance ID. If the service instance ID has already been configured, this command allows the user to specify the VLAN classification for this LIF. Allowed LIF service instance ranges are from 1 through 12288 (12K LIFs are allowed per interface type). Currently, up to 100K LIFs are supported in the system, with 12K for physical port or LAG combined and 8K for PW based.
- A LIF service instance ID has no correlation to the VLAN ID of the LIF.
- Each physical/LAG-based LIF must have an associated VLAN configured or else it will not be usable when the user attempts to add it to a service. Such a configuration request to add the LIF to a service will be rejected.

- Once the LIF is associated with a Layer 2 service, its VLAN value cannot be changed or deleted unless it is first removed from the associated service. In case the LIF is not yet associated to a service, the user is free to remove the VLAN configuration or change the VLAN assignment.
- The "untagged" configuration can only be allowed for one LIF under the same physical port or LAG. If one LIF is already configured as untagged, all subsequent attempts on the same physical port or LAG will be rejected.
- Once the "untagged" option is selected, it will only have one VLAN as the next classification option. There is no dual-tag support for the untagged case.
- In order to configure an untagged LIF, the main interface must be set as "switchport mode trunk-no-default-native". If it is only set to regular trunk mode, the native VLAN is already associated with a regular Layer 2 VLAN LIF and no explicit untagged LIF can be configured on that interface.
- Once the LIF is associated with a service (Layer 2) such as bridge domain, its "untagged/tagged" configuration cannot be changed. The service instance or its current VLAN classification must be deleted by user first and then added back with the proper "untagged/tagged" option.
- VLANs 4091 through 4095 are reserved VLANs and these should not be used as the VLAN ID for either the inner or outer VLAN of the LIF.
- The VLAN specified under the LIF ensures that such a VLAN is not already configured under the **switchport** command for a regular Layer 2 allowed VLAN.

The **no** version of the command removes the LIF from the BD configuration. This can be applied any time if the LIF is not yet associated with (bound to) a service. If it is already associated with a service, the LIF is also implicitly removed from the BD configuration.

Examples

The following example sets "trunk-no-default-native" mode on an Ethernet interface, so that an untagged LIF can be configured on service instance 120.

```
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# switchport mode trunk-no-default-native
device(conf-if-eth-2/6)# logical-interface ethernet 2/6.120
device(conf-if-eth-lif-2/6.120)#
```

The following examples illustrate how up to command options can be configured in a single line.

```
device(conf-if-eth-2/6)# logical-interface ethernet 2/6.120 name myLIF120
device(conf-if-eth-lif-2/6.120)#

device(conf-if-eth-2/6)# logical-interface ethernet 2/6.120 vlan 120
device(conf-if-eth-lif-2/6.120)#
```

The following example sets "trunk-no-default-native" mode on a port-channel (LAG) interface, so that an untagged LIF can be configured on service instance 3.

```
device(config)# int port-channel 10
device(config-port-channel-10)# switchport mode trunk-no-default-native
device(config-port-channel-10)# logical-interface port-channel 10.3
device(config-if-po-lif-10.3)# untagged vlan 3
```

The following example shows how to create a logical Ethernet interface service instance (1/5.10) and bind it to bridge domain 4 by means of the **bridge-domain** command.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# logical-interface ethernet 1/5.10
device(conf-if-eth-lif-1/5.10)# vlan 50
device(conf-if-eth-lif-1/5.10)# exit

device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/5.10
```

The following example shows how to bind a logical port-channel interface service instance (2.200) to bridge domain 4 by means of the **bridge-domain** command.

```
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface port-channel 2.200
```

The following example shows the error message that displays when an attempt is made to bind a logical interface that was not previously created to a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/3.100
Error: Logical Interface not yet created
```

The following example shows the error message that displays when an attempt is made to bind a logical interface that is previously bound to another bridge domain.

```
device>enable
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/3.100
 Error: LIF already Binded
```

History

Release version	Command history
18x.1.00	This command was introduced.

loop-detection

Enables the loop detection (LD) feature at the interface level, VLAN, or bridge domain (BD) level, and enters Protocol Loop Detection configuration mode.

Syntax

loop-detection

no loop-detection

Command Default

This feature is disabled.

Modes

Interface subtype configuration mode (Ethernet or port-channel)

VLAN configuration mode

Bridge domain configuration mode

Usage Guidelines

When configured at the interface level, this command applies to LD strict mode.

When configured at the VLAN level, this command is applied to all ports in the VLAN.

When configured at the bridge domain (BD) level this command is applied to all the attachment circuit (AC) logical interfaces (LIFs) and VXLAN tunnels under the BD.

Use the **no** form of this command to disable loop detection at the interface, VLAN, or BD level.

Examples

The following example enables loop detection on an Ethernet interface and enters Protocol Loop Detection configuration mode:

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# loop-detection
device(config-loop-detect)#
```

The following example disables loop detection on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# no loop-detection
```

The following example enables loop detection on a port-channel interface and enters Protocol Loop Detection configuration mode.

```
device# configure terminal
device(config)# interface port-channel 20
device(config-port-channel-20)# loop-detection
device(config-loop-detect)#
```

The following example enables loop detection on a VLAN and enters Protocol Loop Detection configuration mode.

```
device# configure terminal
device(config)# vlan 5
device(config-vlan-5)# loop-detection
device(config-loop-detect)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

loop-detection shutdown-disable

Disables the shutting down of an interface (Ethernet or port-channel), a VLAN VXLAN tunnel, or a bridge domain (BD) VXLAN tunnel as a result of the loop detection (LD) protocol.

Syntax

loop-detection shutdown-disable

no loop-detection shutdown-disable

Command Default

This feature is disabled.

Modes

Interface subtype configuration mode (Ethernet or port-channel)

VLAN configuration mode

Usage Guidelines

Use the **no** form of this command. to revert to default behavior. (LD protocol shuts down the interface.)

Examples

The following example disables the shutdown of an Ethernet interface as a result of LD protocol.

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# loop-detection shutdown-disable
```

The following example reverts to default behavior.

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# no loop-detection shutdown-disable
```

The following example disables the shutdown of a VLAN VXLAN tunnel.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# loop-detection shutdown-disable
```

History

Release version	Command history
18x.1.00	This command was introduced.

loop-detection vlan

Associates a VLAN at the interface level to support the loop detection (LD) protocol.

Syntax

loop-detection vlan *vlan-id*

no loop-detection vlan

Command Default

This feature is disabled.

Parameters

vlan-id

Specifies a created VLAN. Range is from 1 through 4090.

Modes

Interface subtype configuration mode (Ethernet or port-channel)

Usage Guidelines

The VLAN must already be created.

This command applies to LD loose mode.

The **no** form of this command deletes LD support for all previously configured VLANs, deleting all LD configurations at the interface level.

Examples

To associate a VLAN to an Ethernet interface for LD support:

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# loop-detection vlan 20
```

To disassociate all previously configured VLANs from an Ethernet interface for LD support and delete all LD configurations at the Ethernet interface level:

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# no loop-detection vlan 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

ma-name

Creates a maintenance association (MA) within a specified domain. The command changes the maintenance domain mode to the specified maintenance association mode.

Syntax

ma-name *ma-name* [**id** *ma-id*] [**vlan-id** *vlan-id*] [**bridge-domain** *bridge-domain*] { **priority** *priority* }

no ma-name *ma-name*

Command Default

There are no MA configured.

Parameters

ma-name
Specifies the maintenance association name. The name attribute is case-sensitive.

ma-id
Specifies the short maid that is transmitted in the CCM PDU. This ID is unique. The range is 1 - 4090.

vlan-id
Specifies a unique VLAN identifier of the maintenance association in the range 1-4090. To create a MA, a vlan id must be set.

bridge-domain
Specifies a unique L2VPN domain of the maintenance association. This option supports only Virtual Private LAN Services (VPLS) in this release. VLL is not currently supported for CFM.

priority
Specifies the priority of the CCM messages sent by MEPs, in the range 0-7.

Modes

CFM protocol configuration mode

Usage Guidelines

The **no** form of the command removes the maintenance association.

Examples

This example demonstrates associating the MA "ma1" to VLAN 30.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 4
device(config-cfm-md-ma-ma1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

mac access-group

Applies rules specified in a MAC access control list (ACL) to traffic entering or exiting an interface.

Syntax

mac access-group *ACLname* { **in** | **out** }

no mac access-group *ACLname* { **in** | **out** }

Parameters

ACLname
Specifies the name of the standard or extended MAC access list.

in
Applies the ACL to incoming switched and routed traffic.

out
Applies the ACL to outgoing switched and routed traffic.

Modes

Interface-subtype configuration mode

Usage Guidelines

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

You can apply an ACL to multiple interfaces. And you can apply an ACL twice—ingress and egress—to a given user interface.

Layer 2 ACLs applied on VLANs do not affect tunnel-terminated packets.

To remove an ACL from an interface, enter the **no** form of this command.

Examples

The following example applies a MAC ACL to filter inbound packets only, on a specified Ethernet interface.

```
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# mac access-group macacl2 in
```

The following example removes a MAC ACL from a specified port-channel interface.

```
device(config)# interface port-channel 62
device(config-Port-channel-62)# no mac access-group macacl2 in
```

History

Release version	Command history
18x.1.00	This command was introduced.

mac access-list extended

Creates a MAC extended access control list (ACL).

Syntax

mac access-list extended *ACL-name*

no mac access-list extended *ACL-name*

Parameters

ACL-name

Specifies an ACL name unique among all ACLs (Layer 2 and Layer 3). The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore (_) and hyphen (-).

Modes

Global configuration mode

Usage Guidelines

If the ACL is already created, this command puts the device in MAC extended ACL configuration mode.

An extended ACL contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. Extended ACLs allow you to filter traffic based on the following:

- Source MAC address
- Destination MAC address
- EtherType

You can apply MAC extended ACLs to VLANs and to Layer 2 interfaces.

To enable ARP Guard, you also use a MAC extended ACL.

The **no** form of the command removes a MAC extended ACL from an interface.

Examples

The following example creates a MAC extended ACL named mac1.

```
device(config)# mac access-list extended mac1
```

The following example deletes a MAC extended ACL named mac1.

```
device(conf-macl-ext)# no mac access-list extended mac1
```

History

Release version	Command history
18x.1.00	This command was introduced.

mac access-list standard

Creates a standard MAC access control list (ACL). Standard ACLs contain rules that permit or deny traffic based on source addresses that you specify.

Syntax

mac access-list standard *ACLname*

no mac access-list standard *ACLname*

Parameters

ACLname

Specifies an ACL name unique among all ACLs (Layer 2 and Layer 3). The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

Use this command to create a standard MAC access list. If ACL is already created, this command puts the device in the standard MAC access-list configuration mode.

To remove a MAC ACL from an interface, enter the **no** form of this command.

Examples

The following command creates a MAC standard ACL named mac1.

```
device(config)# mac access-list standard mac1
device(conf-macl-std)#
```

The following command deletes a MAC standard ACL named mac1.

```
device(conf-macl-std)# no mac access-list standard mac1
```

History

Release version	Command history
18x.1.00	This command was introduced.

mac-address-table

Sets the aging time, sets mac-move parameters, and adds static addresses to the MAC address table.

Syntax

mac-address-table aging-time *aging-time*

no mac-address-table aging-time

mac-address-table mac-move { **detect** | **limit** *max-mac-moves* }

no mac-address-table mac-move limit

mac-address-table static *mac-addr* **forward ethernet** *slot/port* **vlan** *vlan-id*

no mac-address-table static *mac-addr* **forward ethernet** *slot/port* **vlan** *vlan-id*

mac-address-table static *mac-addr* **forward logical-interface ethernet** *logical-interface*

no mac-address-table static *mac-addr* **forward logical-interface ethernet** *logical-interface*

mac-address-table static *mac-addr* **forward port-channel** *port-channel-number* **vlan**

no mac-address-table static *mac-addr* **forward port-channel** *port-channel-number* **vlan**

Command Default

Aging time is 1800 seconds.

The MAC-move limit is 20 moves.

Parameters

aging-time *aging-time*
: Specifies the time in seconds that a learned MAC address will persist after the last update. If the aging time is set to zero (0), it means that aging is disabled. Otherwise, values range from 60 through 100000. The default is 1800 seconds.

mac-move
: Configures MAC-move detection.

  detect
  : Enables MAC-move detection.

  limit *max-mac-moves*
  : Specifies the MAC-move limit. Thre range is 5 through 500 moves. The default is 20 moves.

static *mac-addr* **forward**
: Specifies the Media Access Control (MAC) address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.

ethernet
: Specifies an Ethernet interface.

  slot
  : Specifies a valid slot number. The slot must be **0** for devices that do not support line cards.

port
Specifies a valid port number.

logical-interface *logical-interface*
Specifies a logical interface. Logical interfaces are the attachment circuit end-points bound to a bridge domain.

port-channel *number*
Specifies the port-channel number. Valid values range from 1 through 63.

vlan *vlan-id*
Specifies an active VLAN. Values range from 1 through 4090.

Modes

Global configuration mode

Usage Guidelines

The **vlan** keyword is mandatory because the switch only supports independent VLAN learning (IVL).

To restore the default MAC aging time of 1800 seconds, use the **no mac-address-table aging-time** option.

To restore the default MAC-move limit of 20 moves, use the **no mac-address-table mac-move limit** option.

To delete a static MAC address for forwarding to a physical interface, use the **no mac-address-table static** *mac-addr* **forward ethernet** *slot/port* **vlan** *vlan-id* option.

To delete a static MAC address for forwarding to a logical interface, use the **no mac-address-table static** *mac-addr* **forward logical-interface ethernet** *logical-interface* **vlan** *vlan-id* option.

To delete a static MAC address for forwarding to a port-channel interface, use the **no mac-address-table static** *mac-addr* **forward port-channel** *port-channel-number* **vlan** option.

Examples

The following example adds a static address to the MAC address table, with forwarding to a physical interface.

```
device# configure terminal
device(config)# mac-address-table static 0011.2222.3333 forward ethernet 0/1 vlan 100
```

The following example adds a static address to the MAC address table, with forwarding to a logical interface.

```
device# configure terminal
device(config)#mac-address-table static 0000.1111.2222 forward logical-interface ethernet 0/43.100
```

The following example sets the aging time to 600 seconds.

```
device# configure terminal
device(config)# mac-address-table aging-time 600
```

The following example restores aging time to its default value of 1800 seconds.

```
device# configure terminal
device(config)# no mac-address-table aging-time
```

The following example disables aging time by setting its value to 0.

```
device# configure terminal
device(config)# mac-address-table aging-time 0
```

The following example deletes a static MAC address forwarding on a physical interface.

```
device# configure terminal
device(config)# no mac-address-table static aaaa.bbbb.cccc forward ethernet 0/1 vlan 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

maid-format

Sets the Maintenance Association Identifier (MAID) format for a particular maintenance association (MA).

Syntax

maid format [**long** | **default**]

Command Default

The default maid format is short.

Parameters

long

Specifies maid format as long.

default

Specifies maid format as default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command reverts back the maid format to **short**.

You cannot change the MAID format after a MEP is configured under an MA. You must first delete the MEP and then change the MAID format.

Examples

The following example sets the MAID format to long.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 30 vlan-id 30 priority 7
device(config-cfm-md-md1)# maid-format long
```

History

Release version	Command history
18x.1.00	This command was introduced.

map bridge-domain (overlay gateway)

Maps a bridge domain (BD) to a Virtual Network Identifier (VNI) for a VXLAN overlay gateway.

Syntax

map bridge-domain *bridge_domain_id* **vni** *vni*

no map bridge-domain *bridge_domain_id* **vni** *vni*

Parameters

bridge_domain_id
Specifies a bridge domain. Enter an integer from 1 through 4096.

vni *vni*
Specifies a VNI. Enter an integer from 1 through 16777215.

Modes

Overlay gateway configuration mode

Usage Guidelines

Use the **no** form of this command to remove the mapping.

Examples

The following example maps a bridge domain to a VNI.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# map bridge-domain 1 vni 999
```

History

Release version	Command history
18x.1.00	This command was introduced.

map dscp

Maps an ingress DSCP value to an outbound CoS, DSCP, or traffic-class value for a QoS DSCP-to-CoS, DSCP-mutation, or DSCP-to-traffic class map.

Syntax

map dscp *dscp-value* **to** { **cos** *cos-value* } | { **dscp** *dscp-out* } | { **traffic-class** *tc-value* }

no map dscp *dscp-value*

Command Default

The default values for DSCP to CoS, DSCP mutation, or DSCP to traffic class mapping.

Parameters

dscp-value
Specifies the ingress DSCP value or range. Enter an integer from 0 to 63.

cos *cos-value*
Specifies the outbound CoS value. Enter an integer from 0 to 7.

dscp *dscp-out*
Specifies the outbound DSCP value or range. Enter an integer from 0 to 63.

traffic-class *tc-value*
Specifies the outbound Traffic Class value. Enter an integer from 0 to 7.

Modes

DSCP CoS configuration mode

DSCP mutation configuration mode

DSCP traffic-class configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default mapping values.

Examples

In DSCP COS configuration mode, the following example maps an ingress DSCP value to an egress CoS value.

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)# map dscp 43 to cos 4
```

In DSCP mutation configuration mode, the following example maps the ingress DSCP values to an egress DSCP value.

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)# map dscp 1,3,5,7 to dscp 40
```

In DSCP traffic configuration mode, the following example maps the ingress DSCP values to a traffic class.

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)# map dscp 1,3,5,7 to traffic-class 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

map vlan

In a VXLAN overlay gateway configuration that uses Layer 2 extension, associates VLANs with VXLAN Network Identifiers (VNIs).

Syntax

map vlan [*vlan_id*] {**vni** } [*vni*] [**auto**]

no map vlan *vlan_id*

no map vlan vni

Parameters

vlan_id
: A single VLAN ID or range of VLAN IDs. The range is from 1 through 8191. See the Usage Guidelines.

vni
: Specifies the VNI (VXLAN Network Identifier) token.

  vni
  : A single VXLAN VNI or range of VXLAN VNIs. Range is from 1 through 16777215. See the Usage Guidelines.

auto
: Enables automatic VLAN-to-VNI mapping for every VLAN associated with the tunnel.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Note the following conditions:

- Before using this command, you must first set the VXLAN overlay gateway to **layer2-extension**, by means of the **type** command.
- Before using this command, you must first configure the appropriate VLANs to be used by the gateway.
- Before mapping VLANs to VNIs manually, you cannot have automatic mapping configured (by means of the **map vlan vni auto** command).
- You cannot map one VLAN to multiple VNIs. Similarly, you cannot map a single VNI to multiple VLANs. For example, VLAN-to-VNI mapping should be one to one.
- A single VLAN ID and a range of VLAN IDs can both be specified in a single command as follows: *x,y-z*. The same applies to VNIs.
- When using ranges, you must ensure that the number of values in a VLAN ID range corresponds to the number of values in a VNI range.
- The **no** forms of this command are allowed only if no VLANs are referenced by means of the **extend vlan** command (under a submode of the **site** command). For example, VLANs extended to a site should have a VNI mapping.

- The **no map vlan vni auto** command disables the automatic assignment of VNIs. It is not allowed if manual VLAN-to-VNI mappings have been configured. For example, "auto" VLAN-to-VNI mapping and "explicit" VLAN-to-VNI mapping are mutually exclusive.
- The **no map vlan** *vlan_id* command removes the VNI mappings for one or more VLANs.
- You cannot delete a VLAN (by means of the **no interface vlan** command) that is referenced by means of the **map vlan vni** command.
- This command does not trigger VLAN provisioning, unlike the behavior of the **attach vlan** command.

Examples

To configure a manual mapping of VLANs to VNIs in "gateway1":

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# map vlan 10,20-22 vni 5000-5002,6000
```

This results in the following in the running configuration:

```
overlay-gateway gateway1
  type layer2-extension mode vxlan-ipv4
  map vlan 10 vni 5000
  map vlan 20 vni 5001
  map vlan 21 vni 5002
  map vlan 22 vni 6000
```

To configure an automatic mapping of VLANs to VNIs in "gateway1":

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# map vlan vni auto
```

History

Release version	Command history
18x.1.00	This command was introduced.

map vni auto (VXLAN gateway)

Configures an automatic mapping of VLANs/bridge domains (BDs) to Virtual Network Identifiers (VNIs).

Syntax

map vni { **auto** }

map vni { **auto** }

Command Default

This feature is not enabled.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Use the **no** form of this command to undo the automatic mapping.

Examples

The following example configures the automatic mapping of VLANs/BDs) to VNIs.

```
device# configure terminal
device(config)# overlay-gatgeway mygateway
device(config-overlay-gateway-mygateway)# map vni auto
```

The following example undoes the mapping.

```
device# configure terminal
device(config)# overlay-gatgeway mygateway
device(config-overlay-gateway-mygateway)# no map vni auto
```

History

Release version	Command history
18x.1.00	This command was introduced.

master-vlan (STP)

Selects a master VLAN for a topology group.

Syntax

master-vlan *vlan_id*

Command Default

The master VLAN is not configured.

Parameters

vlan_id

The master VLAN ID.

Modes

Topology group configuration mode.

Usage Guidelines

To configure a master VLAN, the VLAN must already be configured. The master VLAN contains the STP settings for all the VLANs in the STP per VLAN group. An STP group can have only one master VLAN. If you add a new master VLAN to an STP group that already has a master VLAN, the new master VLAN replaces the older master VLAN.

If you remove the master VLAN (by entering the **no master-vlan** command), the software selects the new master VLAN from member VLANs. A new candidate master VLAN will be in configured as a member VLAN so that the first added member VLAN will be a new candidate master VLAN. Once you save and reload, a member VLAN with the youngest VLAN ID will be the new candidate master.

Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
```

History

Release version	Command history
18x.1.00	This command was introduced.

match (route maps)

Defines a variety of match conditions for a route map.

Syntax

match as-path *name*

match community *name* **exact-match**]

match extcommunity *number*

match interface { **ethernet** *slot* **/** *port* | **loopback** *num*| **ve-interface** *vlan_id* }

match ip address { **acl** *name* [**prefix-list** *string*] | **prefix-list** *string* [**acl** *name* }

match ip next-hop prefix-list *string*

match ip route-source prefix-list *string*

match ipv6 next-hop prefix-list *string*

match ipv6 route-source prefix-list *string*

match metric *num*

match protocol bgp { **external** | **internal** | **static-network** }

match protocol static

match route-type { **internal** | **type-1** | **type-2** }

match tag *num*

match vrf *name*

no match as-path

no match community

no match extcommunity

no match interface

no match ip address

no match ip next-hop

no match ip route-source

no match ipv6 address

no match ipv6 next-hop

no match ipv6 route-source

no match metric

no match protoocol

no match route-type

no match tag

Command Default

This option is disabled.

Parameters

as-path

Matches an AS-path access list name in a route-map instance.

name

Name of an AS-path access list. Range is from 1 through 32 ASCII characters.

community

Matches a BGP community access list name in a route-map instance.

name

Name of a BGP community access list. Values range from 1 through 32 ASCII characters.

exact-match

Matches a route only if the route community attributes field contains the same community numbers specified in the **match** statement.

extcommunity *number*

Matches a BGP extended community list in a route-map instance and specifies an extended community list number. Valid values range from 1 through 99.

interface

Matches interface conditions in a route-map instance.

ethernet

Specifies an ethernet interface.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback *num*

Specifies a loopback interface.

ve-interface *vlan_id*

Specifies a virtual Ethernet VLAN interface.

ip address

Matches an IP address in a route-map instance.

acl *name*

Name of the access list. Range is from 1 through 32 ASCII characters.

prefix-list *string*

Specifies an IP prefix list. Range is from 1 through 32 ASCII characters.

ip next-hop

Matches IP next-hop match conditions in a route-map instance.

ip route-source

Matches an IP route source in a route-map instance.

ipv6 address
Matches an IPv6 address in a route-map instance.

ipv6 next-hop
Matches IPv6 next-hop match conditions in a route-map instance.

ipv6 route-source
Matches an IPv6 route source in a route-map instance.

metric *num*
Matches a route metric in a route-map instance. Values range from 0 through 4294967295.

protocol bgp external
Matches on BGP routes.

protocol bgp internal
Matches on iBGP routes.

protocol bgp static-network
Matches on BGP4 static network routes. This is applicable only for BGP outbound policy.

protocol static
Matches on static routes.

route-type
Matches a route type in a route-map instance.

internal
Internal route type

type-1
OSPF external route type 1

type-2
OSPF external route type 2

tag *tag-value*
Specifies a route tag and route tag value.

vrf *name*
Specifies a non-default VRF. Valid values range from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

Route-maps are currently supported only under Border Gateway Patrol (BGP).

The **no** form of the command restores the default.

Examples

The following example matches AS-path ACL 1 in route-map instance “myroutes”.

```
device#configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map myroutes/permit/10)# match as-path 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

match access-group

Matches an ACL to a class map.

Syntax

match access-group *name*

Parameters

name

The ACL name.

Modes

Class map configuration mode.

Usage Guidelines

The command is used after the **class-map** command is entered.

Examples

Use this command to match an ACL to a class map.

```
device(config)# class-map default
device(config-classmap)# match access-group class_acl
```

History

Release version	Command history
18x.1.00	This command was introduced.

match additional-paths advertise-set

Enables filtering of additional-paths to be advertised for a route map.

Syntax

match additional-paths advertise-set [**all**] [**best** *num*] [**best-range** *start-num end-num*] [**group-best**]

no match additional-paths [**all**] **advertise-set** [**best** *num*] [**best-range** *start-num end-num*] [**group-best**]

Command Default

By default, a route map is not configured to filter advertised paths.

Parameters

all
Causes all (up to a maximum of 16) routes to be advertised.

best *num*
Specifies the number of best routes to advertise.

best-range
Causes advertisement of routes within a number range.

start-num
Specifies the start number of the range of routes to advertise. The number ranges from 1 through 16.

end-num
Specifies the end number of the range of routes to advertise. The number ranges from 1 through 16.

group-best
Advertises the group-best path.

Modes

Route-map configuration mode

Usage Guidelines

A match occurs when an additional path that is a candidate for advertisement has the same path marking (tag) as the marking configured by using the **match additional-paths advertise-set** command.

Only one **match additional-paths advertise-set** command configuration is allowed for each route map; any subsequent **match additional-paths advertise-set** command configuration overwrites the previous configuration.

The **no** form of the command restores the default configuration.

Examples

The following example shows how to configure route map (rm_example) to advertise the group-best route.

```
device# configure terminal
device(config)# route-map rm_example permit 123
device(config-routemap-rm_example/permit/123)# match additional-paths advertise-set group-best
```

History

Release version	Command history
18x.1.00	This command was introduced.

match bridge-domain

Matches a bridge domain to a class map.

Syntax

match bridge-domain *BD-number*

Parameters

BD-number

Specifies a valid bridge-domain number.

Modes

Class map configuration mode.

Usage Guidelines

The command is used after the **class-map** command is entered.

Examples

The following example matches a bridge domain to a class map.

```
device(config)# class-map BD-1000
device(config-classmap)# match bridge-domain 1000
```

History

Release version	Command history
18x.1.00	This command was introduced.

match community

Matches a community access list name in a route-map instance.

Syntax

match community *name*

no match community

Parameters

name

Name of a community access list. Values range from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Enter **no match community** *name* to disable this feature.

You can configure up to five match community directives within a single stanza.

Examples

Typical command example:

```
device# config terminal
device(config)# route-map myroutes permit 10
device(config-route-map myroutes/permit/10)# match community ABCPath
```

History

Release version	Command history
18x.1.00	This command was introduced.

match extcommunity

Matches an extended community list in a route-map instance.

Syntax

match extcommunity *number*

no match extcommunity

Command Default

BGP extended community access list names are not matched.

Parameters

name

Extended community list number. Values range from 1 through 99.

Modes

Route-map configuration mode.

Usage Guidelines

Enter **no match extcommunity** to remove the community match statement from the configuration file.

You can configure up to five match extcommunity directives within a single stanza.

Examples

To configure a route map that matches on extended community ACL 1.

```
device# configure terminal
device(config)# ip extcommunity-list 1 permit 123:2
device(config)# route-map extComRmap permit 10
device(config-route-map-extComRmap/permit/10)# match extcommunity 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

match vlan

Matches a VLAN to a class map.

Syntax

match vlan *VLAN-number*

Parameters

VLAN-number
Specifies a valid VLAN number.

Modes

Class map configuration mode.

Usage Guidelines

The command is used after the **class-map** command is entered.

Examples

The following example matches a VLAN to a class map.

```
device(config)# class-map p2
device(config-classmap)# match vlan 500
```

History

Release version	Command history
18x.1.00	This command was introduced.

max-age

Sets the interval time in seconds between messages that the spanning tree receives from the interface.

Syntax

max-age *seconds*

no max-age

Command Default

20 seconds.

Parameters

seconds

Configures the STP interface maximum age. Valid values range from 6 through 40.

Modes

Spanning tree configuration mode

Usage Guidelines

Use this command to control the maximum length of time that passes before an interface saves its configuration Bridge Protocol Data Unit (BPDU) information.

If the **vlan** parameter is not provided, the *seconds* value is applied globally for all per-VLAN instances. However, for VLANs that have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

When configuring the maximum age, the **max-age** command setting must be greater than the **hello-time** command setting. The following relationship should be kept:

```
(2 × (forward-delay - 1)) >= max-age >= (2 × (hello-time + 1))
```

Enter **no max-age** to return to the default configuration.

Examples

To configure the maximum age to 10 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# max-age 10

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# max-age 10

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# max-age 10

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# max-age 10

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# max-age 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

max-mcache

Configures the maximum multicast cache size.

Syntax

max-mcache *num*

no max-mcache

Command Default

Multicast cache size is 24576 entries.

Parameters

num

Number of entries in the multicast cache. Valid values range from 1 through 24576.

Modes

Router PIM configuration mode

Usage Guidelines

Entering the **no** form of the command sets the maximum multicast cache size to the default - 24576 entries.

Examples

Setting the multicast cache to 500 entries.

```
device(config)# router pim
device(conf-pim-router)# max-mcache 500
```

max-metric router-lsa

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Syntax

max-metric router-lsa [**all-vrfs**] [**all-lsas** | **external-lsa** *metric-value* | **link** { **all** | **ptp** | **stub** | **transit** } | **summary-lsa** *metric-value* | **on-startup** { *time* | **wait-for-bgp** [**all-lsas** | **summary-lsa** *metric-value* | **external-lsa** *metric-value* | **link** { **all** | **ptp** | **stub** | **transit** }] }]

no max-metric router-lsa [**all-vrfs**] [**all-lsas** | **external-lsa** | **link** { **all** | **ptp** | **stub** | **transit** } | **summary-lsa** | **on-startup** { *time* | **wait-for-bgp** [**all-lsas** | **link** [**all**]] }]

Parameters

all-vrfs
Applies the configuration change to all instances of OSPF.

all-lsas
Sets the **summary-lsa** and **external-lsa** optional parameters to the corresponding default max-metric value. For a non-default instance of OSPF, only the summary-lsa and external-lsa parameters are set.

external-lsa *metric-value*
Modifies the metric of all external type 5 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

link
Specifies the types of links for which the maximum metric is advertised. By default, the maximum metric is advertised only for transit links.

all
Advertises the maximum metric in Router LSAs for all supported link types.

ptp
Advertises the maximum metric in Router LSAs for point-to-point links.

stub
Advertises the maximum metric in Router LSAs for stub links.

transit
Advertises the maximum metric in Router LSAs for transit links. This is the default link type.

summary-lsa *metric-value*
Modifies the metric of all summary type 3 and type 4 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777215 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

on-startup
Applies the configuration change at the next OSPF startup.

time
Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for *time* is 5 to 86,400.

wait-for-bgp

Indicates that OSPF should wait for either 600 seconds or until BGP has finished route table convergence, whichever happens first, before advertising the links with the normal metric.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the device becomes a stub router, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.
- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

Enter **no max-metric router-lsa all-lsas** to disable advertising the maximum metric value in different LSAs.

Examples

The following example advertises the maximum metric value using the **all-lsas** option.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# max-metric router-lsa all-lsas
```

History

Release version	Command history
18x.1.00	This command was introduced.

max-metric router-lsa (OSPFv3)

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Syntax

max-metric router-lsa [**all-lsas** | **external-lsa** *metric-value* | **include-stub** | **on-startup** { *time* | **wait-for-bgp** } | **summary-lsa** *metric-value*]

no max-metric router-lsa [**all-lsas** | **external-lsa** | **include-stub** | **on-startup** { *time* | **wait-for-bgp** } | **summary-lsa**]

Parameters

all-lsas

Sets the **summary-lsa** and **external-lsa** optional parameters to the corresponding default max-metric value. For a non-default instance of OSPFv3, only the summary-lsa and external-lsa parameters are set.

external-lsa *metric-value*

Configures the maximum metric value for all external type-5 and type-7 LSAs. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

include-stub

Specifies the advertisement of the maximum metric value for point-to-point and broadcast stub links in the intra-area-prefix LSA..

on-startup

Applies the configuration change at the next OSPF startup.

time

Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for *time* is 5 to 86400.

wait-for-bgp

Specifies that OSPFv3 should wait until BGP has finished route table convergence before advertising the links with the normal metric, or for no more than 600 seconds.

summary-lsa *metric-value*

Configures the maximum metric value for all summary type 3 and type 4 LSAs. The range for metric value is 1 to 16777215 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the device becomes a stub router, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.
- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

Enter **no max-metric router-lsa** to disable advertising the maximum metric value in different LSAs.

Examples

The following example configures an OSPFv3 device to advertise a maximum metric and sets the maximum metric value for all external type-5 and type-7 LSAs to 1000.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa external-lsa 1000
```

The following example configures an OSPFv3 device to advertise a maximum metric and specifies the advertisement of the maximum metric value for point-to-point and broadcast stub links in the intra-area-prefix LSA.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa include-stub
```

The following example configures an OSPFv3 device to advertise a maximum metric until BGP routing tables converge or until the default timer of 600 seconds expires.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa on-startup wait-for-bgp
```

The following example configures an OSPFv3 device to advertise a maximum metric and sets the maximum metric value for all summary type-3 and type-4 LSAs to 100.

History

Release version	Command history
18x.1.00	This command was introduced.

maxas-limit

Imposes a limit on the number of autonomous systems in the AS-PATH attribute.

Syntax

maxas-limit in *num*

no maxas-limit in

Command Default

Disabled.

Parameters

in

Allows an AS-PATH attribute from any neighbor to impose a limit on the number of autonomous systems.

num

Range is from 0 through 300. The default is 300.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

This example sets the limit on the number of BGP4 autonomous systems in the AS-PATH attribute to 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maxas-limit in 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

maximum-paths (BGP)

Sets the maximum number of BGP4 and BGP4+ shared paths.

Syntax

maximum-paths *num* | **use-load-sharing**

no maximum-paths

Command Default

Disabled.

Parameters

num

Specifies the maximum number of paths across which the device balances traffic to a given BGP destination. Valid values range is from 1 through 64. The default is 1.

use-load-sharing

Uses the maximum IP ECMP path value supported (64) without enabling BGP level ECMP.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use this command to change the maximum number of BGP4 shared paths, either by setting a value or using the maximum IP ECMP path value supported (64) without enabling BGP level ECMP.

If the configured *num* value is less than the possible number of ECMP paths available, BGP routes may not take the same number of ECMP paths. The set of ECMP paths may not be the same for different prefixes.

The **no** form of the command restores the default.

Examples

This example sets the maximum number of BGP4 shared paths to 8.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maximum-paths 8
```

This example sets the maximum number of BGP4+ shared paths to 64 without enabling BGP level ECMP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# maximum-paths use-load-sharing
```

This example sets the maximum number of BGP shared paths to 2 in a nondefault VRF instance in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# maximum-paths 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

maximum-paths (OSPF)

Changes the maximum number of OSPF shared paths.

Syntax

maximum-paths *num*

no maximum-paths

Parameters

num

Maximum number of paths across which the device balances traffic to a given OSPF destination. The range is from 1 through 64. The default is 8.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following example sets the maximum number of shared paths to 22.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# maximum-paths 22
```

History

Release version	Command history
18x.1.00	This command was introduced.

maximum-paths ebgp ibgp

Specifies the number of equal-cost multipath eBGP or iBGP routes or paths that are selected.

Syntax

maximum-paths { **ebgp** *num* | **ibgp** *num* }

no maximum-paths

Command Default

This option is disabled.

Parameters

ebgp

Specifies eBGP routes or paths.

ibgp

Specifies iBGP routes or paths.

num

The number of equal-cost multipath routes or paths that are selected. Range is from 1 through 64. 1 disables equal-cost multipath.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Enhancements to BGP load sharing support the load sharing of BGP4 and BGP4+ routes in IP Equal-Cost Multipath (ECMP), even if the BGP multipath load-sharing feature is not enabled by means of the **use-load-sharing** option for the **maximum-paths** command. You can set separate values for IGMP and ECMP load sharing. Use this command to specify the number of equal-cost multipath eBGP or iBGP routes or paths that are selected.

Examples

This example sets the number of equal-cost multipath eBGP routes or paths that will be selected to 6 in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maximum-paths ebgp 6
```

This example sets the number of equal-cost multipath iBGP routes or paths that will be selected to 4 in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# maximum-paths ibgp 4
```

This example sets the number of equal-cost multipath EBGP routes or paths that will be selected to 3 for the IPv4 address family for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# maximum-paths ebgp 3
```

History

Release version	Command history
18x.1.00	This command was introduced.

measurement-interval

Configures the SLM Measurement interval for Connectivity Fault Management (CFM).

Syntax

measurement-interval { *interval* }

no measurement-interval

Command Default

The default interval is fifteen minutes.

Parameters

interval

The interval period, in minutes. The range of valid vaules is from 1 through 1440.

Modes

CFM protocol configuration mode

Y.1731 configuration mode

Usage Guidelines

The **no measurement-interval** command resets the interval to the default value.

Examples

Example of setting the interval when configured for VLAN 30.

```
device# configure terminal
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 pri 7
device(config-cfm-md-ma-ma1)# measurement interval 25
```

Example of configuring the interval for Y.1731 configuration mode.

```
device# configure terminal
device(config)# protocol cfm
device(protocol-cfm)# y1731
device(protocol-cfm-y1731)# test-profile my_test_profile
device(protocol-cfm-y1731-my_test_profile)# measurement-interval 20
device(protocol-cfm-y1731-my_test_profile)# exit
```

History

Release version	Command history
18x.1.00	This command was introduced.

med-missing-as-worst

Configures the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

Syntax

med-missing-as-worst

no med-missing-as-worst

Modes

BGP configuration mode

Usage Guidelines

When MEDs are compared, by default the device favors a low MED over a higher one. Because the device assigns a value of 0 to a route path MED if the MED value is missing, the default MED comparison results in the device favoring the route paths that do not have MEDs.

The **no** form of the command restores the default where a device does not favor a route that has a MED over other routes.

Examples

The following example configures the device to favor a route containing a MED.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# med-missing-as-worst
```

History

Release version	Command history
18x.1.00	This command was introduced.

member-bridge-domain

Configures member bridge domains for a topology group.

Syntax

member-bridge-domain { **add** | **remove** } *bridge_domain_id*

Command Default

The topology group has no member bridge domains.

Parameters

add

Add a bridge domain to the topology group.

remove

Remove a bridge domain from the topology group.

bridge_domain_id

Bridge domain ID or the bridge domain range; for example: 1, 2, 4-7, 8, 9-22, 55-66. Tha maximun is 253 characters.

Modes

Topology group configuration mode.

Usage Guidelines

You must first add a master VLAN to the topology group.

Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
device(config-topo-group-10)# member-bridge-domain add 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

member-vlan (STP)

Adds member VLANs to an STP topology group.

Syntax

member-vlan { **add** | **remove** } *vlan_id*

Command Default

The topology group has no member VLANs.

Parameters

add

Add a VLAN to the topology group.

remove

Remove a VLAN from the topology group.

vlan_id

Adds a member VLAN ID to the STP topology group. This can be a single VLAN or a range of VLANs. For example: 2, 4-7, 8, 9-22, 55-66. The maximum input is 253 characters.

Modes

Topology group configuration mode.

Usage Guidelines

The VLAN(s) must be configured before adding to the topology group.

You must first add a master VLAN to the topology group.

All the VLANs in the member group inherit the STP settings of the master VLAN in the group.

Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
device(config-topo-group-10)# member-vlan add 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

mep

Adds local ports as Maintenance End Points (MEP) to a specific Maintenance Association (MA).

Syntax

mep { *mep-id* [**up** | **down**] | [**vlan** *vlan-id*] | [**ethernet** *slot/ port*] | [**port-channel** *channel*]

no mep *mep-id*

Command Default

There are no MEP configured.

Parameters

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

inner-vlan *vlan-id*
Specifies the Inner VLAN.

port-channel *index*
Specifies a port-channel.

vlan *vlan-id*
Specifies a VLAN.

Modes

CFM protocol configuration mode

Usage Guidelines

The **no mep** command deletes the MEP from the MA.

A Maintenance Domain (MD) is part of a network controlled by a single operator. The MD levels are carried on all CFM frames to identify different domains. Every MD can be further divided into smaller networks having multiple Maintenance End Points (MEP). Usually an MA is associated with a service instances (for example a VLAN or a VPLS).

MEP is located on the edge of an MA. It defines the endpoint of the MA. Each MEP has unique ID (MEPID) within MA. The connectivity in a MA is defined as connectivity between MEPs. The MEP generates Continuity Check Message and multicasts to all the other MEPs in the same MA to verify connectivity.

Each MEP has a direction, down or up. Down MEP receives CFM PDUs from the LAN and sends CFM PDUs towards the LAN. Up MEP receives CFM PDUs from a bridge relay entity and sends CFM PDUs towards the bridge relay entity on a bridge. End stations support down MEPs only, as they have no bridge relay entities.

Examples

Example defining a MEP for VLAN 30 in the down direction.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
device(config-cfm-md-ma-ma1)# mep 1 down ethernet 1/2
```

History

Release version	Command history
18x.1.00	This command was introduced.

message-interval

Configures the Protocol Independent Multicast (PIM) Join or Prune message interval.

Syntax

message-interval *num*

no message-interval *num*

Command Default

60 seconds

Parameters

num

The interval value in seconds. Valid values range from 10 through 65535 seconds.

Modes

Router PIM configuration mode

Usage Guidelines

Use this command to specify the interval at which the periodic PIM Join or Prune messages must be sent out.

Enter the **no** form of the command to disable this feature.

Examples

Setting the interval to one hour.

```
device(config)# router pim
device(conf-pim-router)# message-interval 3600
```

History

Release version	Command history
18x.1.00	This command was introduced.

metric-type

Configures the default metric type for external routes.

Syntax

metric-type { **type1** | **type2** }

no metric-type { **type1** | **type2** }

Command Default

Type 1

Parameters

type1

The metric of a neighbor is the cost between itself and the device plus the cost of using this device for routing to the rest of the world.

type2

The metric of a neighbor is the total cost from the redistributing device to the rest of the world.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default setting. You must specify a type parameter when using the **no** form.

Examples

The following example sets the default metric type for external routes to type 2.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# metric-type type2
```

History

Release version	Command history
18x.1.00	This command was introduced.

minimum-links

Configures the minimum bandwidth or number of links to be running to allow the port-channel to function.

Syntax

minimum-links *num-of-links*

no minimum-links

Command Default

Number of links is 1.

Parameters

num-of-links

The number of links. Valid values range from 1 through 32.

Modes

Port-channel interface configuration mode

Usage Guidelines

Use this command to allow a port-channel to operate at a certain minimum bandwidth all the time. If the bandwidth of the port-channel drops below that minimum number, then the port-channel is declared operationally DOWN even though it has operationally UP members.

Enter **no minimum-links** to restore the default value.

Examples

The following example sets the minimum number of links to 16 on a specific port-channel interface.

```
device# configure terminal
device(config)# interface port-channel 33
device(config-Port-channel-33)# minimum-links 16
```

History

Release version	Command history
18x.1.00	This command was introduced.

mip-policy

Specifies the conditions in which Maintenance Intermediate Points (MIP) are automatically created on ports.

Syntax

mip-policy { **explicit** | **default** }

no mip-policy

Command Default

The MIP policy is set to **default**.

Parameters

explicit

Specifies that explicit MIPs are configured only if a MEP exists on a lower MD Level.

default

Specifies that MIPs are always configured.

Modes

CFM protocol configuration mode .

Usage Guidelines

Use the **no mip-policy** to reset the values to the default.

A Maintenance Intermediate Point (MIP) can be created on a port and VLAN automatically, but only when either the explicit or default policy has been defined for them. For a specific port and VLAN, a MIP is created at the lowest level. Additionally, the level created should be the next higher than the MEP level defined for the port and VLAN.

Use the **explicit** parameter to specify that explicit MIPs are configured only if a MEP exists on a lower Maintenance Domain (MD) level.

Use the **default** parameter to specify that MIPs are always configured.

Examples

Example of the MIP policy command set for explicit when configured for VLAN 30.

```
device# configure terminal
device(config-cfm)#domain name md1 level 4
device(config-cfm-md-md1)#ma-name ma1 id 1 vlan-id 30 pri 7
device(config-cfm-md-ma-ma1)#mip-policy explicit
```

History

Release version	Command history
18x.1.00	This command was introduced.

mode (LLDP)

Sets the LLDP mode on the device.

Syntax

mode { **tx** | **rx** }

Command Default

Both transmit and receive modes are enabled.

Parameters

tx

Specifies to enable only the transmit mode.

rx

Specifies to enable only the receive mode.

Modes

Protocol LLDP configuration mode

Examples

To enable only the transmit mode:

```
device(conf-lldp)# mode tx
```

To enable only the receive mode:

```
device(conf-lldp)# mode rx
```

History

Release version	Command history
18x.1.00	This command was introduced.

mode gre ip

Enables generic routing encapsulation (GRE) over a tunnel interface and specifies that the tunneling protocol is IPv4.

Syntax

mode gre ip

no mode

Command Default

GRE is disabled.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no mode gre ip** command to disable the GRE IP tunnel encapsulation method for the tunnel interface.

Examples

This example enables GRE IP encapsulation on a tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
```

History

Release version	Command history
18x.1.00	This command was introduced.

monitor session

Enables a Port Mirroring session for monitoring traffic.

Syntax

monitor session *session_number*

no monitor session *session_number*

Parameters

session_number
Specifies a session identification number. Valid values range from 1 through 512.

Modes

Global configuration mode

Usage Guidelines

Enter **no monitor session** to delete the port mirroring session.

Examples

To enable session 22 for monitoring traffic:

```
device# configure terminal
device(config)# monitor session 22
```

History

Release version	Command history
18x.1.00	This command was introduced.

mtu (interface)

Configures the Layer 2 maximum transmission unit (MTU) size for all Ethernet interfaces and Port-channels.

Syntax

mtu *number*

no mtu

Command Default

The default is 1548 bytes.

Parameters

number

Size of the Layer 2 MTU in bytes. Range is from 1548 through 9216.

Modes

Global configuration mode

Interface configuration mode for an Ethernet or port-channel interface

Usage Guidelines

This command can be executed both globally and on an interface. If it is executed globally, interface configurations take precedence over the global configuration.

Use the **no** form of this command to revert to the default.

Examples

The following example configures the Layer 2 MTU size globally.

```
device# configure terminal
device(config)# mtu 2000
```

The following example configures the Layer 2 MTU size on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/13
device(conf-if-eth-1/13)# mtu 2000
```

The following example configures the Layer 2 MTU size on a port-channel interface.

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)# mtu 2000
```

History

Release version	Command history
18x.1.00	This command was introduced.

mtu (PW)

Configures the maximum transmission unit (MTU) for a pseudowire (PW) profile.

Syntax

mtu *mtu-value*

no mtu

Command Default

The MTU value is set to 1500.

Parameters

mtu-value

Specifies the maximum transmission unit (MTU) for the PW profile. Values range from 64 through 15966.

Modes

Pseudowire-profile configuration mode.

Usage Guidelines

The **no** form of the command restores the default configuration.

Examples

The following example shows how to set the MTU value to 2000 for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# mtu 2000
```

History

Release version	Command history
18x.1.00	This command was introduced.

mtu-enforce

Configures MTU enforcement check for a pseudowire (PW) profile.

Syntax

mtu-enforce { *false* | *true* }

no mtu-enforce

Command Default

MTU enforcement is disabled.

Parameters

false

Disables the MTU enforcement check.

true

Enables the MTU enforcement check.

Modes

Pseudowire-profile configuration mode.

Usage Guidelines

MTU enforcement is only supported during PW signaling.

The **no** form of the command restores the default value.

Examples

The following example shows how to enable MTU enforcement check for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# mtu-enforce true
```

History

Release version	Command history
18x.1.00	This command was introduced.

multipath

Changes load sharing to apply to only iBGP or eBGP paths, or to support load sharing among paths from different neighboring autonomous systems.

Syntax

multipath { **ebgp** | **ibgp** | **multi-as** }

no multipath { **ebgp** | **ibgp** | **multi-as** }

Command Default

This option is disabled.

Parameters

ebgp
Enables load sharing of eBGP paths only.

ibgp
Enables load sharing of iBGP paths only.

multi-as
Enables load sharing of paths from different neighboring autonomous systems.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

By default, when BGP load sharing is enabled, both iBGP and eBGP paths are eligible for load sharing, while paths from different neighboring autonomous systems are not.

Examples

This example changes load sharing to apply to iBGP paths in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# multipath ibgp
```

This example enables load sharing of paths from different neighboring autonomous systems in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# multipath multi-as
```

This example changes load sharing to apply to eBGP paths in IPv4 VRF instance "red":

```
device# configure terminal
device(config)# rrouter bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# multipath ebgp
```

History

Release version	Command history
18x.1.00	This command was introduced.

multiplier (LLDP)

Sets the number of consecutive misses of hello messages before LLDP declares the neighbor as dead.

Syntax

multiplier *value*

no multiplier

Command Default

Multiplier default value is 4.

Parameters

value

Specifies a multiplier value to use. Valid values range from 2 through 10.

Modes

Protocol LLDP and profile configuration modes

Usage Guidelines

Enter **no multiplier** to return to the default setting.

The LLDP multipler can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

Examples

To set the number of consecutive misses:

```
device(conf-lldp)# multiplier 2
```

To set the number of consecutive misses for a specific LLDP profile:

```
device(conf-lldp)# profile test1
device(config-profile-test1)# multiplier 5
device(config-profile-test1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

Commands N - Q

nbr-timeout

Configures the neighbor timeout interval after which a neighbor is considered to be absent.

Syntax

nbr-timeout *num*

no nbr-timeout

Command Default

The default is 105 seconds.

Parameters

num

Interval value in seconds. Valid values range from 35 through 12600 seconds.

Modes

Router PIM configuration mode

Usage Guidelines

Neighbor timeout is the interval after which a PIM device will consider a neighbor to be absent. Absence of PIM hello messages from a neighboring device indicates that a neighbor is not present. The interval can be set between 3 and 65535 seconds, and it should not be less than 3.5 times the hello timer value.

Enter **no nbr-timeout** to disable this feature.

Examples

Setting the timeout to 600 seconds.

```
device(config)# router pim
device(config-pim-router)# nbr-timeout 600
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor activate

Enables the exchange of information with BGP neighbors and peer groups.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

Command Default

Enabling address exchange for the IPv4 address family is enabled. Enabling address exchange for the IPv6 address family is disabled.

Parameters

ip-address
Specifies the IPv4 address of the neighbor.

ipv6-address
Specifies the IPv6 address of the neighbor.

peer-group-name
Specifies a peer group.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family EVPN configuration mode

Usage Guidelines

The **no** form of the command disables the exchange of an address with a BGP neighbor or peer group.

Examples

The following example establishes a BGP session with a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 activate
```

The following example establishes a BGP session with a neighbor with the IP address 10.1.1.1 in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 activate
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor additional-paths

Enables an additional-paths capability for a specific peer or peer group in a Border Gateway Protocol (BGP) address family.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths** { **receive** [**send**] | **send** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths receive**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths send**

Command Default

Specific peer devices or peer groups configured under a BGP address family are not capable of receiving or sending additional-paths.

Parameters

ip-address
Address of the neighbor in IPv4 address format.

ipv6-address
Address of the neighbor in IPv6 address format.

peer-group-name
Peer group name of the neighbor.

additional-paths
Enables an additional-paths capability.

receive
Enables the capability to receive additional-paths.

send
Enables the capability to send additional-paths.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

NOTE
An additional-paths capability configured at peer level takes precedence over any additional-paths capability configured at either the peer group or BGP address family level.

Peers exchange and negotiate additional-paths capability during session establishment.

An additional-paths capability can be enabled for a specific peer or peer group as receive only, send only, or both send and receive.

The **no** form of the command disables the additional-paths capability for a specific peer device or peer group.

To remove the configuration when both the **receive** and **send** options have been set, you should enter both the **no neighbor additional-paths** command, specifying the **receive** option to disable the capability to receive additional-paths, and the **no neighbor additional-paths** command, specifying the **send** option to disable the capability to send additional-paths.

Examples

The following example shows how to enable a peer device (10.1.2.3) configured under the IPv4 unicast address family to both receive and send additional-paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.1.2.3 additional-paths receive send
```

The following example shows how to disable the capability to receive additional-paths for a specific peer device (10.1.2.3) in the IPv4 unicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# no neighbor 10.1.2.3 additional-paths receive
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor additional-paths advertise

Configures the additional-paths to advertise to a neighbor for a Border Gateway Protocol (BGP) address family.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise** { **all** [**best** *num*] [**group-best**] | **best** *num* | **group-best** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise all**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise best** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise group-best**

Parameters

ip-address
: Address of the neighbor in IPv4 address format.

ipv6-address
: Address of the neighbor in IPv6 address format.

peer-group-name
: Peer group name of the neighbor.

all
: Causes all routes to be advertised as additional-paths to the specified neighbor or peer group. A maximum of 16 routes is allowed.

best *num*
: Specifies the number of best paths allowed for advertisement as additional-paths to the specified neighbor or peer group. The number ranges from 2 through 16.

group-best
: Causes group-best paths to be advertised as additional-paths to the specified neighbor or peer group. Only routes with a rank less than or equal to 16 are allowed. A route with a rank greater than 16 (even when it is the group best path), is not eligible for selection as an additional path advertised to a neighbor or peer group.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

NOTE

The set of paths configured by using the **neighbor additional-paths advertise** command must be a subset of selected paths; that is, paths previously configured by using the **additional-paths select** command under the particular BGP address-family configuration mode.

The **additional-paths advertise** command options (**all**, **best**, and **group-best**) are not mutually exclusive. When you configure a combination of these options, the combined configuration is applied to the BGP address family.

The **no** form of the command removes the specified configuration. When more than one option is configured, it is recommended that you disable each configured option separately; for example, by using the **no neighbor additional-paths advertise** command specifying the **all** option to disable the **all** configuration, and so on.

Examples

The following example shows how to configure the advertisement of all (a maximum of 16 is allowed) routes for a peer device, 10.123.123.1, under the IPv4 unicast address family.

```
device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-router-ipv4u)# neighbor 10.123.123.1 additional-paths advertise all
```

The following example shows how to restore the default configuration when all options (**all**, **best**, and **group-best**) were previously configured under the IPv4 unicast address family.

```
device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-router-ipv4u)# no neighbor 10.123.123.1 additional-paths advertise all
device(config-bgp-router-ipv4u)# no neighbor 10.123.123.1 additional-paths advertise best 2
device(config-bgp-router-ipv4u)# no neighbor 10.123.123.1 additional-paths advertise group-best
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor additional-paths disable

Disables the inheritance of an additional-paths capability (from the address family or peer group level) for a specific peer or peer group in a Border Gateway Protocol (BGP) address family.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths disable**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths disable**

Command Default

By default, an additional-paths capability configured for a specific BGP address family applies to all peer groups and peers configured under the address family, and an additional-paths capability configured for a peer group applies to all peers within the group.

Parameters

ip-address
: Address of the neighbor in IPv4 address format.

ipv6-address
: Address of the neighbor in IPv6 address format.

peer-group-name
: Peer group name of the neighbor.

Modes

BGP configuration mode

Usage Guidelines

When the capability to send and receive additional-paths is configured at the address family or peer group level, the capability applies to all neighbors configured under the address family or within the peer group: you can use the **neighbor additional-paths disable** command to disable this capability inheritance for an individual peer or peer-group.

The **no** form of the command restores the default configuration.

Examples

The following example shows how to disable additional-paths capability inheritance (from the address-family configuration) for an IPv4 address-family peer (10.123.123.1).

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# neighbor 10.123.123.1 additional-paths disable
```

The following example shows how to restore additional-paths capability inheritance (from the address-family configuration) for an IPv4 peer (10.123.123.1).

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# no neighbor 10.123.123.1 additional-paths disable
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor advertisement-interval

Enables changes to the interval over which a specified neighbor or peer group holds route updates before forwarding them.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **advertisement-interval** *seconds*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **advertisement-interval**

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

seconds
Range is from 0 through 3600. The default is 0.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default interval.

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor allowas-in

Disables the AS_PATH check function for routes learned from a specified neighbor so that BGP does not reject routes that contain the recipient BGP speaker's AS number.

Syntax

neighbor {*ip-address* | *ipv6-address* | *peer-group-name* } **allowas-in** *number*

no neighbor allowas-in {*ip-address* | *ipv6-address* | *peer-group-name* } **allowas-in**

Command Default

The AS_PATH check function is enabled and any route whose path contains the speaker's AS number is rejected as a loop.

Parameters

ip-address
: Specifies the IP address of the neighbor.

ipv6-address
: Specifies the IPv6 address of the neighbor.

peer-group-name
: Specifies a peer group.

number
: Specifies the number of times that the AS path of a received route may contain the recipient BGP speaker's AS number and still be accepted. Valid values are 1 through 10.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

If the AS_PATH check function is disabled after a BGP session has been established, the neighbor session must be cleared for this change to take effect.

The **no** form of the command re-enables the AS_PATH check function.

Examples

The following example specifies that the AS path of a received route may contain the recipient BGP4+ speaker's AS number three times and still be accepted.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example specifies for VRF instance "red" that the BGP4+ AS path of a received route may contain the recipient BGP speaker's AS number three times and still be accepted.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::124 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example specifies that the AS path of a received route may contain the recipient BGP speaker's AS number three times and still be accepted in EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor as-override

Replaces the autonomous system number (ASN) of the originating device with the ASN of the sending BGP device.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **as-override**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **as-override**

Command Default

This feature is disabled.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to disable this feature.

BGP loop prevention verifies the ASN in the AS path. If the receiving router sees its own ASN in the AS path of the received BGP packet, the packet is dropped. The receiving router assumes that the packet originated from its own AS and has reached the place of origination. This can be a significant problem if the same ASN is used among various sites, preventing sites with identical ASNs from being linked by another ASN. In this case, routing updates are dropped when another site receives them.

Examples

This example replaces the ASN globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 as-override
```

This example replaces the BGP4+ ASN for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 as-override
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor bfd

Enables Bidirectional Forwarding Detection (BFD) sessions for specified Border Gateway Protocol (BGP) neighbors or peer groups.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **bfd** [**holdover-interval** *time* | **interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **bfd** [**holdover-interval** *time* | **interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

Command Default

BFD sessions are not enabled on specific BGP neighbors or peer groups.

Parameters

ip-address
Specifies the IP address of the neighbor.

ipv6-address
Specifies the IPv6 address of the neighbor.

peer-group-name
Specifies a peer group.

holdover-interval *time*
Specifies the holdover interval, in seconds, for which BFD session down notifications are delayed before notification that a BFD session is down. Valid values range from 1 through 30.

interval *transmit-time*
Specifies the interval, in milliseconds, a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000.

min-rx *receive-time*
Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000.

multiplier *number*
Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD determines that the connection to that peer is not operational. Valid values range from 3 through 50.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Before using the **holdover-interval**, **interval**, **min-rx**, and **multiplier** parameters, you must first enable BFD using the **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name* } **bfd** command.

For single-hop BFD sessions, BFD considers the interval values that are configured on the interface, but not the nondefault values that are configured with this global command.

The **no** form of the command removes the BFD for BGP configuration for BGP neighbors or peer groups.

Examples

The following example configures BFD for a specified peer group and sets the BFD holdover interval to 18.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor pg1 bfd
device(config-bgp-router)# neighbor pg1 bfd holdover-interval 18
```

The following example configures BFD for a BGP neighbor with the IP address 10.10.1.1 and sets the BFD session timer values.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.10.1.1 bfd
device(config-bgp-router)# neighbor 10.10.1.1 bfd interval 120 min-rx 150 multiplier 8
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor capability as4

Enables or disables support for 4-byte autonomous system numbers (ASNs) at the neighbor or peer-group level.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **capability as4** [**disable** | **enable**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **capability as4** [**disable** | **enable**]

Command Default

4-byte ASNs are disabled by default.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor .

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

disable
Disables 4-byte numbering.

enable
Enables 4-byte numbering.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **disable** keyword or the **no** form of this command to remove all neighbor capability for 4-byte ASNs.

4-byte ASNs are first considered at the neighbor, then at the peer group, and finally at the global level.

Examples

This example enables 4-byte ASNs for a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 capability as4 enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor capability orf prefixlist

Advertises outbound route filter (ORF) capabilities to peer routers.

Syntax

neighbor { *ip_address* | *ipv6_address* | *peer-group-name* } **capability orf prefixlist** [**receive** | **send**]

no neighbor { *ip_address* | *ipv6_address* | *peer-group-name* } **capability orf prefixlist** [**receive** | **send**]

Command Default

ORF capabilities are not advertised to a peer device.

Parameters

ip_address
Specifies the IPv4 address of the neighbor.

ipv6_address
Specifies the IPv6 address of the neighbor.

peer-group-name
Specifies a peer group.

receive
Enables the ORF prefix list capability in receive mode.

send
Enables the ORF prefix list capability in send mode.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to disable ORF capabilities.

Examples

This example advertises the ORF send capability to a neighbor with the IP address 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 capability orf prefixlist send
```

This example advertises the ORF receive capability to a neighbor with the IPv6 address 2001:2018:8192::125 for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 capability orf prefixlist receive
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor default-originate

Configures the device to send the default route 0.0.0.0 to a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate**

Command Default

Disabled.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

Examples

The following example sends the default route to the BGP4 neighbor 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 default-originate
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor description

Specifies a name for a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **description** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **description**

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

description *string*
Specifies the name of the neighbor, an alphanumeric string up to 220 characters long.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command removes the name.

Examples

The following example specifies a BGP4 neighbor name.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 description mygoodneighbor
```

The following example specifies a BGP4+ neighbor name for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 default-originate route-map myroutemap
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor ebgp-btsh

Enables BGP time to live (TTL) security hack protection (BTSH) for eBGP.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-btsh**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-btsh**

Command Default

Disabled.

Parameters

ip-address
Specifies the IPv4 address of the neighbor.

ipv6-address
Specifies the IPv6 address of the neighbor.

peer-group-name
Specifies a peer group.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

To maximize the effectiveness of this feature, the **neighbor ebgp-btsh** command should be executed on each participating device. The **neighbor ebgp-btsh** command is supported for both directly connected peering sessions and multihop eBGP peering sessions. For directly connected neighbors, when the **neighbor ebgp-btsh** command is used, the device expects BGP control packets received from the neighbor to have a TTL value of either 254 or 255. For multihop peers, when the **neighbor ebgp-btsh** command is used, the device expects the TTL for BGP control packets received from the neighbor to be greater than or equal to 255 minus the configured number of hops to the neighbor.

The **no** form of the command disables BTSH for eBGP.

Examples

The following example enables GTSM between a device and a neighbor with the IP address 10.10.10.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.1.1.1 ebgp-btsh
```

The following example enables GTSM between a device and a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 ebgp-btsh
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor ebgp-multihop

Allows eBGP neighbors that are not on directly connected networks and sets an optional maximum hop count.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-multihop** [*max-hop-count*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-multihop**

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

max-hop-count
Maximum hop count. Range is from 1 through 255.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Examples

The following example enables BGP4+ eBGP multihop for VRF instance "red" and sets the maximum hop count to 40.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 ebgp-multihop 40
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor encapsulation

Sets the encapsulation type for an IPv4 neighbor, IPv6 neighbor, or a peer group.

Syntax

neighbor { *IPv4-address* | *IPv6-address* | *peer-group-name* } { **mct** | **vxlan** }

no neighbor { *IPv4-address* | *IPv6-address* | *peer-group-name* } { **mct** | **vxlan** }

Command Default

None

Parameters

IPV4-address
: Specifies an IPv4 address.

IPV6-address
: Specifies an IPv6 address.

peer-group-name
: Specifies a peer group.

mct
: Specifies MCT encapsulation.

vxlan
: Specifies VXLAN encapsulation.

Modes

BGP address-family EVPN configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following example specifies the VXLAN encapsulation for an IPv4 neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 encapsulation vxlan
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor enforce-first-as

Ensures that a device requires the first ASN listed in the AS_SEQUENCE field of an AS path-update message from EBGP neighbors to be the ASN of the neighbor that sent the update.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enforce-first-as** [**disable** | **enable**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enforce-first-as** [**disable** | **enable**]

Command Default

Disabled by default.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

disable
Disables this feature.

enable
Enables this feature.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to disable this requirement globally for the device.

Examples

This example enables the enforce-first-as feature for a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 enforce-first-as enable
```

This example enables the enforce-first-as feature for a BGP4+ specified neighbor for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 enforce-first-as enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor filter-list

Specifies a filter list to be applied to updates from or to the specified neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **filter-list** *ip-prefix-list-name* { **in** | **out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **filter-list** *ip-prefix-list-name* { **in** | **out** }

Command Default

No filter list is applied.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

ip-prefix-list-name
Name of the filter list. The name must be between 1 and 63 ASCII characters in length.

in
Specifies that the list is applied on updates received from the neighbor.

out
Specifies that the list is applied on updates sent to the neighbor.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

This example specifies that filter list “myfilterlist” be applied to updates to a neighbor with the IP address 10.11.12.13 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 filter-list myfilterlist out
```

This example specifies that filter list “2” be applied to updates from a neighbor with the IPv6 address 2001:2018:8192::125 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 filter-list 2 in
```

This example specifies that filter list “2” be applied to updates from a neighbor with the IPv6 address 2001:2018:8192::125 for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 filter-list 2 in
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor local-as

Causes the device to prepend the local autonomous system number (ASN) automatically to routes received from an eBGP peer.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **local-as** *num* [**no-prepend**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **local-as** *num* [**no-prepend**]

Command Default

This feature is disabled.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

num
Local ASN. Range is from 1 through 4294967295.

no-prepend
Causes the device to stop prepending the selected ASN.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove the local ASN.

Examples

This example ensures that a device prepends the local ASN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100
```

This example stops the device from prepending the selected ASN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100 no-prepend
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor maxas-limit in

Causes the device to discard routes received in UPDATE messages if those routes exceed a maximum AS path length.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maxas-limit in** { *num* | **disable** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maxas-limit in**

Command Default

This command is disabled by default.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

num
Maximum length of the AS path. Range is from 0 through 300. The default is 300.

disable
Prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead uses the default system value.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove this configuration.

Examples

This example changes the length of the maximum allowed AS path length from the default.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 maxas-limit in 200
```

This example prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead use the default system value.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 maxas-limit in disable
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor maximum-prefix

Specifies the maximum number of IP network prefixes (routes) that can be learned from a specified neighbor or peer group.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**]

Command Default

This feature is disabled.

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

num
: Maximum number of IP prefixes that can be learned. Range is from 0 through 2147483647. Default is 0 (unlimited).

threshold
: Specifies the percentage of the value specified by *num* that causes a syslog message to be generated. Range is from 1 through 100.

teardown
: Tears down the neighbor session if the maximum number of IP prefixes is exceeded.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family EVPN configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

Examples

The following example sets the maximum number of prefixes that will be accepted from the neighbor with the IP address 10.11.12.13 to 100000, and sets the threshold value to 80%.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 maximum-prefix 100000 threshold 80
```

The following example, for VRF instance "red," sets the maximum number of prefixes that will be accepted from the neighbor with the IPv6 address 2001:2018:8192::125 to 100000, and sets the threshold value to 90%.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 maximum-prefix 100000 threshold 90
```

The following example sets the maximum number of prefixes that will be accepted from the neighbor with the IP address 10.1.2.3 to 100000 in EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# neighbor 10.1.2.3 maximum-prefix 100000
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor next-hop-self

Causes the device to list itself as the next hop in updates that are sent to the specified neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-self** [**always**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-self** [**always**]

Parameters

ip-address
Specifies the IPv4 address of the neighbor.

ipv6-address
Specifies the IPv6 address of the neighbor.

peer-group-name
Specifies the peer group name configured by the **neighbor** *peer-group-name* command.

always
Enables this feature for route reflector (RR) routes.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command disables this feature.

Examples

The following example causes all updates destined for the neighbor with the IP address 10.11.12.13 to advertise this device as the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 next-hop-self
```

The following example, for the VRF instance "red," causes all updates destined for the neighbor with the IPv6 address 2001:2018:8192::125 to advertise this device as the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 next-hop-self
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor next-hop-unchanged

Enables BGP to send updates to eBGP peers with the next-hop attribute unchanged.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-unchanged**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-unchanged**

Command Default

This functionality is not enabled.

Parameters

ip-address
Specifies an IPv4 address.

ipv6-address
Specifies an IPv6 address.

peer-group-name
Specifies a peer group.

Modes

BGP address-family EVPN configuration mode

Usage Guidelines

By default, BGP speakers change the next hop while sending the updates to eBGP neighbors. Use this command to override this behavior. When this command is used, the next hop attribute remains unchanged while updates are sent to eBGP peers, and the BGP speaker is forced to retain the next hop address in the BGP updates received from neighbors.

The **no** form of the command disables the sending of updates to eBGP peers with the next-hop attribute unchanged.

Examples

The following example disables the sending of updates to eBGP peers with the next-hop attribute unchanged.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# no neighbor 10.11.12.13 next-hop-unchanged
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor password

Specifies an MD5 password for securing sessions between the device and a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **password** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **password**

Command Default

No password is set.

Parameters

ip-address
Specifies the IPv4 address of the neighbor.

ipv6-address
Specifies the IPv6 address of the neighbor.

peer-group-name
Specifies the peer group name configured by the **neighbor** *peer-group-name* command.

string
Password of up to 63 characters in length that can contain any alphanumeric character.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command removes a configured MD5 password.

Examples

The following example specifies a password for securing sessions with a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 password s0M3P@55W0Rd
```

The following BGP4+ example, for VRF instance "red," specifies a password for securing sessions with a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 2001:2018:8192::125 password s0M3P@55W0Rd
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor peer-group

Configures a BGP neighbor to be a member of a peer group.

Syntax

neighbor { *ip-address* | *ipv6-address* } **peer-group** *string*

no neighbor { *ip-address* | *ipv6-address* } **peer-group** *string*

Parameters

ip-address
Specifies the IPv4 address of the neighbor.

ipv6-address
Specifies the IPv6 address of the neighbor.

peer-group *string*
Specifies the name of a BGP peer group. The name can be up to 63 characters in length and can be composed of any alphanumeric character.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command removes a neighbor from the peer group.

Examples

The following example assigns a specified neighbor to a peer group called “mypeergroup1”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 peer-group mypeergroup1
```

The following BGP4+ example, for VRF instance "red," assigns a specified neighbor to a peer group called "mypeergroup1".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u)# neighbor 2001:2018:8192::125 peer-group mypeergroup1
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor prefix-list

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to IP address and mask length.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **prefix-list** *string* { **in** | **out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **prefix-list** *string* { **in** | **out** }

Command Default

This feature is disabled.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

string
Name of the prefix list. Range is from 1 through 63 ASCII characters.

in
Applies the filter in incoming routes.

out
Applies the filter in outgoing routes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

This example applies the prefix list "myprefixlist" to incoming advertisements to neighbor 10.11.12.13 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 prefix-list myprefixlist in
```

This example applies the prefix list "myprefixlist" to outgoing advertisements to neighbor 2001:2018:8192::125 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 prefix-list myprefixlist out
```

This example applies the prefix list "myprefixlist" to outgoing advertisements to neighbor 2001:2018:8192::125 for VRF instance "red," .

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 prefix-list myprefixlist out
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor remote-as

Specifies the autonomous system (AS) in which a remote neighbor resides.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remote-as** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remote-as**

Command Default

No AS is specified.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

num
Remote AS number (ASN). Range is from 1 through 4294967295.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command removes the neighbor from the AS.

Examples

The following example specifies AS 100 for a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 remote-as 100
```

The following BGP4+ example, for VRF instance "red," specifies AS 100 for a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 remote-as 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor remove-private-as

Configures a device to remove private autonomous system numbers (ASNs) from UPDATE messages that the device sends to a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remove-private-as**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remove-private-as**

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The device will remove ASNs 64512 through 65535 (the well-known BGP4 private ASNs) from the AS-path attribute in UPDATE messages that the device sends to a neighbor.

The **no** form of the command restores the default so that private ASNs are not removed from UPDATE messages sent to a neighbor by a device.

Examples

The following example removes private ASNs globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 remove-private-as
```

The following example removes private ASNs for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 remove-private-as
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor route-map

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to a set of attributes defined in a route map.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-map** { **in** *string* | **out** *string* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-map** { **in** *string* | **out** *string* }

Command Default

This feature is disabled.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

in
Applies the filter on incoming routes.

string
Name of the route map. Range is from 1 through 63 ASCII characters.

out
Applies the filter on outgoing routes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family EVPN configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

Examples

The following example applies a route map named "myroutemap" to an outgoing route from 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 route-map out myroutemap
```

The following example applies a route map named "myroutemap" to an incoming route from 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 route-map in myroutemap
```

The following example applies a route map named "myroutemap" to an outgoing route from 10.11.12.13 in EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# neighbor 10.11.12.13 route-map out myroutemap
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor route-reflector-client

Configures a neighbor as a route-reflector client.

Syntax

neighbor { *ip-address* | *peer-group-name* } **route-reflector-client**

no neighbor { *ip-address* | *peer-group-name* } **route-reflector-client**

Parameters

ip-address
Specifies the IPv4 address of the neighbor

peer-group-name
Specifies the peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use this command on a host device to configure a neighbor to be a route-reflector client. Once configured, the host device from which the configuration is made acts as a route-reflector server.

Examples

The following example configures a neighbor as a route-reflector client.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family vpnv4 unicast
device(config-bgp-vpnv4u)# neighbor 10.11.12.13 route-reflector-client
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor send-community

Enables sending the community attribute in updates to the specified BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]

Command Default

The device does not send community attributes.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

both
Sends both standard and extended attributes.

extended
Sends extended attributes.

standard
Sends standard attributes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family EVPN configuration mode

Usage Guidelines

If the **send-community** attribute is enabled after a BGP session has been established, the neighbor session must be cleared for this change to take effect.

The **no** form of the command restores the defaults.

Examples

The following example sends standard community attributes to a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 send-community standard
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sends extended community attributes to a neighbor for VRF instance "red".

```
device# configure terminal
ddevice(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 send-community extended
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sends standard and extended community attributes to a neighbor in EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 send-community both
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor shutdown

Causes a device to shut down the session administratively with its BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **shutdown** [**generate-rib-out**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **shutdown** [**generate-rib-out**]

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

generate-rib-out
When a peer is put into the shutdown state, Routing Information Base (RIB) outbound routes are not produced for that peer. Use this option to produce those routes.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Shutting down a session lets you configure the neighbor and save the configuration without the need to establish a session with that neighbor.

Examples

The following example causes a device to shut down the session administratively with its neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 shutdown
```

The following example causes a device to shut down the session administratively with its neighbor and generate RIB outbound routes for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 shutdown generate-rib-out
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor soft-reconfiguration inbound

Stores all the route updates received from a BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

Parameters

ip-address
Specifies the IPv4 address of the neighbor

ipv6-address
Specifies the IPv6 address of the neighbor

peer-group-name
Specifies the peer group name.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Soft reconfiguration stores all the route updates received from a neighbor. If you request a soft reset of inbound routes, the software compares the policies against the stored route updates, instead of requesting the neighbor's BGP4 or BGP4+ route table or resetting the session with the neighbor.

Examples

The following example globally stores route updates from a BGP4 neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 soft-configuration inbound
```

The following example stores route updates from a BGP4+ neighbor for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 soft-configuration inbound
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor static-network-edge

Overrides the default BGP4 behavior and advertises the network to a neighbor or peer group only when the corresponding route is installed as a forward route in the routing table.

Syntax

neighbor { *ip-address* | *peer-group-name* } **static-network-edge**

no neighbor { *ip-address* | *peer-group-name* } **static-network-edge**

Parameters

ip-address
Specifies the IPv4 address of the neighbor

peer-group-name
Specifies the peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

A BGP static network is always advertised to neighbors or a peer group, and if the corresponding route is not present in the routing table, BGP installs the null0 route. This command overrides the default behavior. This command is not supported for BGP4+.

Examples

The following example globally overrides the default BGP4 behavior.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 static-network-edge
```

The following example overrides the default BGP4 behavior for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 10.11.12.13 static-network-edge
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor timers

Specifies how frequently a device sends KEEPALIVE messages to its BGP neighbors, as well as how long the device waits for KEEPALIVE or UPDATE messages before concluding that a neighbor is dead.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **timers keep-alive** *keepalive_interval* **hold-time** *holdtime_interval*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **timers keep-alive** *keepalive_interval* **hold-time** *holdtime_interval*

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

keep-alive *keepalive_interval*
Frequency (in seconds) with which a device sends keepalive messages to a peer. Range is from 0 through 65535 seconds. The default is 60.

hold-time *holdtime_interval*
Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Range is from 0 through 65535 seconds. The default is 180.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

Examples

The following example sets the keepalive timer for a device to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

The following example sets the keepalive timer to 120 seconds and the hold-timer to 360 seconds for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor unsuppress-map

Removes route suppression from BGP neighbor routes when those routes have been suppressed as a result of aggregation. All routes matching route-map rules are unsuppressed.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **unsuppress-map** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **unsuppress-map** *string*

Command Default

This feature is disabled.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

string
Name of the route map. Range is from 1 through 63 ASCII characters.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

The following BGP4 example removes route suppression for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 unsuppress-map myroutemap
```

The following BGP4+ example removes route suppression for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 unsuppress-map myroutemap
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor update-source

Configures the BGP device to communicate with a neighbor through a specified interface.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address* | **ethernet** *slot* **/** *port* | **loopback** *num*| **ve-interface** *vlan_id* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address* | **ethernet** *slot* **/** *port* | **loopback** *num*| **ve-interface** *vlan_id* }

Command Default

Disabled.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

ip-address
IP address of the update source.

ethernet
Specifies an ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

loopback *num*
Specifies a loopback interface.

ve-interface *vlan_id*
Specifies a virtual Ethernet VLAN interface.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

The following example configures the device to communicate with a neighbor through the specified IPv4 address and Ethernet interface 3/2.

```
device#configure terminal
device#(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 update-source ethernet 3/2
```

History

Release version	Command history
18x.1.00	This command was introduced.

neighbor weight

Specifies a weight that the device will add to routes that are received from the specified BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight**

Command Default

The default for *num* is 0.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor

peer-group-name
Name of the peer group.

num
Value from 1 through 65535.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

BGP prefers larger weights over smaller weights.

Examples

This example changes the weight from the default.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 weight 100
```

This example changes the weight from the default for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 weight 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

network

Configures the device to advertise a BGP network.

Syntax

network *network/mask* [**backdoor** | **route-map** *map-name* | **weight** *num*]

no network *network/mask* [**backdoor** | **route-map** *map-name* | **weight** *num*]

Command Default

No network is advertised.

Parameters

network/mask
Network and mask in CIDR notation.

backdoor
Changes administrative distance of the route to this network from the eBGP administrative distance (the default is 20) to the local BGP weight (the default is 200), tagging the route as a backdoor route.

route-map *map-name*
Specifies a route map with which to set or change BGP attributes for the network to be advertised. Range is from 1 through 63 ASCII characters.

weight*num*
Specifies a weight to be added to routes to this network. Range is 0 through 65535. The default is 0.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

This example imports the IP prefix 10.1.1.1/32 into the BGP4 database and specifies a route map called “myroutemap”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# network 10.1.1.1/32 route-map myroutemap
```

This example imports the IPv6 prefix 2001:db8::/32 into the BGP4+ database and sets a weight of 300.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# network 2001:db8::/32 weight 300
```

History

Release version	Command history
18x.1.00	This command was introduced.

next-hop-enable-default

Configures the device to use the BGP default route as the next hop.

Syntax

next-hop-enable-default

no next-hop-enable-default

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following BGP4 example configures the device to use the default route as the next hop for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-enable-default
```

The following BGP4+ example configures the device to use the default route as the next hop for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# next-hop-enable-default
```

History

Release version	Command history
18x.1.00	This command was introduced.

next-hop-recursion

Enables BGP recursive next-hop lookups.

Syntax

next-hop-recursion

no next-hop-recursion

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

If the BGP next hop is not the immediate next hop, a recursive route lookup in the IP routing information base (RIB) is needed. With recursion, a second routing lookup is required to resolve the exit path for destination traffic. Use this command to enable recursive next-hop lookups.

Examples

This example enables recursive next-hop lookups for BGP4.

```
device# configure terminal
device(config)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-recursion
```

This example enables recursive next-hop lookups for BGP4+.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# next-hop-recursion
```

History

Release version	Command history
18x.1.00	This command was introduced.

nonstop-routing (OSPF)

Enables nonstop routing (NSR) for OSPF.

Syntax

nonstop-routing

no nonstop-routing

Command Default

Enabled.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command disables non-stop routing.

Examples

The following example re-enables NSR on a device.

```
device# configuration terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# nonstop-routing
```

History

Release version	Command history
18x.1.00	This command was introduced.

ntp authenticate

This command enables or disables the NTP authentication at global level. If the authentication is enabled, the NTP packets from servers, peers, clients not having MAC is dropped. Only those servers/peers configured with key authentication is considered for time synchronization. Client requests only with authentication is served, whose key-IDs match with one of the trusted key-IDs.

Syntax

ntp authenticate

no ntp authenticate

Command Default

By default the authentication is disabled.

Modes

Global configuration mode

Usage Guidelines

The no form of **ntp authenticate** disables the NTP authentication.

Examples

```
device(config)# ntp authenticate
```

History

Release version	Command history
18x.1.00	This command was introduced.

ntp authentication-key

Creates an authentication key to associate with the NTP server, thereby enabling NTP authentication.

Syntax

ntp authentication-key *key-id* {**md5**| **sha1 sha256**}*key-string*

no ntp authentication-key *key-id*

Command Default

By default the authentication keys are not configured.

Parameters

key-id
Specifies an ID for an authentication key. The range is from 1 through 65534.

md5
The MD5 encryption.

key-string
Specifies a key string. The string can be a maximum of 15 ASCII characters.

Modes

Global configuration mode

Usage Guidelines

This command adds an NTP authentication key to a list of authentication keys in the database. The key is shared by the client (device) and an external NTP server.

The maximum number of configurable NTP authentication keys is five. You cannot configure a duplicate key ID with a different key string. Use the **no ntp authentication-key** *key-id* command to remove the specified authentication key.

Authentication key must be created before associating the key with any server. Refer to the **ntp server** command for information on how to create this association.

Before downgrading the firmware to a version that does not support the encryption-level option, the encryption-level should be set to 0.

Examples

To create an authentication key with an ID of 33, an MD5 string called *check*, and an encryption level of 0 :

```
device# configure
device(config)# ntp authentication-key 33 md5 check encryption-level 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

ntp disable

Disables the NTP server/client mode. Disabling the NTP server/client mode does not remove the configuration.

Syntax

ntp disable { **ntp disable**} [**serve**]

no ntp disable*serve*

Command Default

By default, the NTP is enabled.

Parameters

serve

If this keyword is specified, then NTP will not serve the time to downstream devices. This keyword disables the NTP server mode functionalities.If this keyword is not specified, then both NTP client mode and NTP server mode functionalities will be disabled.

Modes

Global configuration mode

Examples

Use **no** to disable NTP server and client mode.

```
Disable NTP server and client mode:
 device(config)# ntp disable
Disable NTP client mode:
 device(config)# ntp disable serve
```

History

Release version	Command history
18x.1.00	This command was introduced.

ntp master

Configures the device as an authoritative NTP Server. **ntp master** enables device to use its own clock to synchronize with peers/clients. This command is not effective, if the NTP is enabled in client-only mode.

Syntax

ntp master [**stratum***number*]

no ntp master*stratum number*

Command Default

The master clock is disabled by default. The stratum number is default set to 8, if not specified.

Parameters

stratum*number*
The NTP stratum number.

Modes

Global configuration mode

Usage Guidelines

The no form of the command removes the NTP master configuration. The stratum range is 2 to 15.

Examples

ntp master command configures the device as an authoritative device.

```
device(config)# ntp master stratum 5

The following error message is displayed when stratum number is out of range.
"Stratum number must be in the range 2..15"
```

History

Release version	Command history
18x.1.00	This command was introduced.

ntp peer

Configures the NTP peers and specify the peers to synchronize the system clock. Maximum 8 NTP peers can be configured.

Syntax

ntp peer { **ipv4** | **ipv6** } [*vrf name*]

no ntp peeripv4 | ipv6*vrf name*

Command Default

No default peer are configured. This command is not effective, if the NTP is enabled in client-only mode. If the peer is already mobilized as symmetric passive, then configuring statically will not be effective.

Parameters

ipv4 address | ipv6 address
IPv4 or IPv6 address of the NTP peer.

use-vrf name
Use VRF name to synchronize the time with server. If this option is not specified, it defaults to **mgmt-vrf**.

key
The symmetric key ID. By default, no symmetric key is configured. The range is 1 to 65,534.

version*3 | 4*
The NTP version supported by peer. If this option is not specified, then defaults to 4.

minpoll*interval*
The shortest polling interval. The range is 4 to 17. Default is 6. The interval argument is power of 2: 3=8s, 4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s etc.

maxpoll*interval*
The longest polling interval. The range is 4 to 17. Default is 10. The interval argument is power of 2: 3=8s, 4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s etc.

Modes

Global configuration mode

Usage Guidelines

The no form of **ntp peer** command removes the peer configuration and applied options.

Examples

Configures the NTP peers and specify the peers to synchronize the system clock.

```
device(config)# ntp peer 1.2.3.4
device(config-peer-1.2.3.4/mgmt-vrf)# key 1
device(config-peer-1.2.3.4/mgmt-vrf)# minpoll 7

The below error message is displayed when the minimum poll interval is greater than maximum poll
interval:
"Minimum poll interval cannot be greater than maximum poll interval”
```

NOTE

If maximum poll interval is not entered and minimum poll interval entered is greater than 10, then above error message is displayed as the default maximum poll interval is 10.

History

Release version	Command history
18x.1.00	This command was introduced.

ntp server

Specifies or adds an NTP server IP address and optionally associates an authentication key to the server.

Syntax

ntp server { **ipv4** | **ipv6** } [*vrf name*]

no ntp server { **ipv4** | **ipv6** } [*vrf name*]

Command Default

No default peer are configured.

Parameters

ipv4 | **ipv6**
IPv4 or IPv6 address of the NTP peer

use-vrf name
Use VRF name to synchronize the time with server. If this option is not specified, it defaults to **mgmt-vrf**.

minpoll*interval*
The shortest polling interval. The range is 4 to 17. Default is 6. The interval argument is power of 2: 3=8s, 4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s etc.

maxpoll*interval*
The longest polling interval. The range is 4 to 17. Default is 10. The interval argument is power of 2: 3=8s, 4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s etc.

Modes

Global configuration mode

Usage Guidelines

Use this command to add an NTP server IPv4 or IPv6 address to a list of server IP addresses, or to associate an existing authentication key with an NTP server IP address.

The maximum number of NTP servers allowed is five.

Network Time Protocol (NTP) commands must be configured on each individual switch.

Use the **no ntp server** *ip-address* command to remove the specified NTP server IP address. Removing the current active NTP server resets the NTPstatus to "LOCL" until a new, active server is selected.

Use the **no ntp server** *ip-address* **key** *key-id* command to remove the key from the specified NTP IP address.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

To associate a configured key ID of 15 to an NTP server on the management VRF:

```
device(config)# ntp peer 1.2.3.4
device(config-server-1.2.3.4/mgmt-vrf)# key 1
device(config-server-1.2.3.4/mgmt-vrf)# minpoll 7

The below error message is displayed when the minimum poll interval is greater than maximum poll
interval:
"Minimum poll interval cannot be greater than maximum poll interval”
```

NOTE

If maximum poll interval is not entered and minimum poll interval entered is greater than 10, then above error message is displayed as the default maximum poll interval is 10.

History

Release version	Command history
18x.1.00	This command was introduced.

ntp source-ip

Configures the source IP address to be used to access the NTP server.

Syntax

ntp source-ip *ip_address*

no ntp source-ip

Command Default

The NTP source IP is not configured.

Parameters

ip_address

Uses the IP address of the device for the NTP server.

Modes

Global configuration mode

Usage Guidelines

Use the **no ntp source-ip** command to remove the configuration.

Examples

Typical command example:

```
device# configure terminal
device(config)# ntp source-ip chassis-ip 10.28.52.26
```

History

Release version	Command history
18x.1.00	This command was introduced.

ntp trusted-keys

This command configures additional subset of trusted key-IDs which can be used for NTP and client authentication. The keys configured for server/peer is implicitly considered as part of trusted keys.

Syntax

ntp trusted-keys [*key-id-1 key-id-2key-id-n*]

no ntp trusted keys

Command Default

By default the trusted key-IDs are not configured.

Parameters

key-id-1key-id-2key-id-n
List of authentication keys.

Modes

Global configuration mode

Usage Guidelines

The no form of **ntp trusted-keys** clears a configured key-ID from the trusted key list.

Examples

This command configures an additional subset of trusted key-IDs.

```
device(config)# ntp trusted-keys 1 5 15
 device(config)# no ntp trusted-keys 15
```

History

Release version	Command history
18x.1.00	This command was introduced.

oscmd

Runs commands or scripts supported by the Linux OS directly from the SLX-OS CLI.

Syntax

oscmd { *Linux-command* | *script-name* }

Parameters

Linux-command
Specifies the Linux command that you want to run.

script-name
Specifies the script that you want to run.

Modes

Privileged EXEC mode

Usage Guidelines

This command is only available for users with admin-level permissions.

All scripts run under **oscmd** must have execute permission.

After writing and testing a user-defined script file, you can copy it to the SLX-OS device. Imported scripts are stored in the `/var/config/vcs/scripts` directory.

You can also create scripts from the Linux shell using the "vi" editor. The newly-created scripts must exist in the `/fabos/users/admin` directory.

Although as an SLX-OS admin you have permissions to run the following commands from the Linux shell, you do not have permissions to run them—from the SLX-OS CLI—appended to the **oscmd** command.

- **bash**
- **script**
- **vi**
- **vim**

Examples

In the following example, the Linux **ps -ef** command lists the process status from the CLI.

```
device#  oscmd ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Jul24 ?        00:00:04 /sbin/init
root         2     0  0 Jul24 ?        00:00:00 [kthreadd]
root         3     2  0 Jul24 ?        00:00:00 [migration/0]
root         4     2  0 Jul24 ?        00:00:03 [ksoftirqd/0]
root         5     2  0 Jul24 ?        00:00:00 [migration/1]
root         6     2  0 Jul24 ?        00:00:03 [ksoftirqd/1]
root         7     2  0 Jul24 ?        00:00:00 [migration/2]
root         8     2  0 Jul24 ?        00:00:02 [ksoftirqd/2]
root         9     2  0 Jul24 ?        00:00:00 [migration/3]
root        10     2  0 Jul24 ?        00:00:02 [ksoftirqd/3]
root        11     2  0 Jul24 ?        00:00:00 [migration/4]
root        12     2  0 Jul24 ?        00:00:02 [ksoftirqd/4]
root        13     2  0 Jul24 ?        00:00:00 [migration/5]
root        14     2  0 Jul24 ?        00:00:03 [ksoftirqd/5]
root        27     2  0 Jul24 ?        00:00:00 [cpuset]
root        28     2  0 Jul24 ?        00:00:01 [khelper]
root        31     2  0 Jul24 ?        00:00:00 [netns]
root        34     2  0 Jul24 ?        00:00:00 [async/mgr]
root       270     2  0 Jul24 ?        00:00:00 [sync_supers]
root       272     2  0 Jul24 ?        00:00:00 [bdi-default]

...

root      8kblockd/6]182     1  0 Jul24 ?        00:00:00 /usr/sbin/inetd
root      8237     1  0 Jul24 ?        00:00:00 /usr/sbin/sshd
admin    27536 27535  0 04:19 pts/4    00:00:00 ps -ef
```

In the following example, "my_script" is the name of a user-defined script that is downloaded by using the **copy** command or exists in the `/fabos/users/admin` directory; and is executable under the Linux OS .

```
device# oscmd my_script
```

History

Release version	Command history
18x.1.00	This command was introduced.

overlay-gateway

Creates a VXLAN overlay gateway instance and enables VXLAN overlay gateway configuration mode.

Syntax

overlay-gateway *name*

no overlay-gateway *name*

Parameters

name

Specifies a name for the VXLAN overlay gateway. Only one gateway instance can be configured. The name is an alphanumeric, 32-character-maximum string that can also contain hyphens and underscores.

Modes

Global configuration mode

Usage Guidelines

Use this command to create a VXLAN overlay gateway instance with the given name. An overlay network is a virtual network that is built on top of existing network Layer 2 and Layer 3 technologies. Setting up a gateway consists of the following:

- Configuring the source IP address
- Configuring the VLAN or bridge domain
- Mapping a bridge domain to a VNI
- Configuring MAC addresses to export to the VXLAN domain
- Enabling statistics collection for VLAN domains
- Enabling SPAN

One you create the gateway instance, you enter VXLAN overlay gateway configuration mode, where you can configure other properties for this gateway. The key commands available in this mode are summarized below:

TABLE 4 Key commands available in VXLAN overlay gateway configuration mode

Command	Description
activate	Activates a VXLAN overlay gateway instance.
ip interface loopback	Sets the loopback port number for the overlay gateway instance.
map bridge-domain	In a VXLAN overlay gateway configuration that uses the Layer 2 extension, maps a bridge domain with VXLAN Network Identifiers (VNIs).
map vlan	In a VXLAN overlay gateway configuration that uses Layer 2 extension, associates VLANs with VXLAN Network Identifiers (VNIs).
sflow	Enables sFlow monitoring of the tunnel endpoints for a VXLAN overlay gateway.
site	Configures a remote Layer 2 extension site in a VXLAN overlay gateway context.

TABLE 4 Key commands available in VXLAN overlay gateway configuration mode (continued)

Command	Description
type layer2-extension	Specifies that a VXLAN overlay gateway uses Layer 2 extension.

Only one VXLAN overlay gateway instance can be configured.

Use the **no overlay-gateway** command to delete the VXLAN overlay gateway instance from the cluster. All tunnels for the gateway are also deleted. There are no other **no** forms of this command.

By default, a VXLAN overlay gateway instance is inactive. To activate an instance, first configure its other properties (such as which devices it attaches to), and then enter the **activate** command.

Examples

The following example creates a VXLAN overlay gateway instance named gateway1 and accesses VXLAN overlay gateway configuration mode.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

password-attributes

Configures global password attributes.

Syntax

password-attributes { [**max-retry** *maxretry*] [**min-length** *minlen*] [**max-lockout-duration** *duration*] [**admin-lockout** | **character-restriction** { [**lower** *numlower*] [**numeric** *numdigits*] [**special-char** *numsplchars*] [**upper** *numupper*] } }

no password-attributes { [**max-retry** *maxretry*] [**min-length** *minlen*] [**max-lockout-duration** *duration*] [**admin-lockout** | **character-restriction** { [**lower** *numlower*] [**numeric** *numdigits*] [**special-char** *numsplchars*] [**upper** *numupper*] }] }

Command Default

The default for *min-length* is 8. All other defaults are 0.

Parameters

admin-lockout

Enables lockout for admin role accounts.

character-restriction

Configures the restriction on various types of characters.

lower *numlower*

Specifies the minimum number of lowercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

numeric *numdigits*

Specifies the minimum number of numeric characters that must occur in the password. Values range from 0 through 32 characters. The default is 0.

special-char *numsplchars*

Specifies the number of punctuation characters that must occur in the password. All printable, nonalphanumeric punctuation characters, except colon (:) are allowed. Values range from 0 through 32 characters. The default value is 0.

upper *numupper*

Specifies the minimum number of uppercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

max-retry *maxretry*

Specifies the number of failed password logins permitted before a user is locked out. Values range from 0 through 16 attempted logins. The default value is 0.

min-length *minlen*

Specifies the minimum length of the password. Valid values range from 8 through 32 characters. The default is 8 characters.

max-lockout-duration *duration*

Specifies the maximum number of minutes after which the user account is unlocked. Range is from 0 through 99999. The default is 0, representing an infinite duration.

Modes

Global configuration mode

Usage Guidelines

To reset password attributes to their default values, enter the **no** form of this command.

Examples

The following example configures global password attributes and verifies the configuration.

```
device#configure terminal
device(config)# password-attributes max-retry 4
device(config)# password-attributes character-restriction lower 2
device(config)# password-attributes character-restriction upper 1 numeric 1 special-char 1
device(config)# exit
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
```

The following example resets the character restriction attributes and verifies the configuration.

```
device#configure terminal
device(config)# no password-attributes character-restriction lower
device(config)# no password-attributes character-restriction upper
device(config)# exit
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
```

The following example clears all global password attributes.

```
device#configure terminal
device(config)# no password-attributes
device(config)# exit
device# show running-config password-attributes
% No entries found.
```

The following example sets the maximum number of retries to 3 and enables lockout policy for admin role accounts.

```
device#configure terminal
device(config)# password-attributes max-retry 3 admin-lockout
```

The following example specifies that the user account be unlocked after 5 minutes and enables lockout policy for admin role accounts.

```
device#configure terminal
device(config)# password-attributes max-lockout-duration 5 admin-lockout
```

History

Release version	Command history
18x.1.00	This command was introduced.

pdu-rate

Configures pdu-rate value, which is the number of OAMPDUs per second.

Syntax

pdu-rate *rate*

Command Default

The default value is 1.

Parameters

rate

Specifies the pdu rate per second.

Modes

Link OAM configuration mode

Usage Guidelines

The range is from 1 through 10. Configure the timeout interval at least three times the pdu interval to avoid Link OAM protocol flaps against loss of one or two PDUs for any latency issues in general and during HA fail over.

Examples

```
(config-link-oam)# pdu-rate 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

peer

Configures a peer IP address in a bridge domain. A corresponding pseudowire (PW) interface is created when the peer IP address is configured.

Syntax

peer *ip-address* [**control-word**] [**cos** *num*] [**flow-label**] [**load-balance**] [**lsp** *lsp-name1*, *lsp-name2*, . . . *lsp-name32*]

no peer [*ip-address* [**lsp** *lsp-name1*, *lsp-name2*, . . . *lsp-name32*]]

Command Default

No PW interfaces are configured.

Parameters

ip-address
A PW IP address for a remote peer.

control-word
Enables control word for routing of pseudowire (PW) traffic to the peer.

cos *num*
Specifies a Class of Service (CoS) value for selecting a label-switched path to reach the peer. The value ranges is from 0 through 7.

flow-label
Enables flow label to support PW load balancing.

load-balance
Specifies load balancing. As many as16 alternate paths are used for load balancing.

lsp *lsp-name1*, *lsp-name2*, . . . *lsp-name32*
Specifies the name of a label-switched path. As many as 32 label-switched path names can be configured.

Modes

Bridge-domain configuration mode.

Usage Guidelines

The virtual connection identifier (VC ID) must be configured by using the **vc-id** command prior to configuring the peer IP address to create a PW interface.

The **no** form of the command deletes the peer IP address configuration and the PW interface that corresponds to the specified peer IP address.

The following are examples of configuration combinations that are allowed:

- **peer** *ip-address* **control-word**
- **peer** *ip-address* **cos** *num*

- **peer** *ip-address* **flow-label**
- **peer** *ip-address* **load-balance**
- **peer** *ip-address* **control-word flow-label**
- **peer** *ip-address* **control-word cos** *num* **flow-label**
- **peer** *ip-address* **control-word cos** *num* **flow-label load-balance**
- **peer** *ip-address* **control-word cos** *num* **flow-label**
- **peer** *ip-address* **control-word flow-label load-balance**
- **peer** *ip-address* **cos** *num* **load-balance**
- **peer** *ip-address* **cos** *num* **flow-label**
- **peer** *ip-address* **load-balance cos**
- **peer** *ip-address* **load-balance lsp** *lsp-name1*, *lsp-name2*,...*lsp-name32*
- **no peer** *ip-address*
- **no peer** *ip-address* **lsp** *lsp-name1*, *lsp-name2*, . . . *lsp-name32*

NOTE
When a peer is already configured, you cannot add a CoS or load balancing configuration. To configure a CoS value or load-balancing, the peer must be removed by using the **no peer** command and reconfigured by specifying the required **cos** or **load-balance** options.
To remove the CoS or load-balance configuration, the peer configuration must be removed by using the **no peer** command.

Examples

The following example shows how to configure a peer IP address (10.12.12.12) for bridge domain 1 with the **load-balance** option.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.12.12.12 load-balance
```

The following example shows how to configure a peer IP address (10.12.12.12) for bridge domain 1 specifying two label-switched paths (lsp1 and lsp2).

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.12.12.12 lsp lsp1 lsp2
```

The following example shows how to configure a peer IP address (10.1.1.1) for bridge domain 1 specifying load balancing and four label-switched paths (lsp1, lsp2, lsp3 and lsp4).

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.1.1.1 load-balance lsp lsp1 lsp2 lsp3 lsp4
```

The following example shows the error message that is displayed when you try to configure the **load-balance** option for an existing peer. The peer configuration must be removed and reconfigured to specify the **load-balance** option, as shown in the example.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 15.15.15.15
device(config-bridge-domain-1)# peer 15.15.15.15 load-balance
Error: can not configure load-balance on existing peer.
device(config-bridge-domain-1)#no peer 15.15.15.15
device(config-bridge-domain-1)# peer 15.15.15.15 load-balance
```

History

Release version	Command history
18x.1.00	This command was introduced.

peer (MCT)

Configures the IP address for the MCT cluster peer.

Syntax

peer *ip-address*

no peer [*ip-address*]

Parameters

ip-address

Specifies the IP address for the cluster peer. The address is either the peer loopback address or nexthop IP address.

Modes

Cluster configuration mode.

Usage Guidelines

Configure a corresponding neighbor in BGP EVPN address family for the peer. If the peer is already configured as a neighbor, when you deploy and undeploy the cluster, the BGP neighbor resets to renegotiate its capability.

If the peer already exists for other address family, clear the IP BGP peer session.

The **no** form of the command deletes the peer IP address configuration.

Examples

The following example shows the configuring of the cluster peer IP address.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# peer 10.10.10.12
```

History

Release version	Command history
18x.1.00	This command was introduced.

peer-interface

Configures the Ethernet or VE interface to reach the MCT cluster peer.

Syntax

peer-interface Ethernet *slot/port* | **Ve** *number*

no peer-interface

Parameters

Ethernet *slot/port*
Specifies the Ethernet interface for the cluster peer.

Ve *number*
Specifies the VE interface for the cluster peer.

Modes

Cluster configuration mode.

Usage Guidelines

The **no** form of the command deletes the peer interface configuration.

You must configure the peer interface before deploying the cluster configuration.

You cannot change the peer interface when the cluster is deployed.

Examples

The following example shows the configuring of the cluster peer interface.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# peer-interface Ve 20
```

History

Release version	Command history
18x1.00	This command was introduced.

permit ip host

Creates a rule in an Address Resolution Protocol (ARP) ACL that permits ARP messages from a host specified by both IP and MAC addresses.

Syntax

permit ip host *sender-ip* **mac host** *sender-mac-address*

no permit ip host *sender-ip* **mac host** *sender-mac-address*

Command Default

No permit rules are defined.

Parameters

sender-ip
Specifies the sender IP address.

mac host *sender-mac-address*
Specifies the sender MAC address, in hexadecimal format.

Modes

ARP ACL configuration mode

Usage Guidelines

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

The **no** form of the command removes the permit rule from the ACL.

Examples

The following example defines a **permit ip host** rule in an ARP ACL, applies the ACL to a VLAN, and enables DAI on that VLAN.

```
device# configure terminal
device(config)# arp access-list arp_acl_1
device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222
device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223
device(config-arp-acl)# exit

device(config)# vlan 200
device(config-vlan-200)# ip arp inspection filter arp_acl_1
device(conf-vlan-200)# ip arp inspection
```

The following example creates a **permit ip host** rule within the **arp access-list** command.

```
device# configure terminal
device(config)# arp access-list host2 permit ip host 1.1.1.1 mac host 0000.0011.0022
```

History

Release version	Command history
18x.1.00	This command was introduced.

police cir

Configures the committed information rate, committed burst size, exceeded information rate, and the exceeded burst size for the class map.

Syntax

police cir *cir-bps* [**cbs** *bytes*] [**eir** *bps* [**ebs** *bytes*]]

no police cir [**cbs**] [**eir** [**ebs**]]

Parameters

cir-bps
Specifies the committed information rate in bits per second. Enter an integer from 0 to 300000000000.

cbs *bytes*
Specifies the committed burst size in bytes. Enter an integer from 1250 to 37500000000.

eir *bps*
Specifies the exceeded information rate in bits per second. Enter an integer from 0 to 300000000000.

ebs *bytes*
Specifies the exceeded burst size in bytes. Enter an integer from 1250 to 37500000000.

Modes

Policy-map class configuration mode

Usage Guidelines

Use the **no** version of this command to remove the parameter from the class map.

You can enter CIR and EIR values from 0 to 300000000000, but the operational values are from 22000 to 300000000000.

Only the **police cir** command is mandatory for configuring a class map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete all parameters for a class-map, use the **no police** command.

If CBS and EBS values are not configured, then these values are derived from the CIR and EIR values, respectively. The burst size calculation is as follows: Burst size (CBS or EBS) = 1.2*information rate (CIR/EIR)/8.

If the configured CBS value is less than 2*(default MTU) value, then 2*(default MTU) is programmed as the CBS in the hardware. For example, if you configure CBS at 2000 bytes and the default MTU on an interface is 1548 bytes, when a policy map is applied on this interface, the CBS programmed in the hardware is 2*MTU (3096 bytes). If you update the MTU value, the CBS value is not be updated.

If the optional EIR or EBS value is not configured, it is disabled and Always Violated traffic is dropped.

To disable the learning of MAC addresses for stream matching of the ACL-based rate limiting entries, the CIR and EIR values must be 0.

The MAC address entries in the MAC-address table which are already learned will not be flushed when you configure the CIR or EIR value as 0. You must explicitly clear the entries in MAC-address table by using the **clear mac-address-table dynamic** command.

Examples

The following example sets the committed information rate (cir), committed burst size (cbs), exceeded information rate (eir), and the exceeded burst size (ebs).

```
device# configure terminal
device(config)# policy-map policy_2
device(config-policymap)# class default
device(config-policymap-class)# police cir 3000000 cbs 375000000 eir 300000000 ebs 37500000
```

History

Release version	Command history
18x.1.00	This command was introduced.

policy-map

Configures a policy map containing a class map so that you can apply policer and QoS attributes to a particular interface.

Syntax

policy-map *policy-mapname*

no policy-map *policy-mapname*

Command Default

No policy map is created.

Parameters

policy-mapname
Name of police policy map

Modes

Global configuration mode

Usage Guidelines

When you launch the **policy-map** command, the system is placed in `config-policymap mode` for the configured map. At this point, you can add a class map containing policing parameters to the policy map. (Refer to the description of the **class** command.)

This command creates a policer policy map to apply policer and QoS attributes to a particular interface. Each policy map can contain up to 32 class maps. The class map can be associated with specific policing and QoS parameters.

Maximum number of policy map creations are 128

Associate the policy map to the interface for inbound or outbound direction with the **service-policy** command.

Enter **no policy-map** *policy-mapname* while in global configuration mode to remove the policy map.

Examples

Create a policy map and place system into config-policymap mode so that you can add a class map.

```
device# configure terminal
device(config)# policy-map policymap1
device(config-policymap)#
```

Remove the policy map while in global configuration mode.

```
device# configure terminal
device(config)# no policy-map policymap1
```

History

Release version	Command history
18x.1.00	This command was introduced.

port-channel path-cost

Sets the port channel path cost behavior.

Syntax

port-channel path-cost [**custom** | **standard**]

Command Default

Path cost is standard.

Parameters

custom

Specifies to use the custom behavior, which sets the path cost changes according to the port-channel's bandwidth.

standard

Specifies to use the standard behavior, which sets that the path cost does not change according to port-channel's bandwidth.

Modes

Spanning tree configuration mode

Examples

To set the behavior for the path cost to custom:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# port-channel path-cost custom

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# port-channel path-cost custom

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# port-channel path-cost custom

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# port-channel path-cost custom

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# port-channel path-cost custom
```

To set the behavior for the path cost to standard:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# port-channel path-cost standard

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# port-channel path-cost standard

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# port-channel path-cost standard

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# port-channel path-cost standard

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# port-channel path-cost standard
```

History

Release version	Command history
18x.1.00	This command was introduced.

preempt-mode

Enables or disables preempt mode for a VRRP or VRRP Extended (VRRP-E) router session.

Syntax

preempt-mode

no preempt-mode

Command Default

Enabled for VRRP; Disabled for VRRP-E.

Modes

Virtual-router-group configuration mode

Virtual-router-extended-group configuration mode

Usage Guidelines

This command is for VRRP and VRRP-E.

For VRRP-E, the interface must be a virtual interface (Ve).

When set, the highest-priority backup router will always be the master if the owner is not available. If not set, a higher priority backup will not preempt a lower-priority master.

Enter **no preempt-mode** to turn off preempt mode.

Examples

To turn on preempt mode for a virtual-router-group 1 session:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 10
device(config-if-Ve-10)# ipv6 vrrp-extended-group 1
device(config-vrrp-extended-group-1)# preempt-mode
```

History

Release version	Command history
18x.1.00	This command was introduced.

priority

Sets the priority of a physical router in a VRRP router group.

Syntax

priority *range*

Command Default

The default priority is 100.

Parameters

range

The priority of a physical router in a virtual router group. Higher numbers have priority over lower numbers. Valid values range from 1 to 254.

Modes

Virtual-router-group configuration mode

Virtual-router-extended-group configuration mode

Usage Guidelines

You can perform this command for VRRP or VRRP-E.

When set, the highest priority backup router will always be the master. (For VRRP, however, the owner is always the master if it is available.) If not set, a higher priority backup will not preempt a lower priority backup that is acting as master.

For an owner router in VRRP, the priority automatically becomes 255 if the virtual IP address of the virtual router and the real IP address of the owner are the same.

Examples

To set the priority to 110 for the VRRP virtual group 1:

```
device# configure terminal
device(config)# protocol vrrp
device(config)# interface ve 10
device(config-if-Ve-10)# vrrp-group 1
device(config-vrrp-group-1)# priority 110
```

To set the priority to 110 for the VRRP-E virtual group 1:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 10
device(config-if-Ve-10)# ipv6 vrrp-extended-group 1
device(config-vrrp-extended-group-1)# priority 110
```

History

Release version	Command history
18x.1.00	This command was introduced.

profile (LLDP)

Creates an LLDP profile.

Syntax

profile *name*

no profile *name*

Parameters

name

Assigns a name to the profile. The name must be between 1 and 63 ASCII characters in length.

name

Assigns a name to the profile. The name must be between 1 and 32 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile. Up to 64 profiles can be created.

Enter **no profile** *name* to remove the named profile.

Examples

The following example creates a profile named test.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# profile test
```

The following example creates a profile named test1.

```
device(config)# protocol lldp
device(conf-lldp)# profile ?
Possible completions:
<Profile Name (Max Size - 32)>
device(conf-lldp)# profile test1
device(config-profile-test1)#
```

The following example deletes a profile named test:

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# no profile test
```

History

Release version	Command history
18x.1.00	This command was introduced.

protocol

Configures the authentication protocol to use for communication with the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

protocol { **chap** | **pap** | **peap** }

no protocol

Command Default

The default protocol is Challenge Handshake Authentication Protocol (CHAP).

Parameters

chap

Specifies using CHAP for communication with the RADIUS server.

pap

Specifies using Password Authentication Protocol (PAP) for communication with the RADIUS server.

peap

Specifies using Protected Extensible Authentication Protocol (PEAP) for communication with the RADIUS server.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure PAP as the authentication protocol for communication with the RADIUS server.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# protocol pap
```

History

Release version	Command history
18x.1.00	This command was introduced.

protocol cfm

Enables the CFM protocol globally on the devices and enter into the CFM Protocol Configuration mode.

Syntax

protocol cfm

no protocol cfm

Command Default

This command is executed on the local switch.

Modes

Privileged EXEC mode

Usage Guidelines

The **no** form of this command disables the CFM protocol on the device.

Examples

```
device#(config)protocol cfm
device(config-cfm)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

protocol link-oam

Allows you to enter the link OAM global configuration mode.

Syntax

protocol link-oam

Command Default

This command is executed on the local switch.

Modes

Privileged EXEC mode

Examples

```
device# configure terminal
device(config)#protocol link-oam
device(config-link-oam)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

protocol lldp

Enters the Link Layer Discovery Protocol (LLDP) configuration mode.

Syntax

protocol lldp

no protocol lldp

Command Default

LLDP protocols are enabled.

Modes

Global configuration mode

Usage Guidelines

Enter **no protocol lldp** to restore the default settings.

Examples

To enter LLDP mode:

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)#
```

To reset all LLDP configurations:

```
device# configure terminal
device(config)# no protocol lldp
device(conf-lldp)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

protocol loop-detection

Enables the loop detection (LD) feature globally and enters Protocol Loop Detection configuration mode.

Syntax

protocol loop-detection

no protocol loop-detection

Command Default

This feature is disabled.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to disable loop detection globally.

Examples

To enable loop detection globally and enter Protocol Loop Detection configuration mode:

```
device# configure terminal
device(config)# protocol loop-detection
device(config-loop-detect)#
```

To disable loop detection globally:

```
device# configure terminal
device(config)# no protocol loop-detection
```

History

Release version	Command history
18x.1.00	This command was introduced.

protocol spanning-tree

Designates the context for spanning tree.

Syntax

protocol spanning-tree { **mstp** | **rstp** | **stp** | **pvst** | **rpvst** }

no protocol spanning-tree

Command Default

STP is not enabled. STP is not required in a loop-free topology.

Parameters

mstp
Specifies the Multiple Spanning Tree Protocol (MSTP).

rstp
Specifies the Rapid Spanning Tree (RSTP).

stp
Specifies the Spanning Tree Protocol (STP).

pvst
Specifies Per-VLAN Spanning Tree Protocol Plus (PVST+).

rpvst
Specifies Rapid Per-VLAN Spanning Tree Protocol Plus (R-PVST+).

Modes

Global configuration mode

Usage Guidelines

Consider enabling STP to detect or avoid loops. You must turn off one form of STP before turning on another form.

Packet drops or packet flooding may occur if you do not enable xSTP on all devices connected on both sides of parallel links.

Enter **no protocol spanning-tree** to delete the context and all the configurations defined within the context or protocol for the interface.

Examples

To enable the Spanning Tree Protocol:

```
device# configure terminal
device(config)# protocol spanning-tree stp
```

History

Release version	Command history
18x.1.00	This command was introduced.

protocol vrrp

Globally enables Virtual Router Redundancy Protocol (VRRP).

Syntax

protocol vrrp

no protocol vrrp

Command Default

VRRP is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command globally disables VRRP.

Examples

To enable VRRP:

```
device# configure terminal
device(config)# protocol vrrp
```

History

Release version	Command history
18x.1.00	This command was introduced.

protocol vrrp-extended

Globally enables VRRP-Extended.

Syntax

protocol vrrp-extended

no protocol vrrp-extended

Command Default

Disabled

Modes

Global configuration mode

Usage Guidelines

The **no protocol vrrp-extended** command globally disables VRRP-E.

Examples

To enable VRRP-Extended:

```
device# configure terminal
device (config)# protocol vrrp-extended
```

History

Release version	Command history
18x.1.00	This command was introduced.

prune-wait

Configures the time a PIM device waits before stopping traffic to neighbor devices that do not want the traffic.

Syntax

prune-wait *seconds*

no prune-wait

Command Default

The prune wait time is 3 seconds.

Parameters

seconds

Specifies the wait time in seconds. The range is 0 through 30 seconds. The default is 3 seconds.

Modes

PIM router configuration mode

Usage Guidelines

A smaller prune wait value reduces flooding of unwanted traffic. A prune wait value of 0 causes the PIM device to stop traffic immediately upon receiving a prune message.

If there are two or more neighbors on the physical port, you should not configure the **prune-wait** command because one neighbor may send a prune message while the other sends a join message at the same time, or within less than 3 seconds.

The **no** form of this command restores the default prune wait time of 3 seconds.

Examples

This example configures the prune wait time to 0 seconds.

```
device(config)# router pim
device(config-pim-router)# prune-wait 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

pw-profile

Creates a pseudowire (PW) profile that can be shared across multiple Virtual Private LAN Services (VPLS) bridge domains.

Syntax

pw-profile [*pw-profile-name* [**mtu** *mtu-value*] [**mtu-enforce** { *false* | *true* }] [**vc-mode** { **raw** | **raw-passthrough** | **tag** }]

no pw-profile *pw-profile-name* [**mtu**] [**mtu-enforce**] [**vc-mode**]]

Command Default

No PW profile is configured.

Parameters

pw-profile-name
Specifies the name of a PW profile.

mtu *mtu-value*
Specifies the maximum transmission unit (MTU) for the PW profile. The range is from 64 through 15966.

mtu-enforce
Configures MTU enforcement check during PW signaling.

false
Enables the MTU enforcement check.

true
Disables the MTU enforcement check.

vc-mode

NOTE
When a pseudowire profile is attached to a bridge domain, on which routing is enabled (by using the **router-interface** command), you are not allowed to change the pseudowire profile **vc-mode** configuration to **raw**.

Configures the virtual connection (VC) mode for the profile:

raw
Specifies using raw mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the VLAN tag is removed before it is sent out on the wire. When an untagged packet is received on an untagged AC endpoint it is encapsulated as is and sent out on the wire.

raw-passthrough
Specifies using raw-passthrough mode which enables interoperation with third-party devices. When all endpoints are configured as tagged endpoints, raw passthrough mode behaves the same way as tagged mode. When all endpoints are configured as untagged endpoints, raw-passthrough mode behaves the same way as raw mode. Select the **raw-passthrough** option, when all endpoints are configured as untagged endpoints (even when peer devices signal the PW VC mode as raw).

tag

Specifies using tag mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the packet is encapsulated as is and sent out on the wire. When an untagged packet is received on an untagged AC endpoint, a dummy tag is added and it is sent out on the wire.

Modes

Global configuration mode.

Usage Guidelines

You can configure up to 64 PW profiles.

The **no** form of the command removes the PW profile configuration.

Examples

The following example shows how to create a PW profile named test specifying that the VC mode for the profile is raw-passthrough.

```
device# configure terminal
device(config)# pw-profile test vc-mode raw-passthrough
```

History

Release version	Command history
18x.1.00	This command was introduced.

pw-profile (bridge domain)

Configures a pseudowire (PW) profile for a bridge domain.

Syntax

pw-profile *pw-profile-name*

no pw-profile

Command Default

A PW profile is not configured.

Parameters

pw-profile-name

Specifies the name of the PW profile to attach to the bridge profile.

Modes

Bridge-domain configuration mode.

Usage Guidelines

The **no** form of the command removes the PW profile from the bridge-domain configuration.

Examples

The following example shows how to configure a PW profile named test for bridge domain 1.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# pw-profile test
```

History

Release version	Command history
18x.1.00	This command was introduced.

python

Launches an interactive Python shell, with an option to launch a Python script.

Syntax

python [*python-statement* | *python-script-filename*] [*script-arguments*]

Parameters

python-statement
: Must be a valid python interpreter argument.

python-script-filename
: Runs a Python script file. Valid values range from 4 through 32 characters (including the **.py** extension). The first character must be alphabetic.

script-arguments
: Passes one or more arguments defined in the script.

Modes

Privileged EXEC mode

Usage Guidelines

This command is available only to users with admin-level permissions.

Entering **python**—with no additional parameters—launches an interactive Python shell.

Entering **python** *python-statement* launches an interactive Python shell and runs a valid *python-statement* that you enter. For example, entering `python -h` invokes the Python shell and displays Python options and arguments.

Entering **python** *python-script-filename* launches an interactive Python shell and runs the Python file. (To make a Python file available to this command, copy the Python file to the `flash://` location on the device, using the **copy** command.)

Note the following divergence between SLX-OS CLI syntax and Python syntax:

- Although in general, SLX-OS CLI syntax is not case-sensitive, Extreme convention is to use lower-case.
- Python syntax is case sensitive.

To exit the Python environment and return to the SLX-OS CLI, enter either:

- **exit()**
- **Ctrl-D**

Examples

The following example launches the Python shell and then both assigns an SLX CLI operational command to a Python variable and runs that command.

```
device# python
Python 3.3.2 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_show_users = CLI('show users')
!Command: show users
!Time: Tue Aug  9 09:09:39 2016

**USER SESSIONS**
Username            Role       Host IP       Device  Time Logged In
jdoe                admin      10.11.12.13   Cli     2016-08-09 09:06:46
admin               admin      127.1.0.1     Cli     18640
**LOCKED USERS**
Username
no locked users
>>>
```

The following example (partial) launches the Python shell to run a Python script-file.

NOTE

For an annotated text of this script, refer to the *Extreme SLX-OS Management Configuration Guide* under "Python Event-Management and Scripting" and "Python scripts and run-logs."

```
device# python create_po.py
!Command: show running-config vlan
!Time: Mon Aug 22 18:33:03 2016

vlan 1
!
vlan dot1q tag native

!Command: config
 vlan 101-105
!Time: Mon Aug 22 18:33:03 2016

!Command: show running-config vlan
!Time: Mon Aug 22 18:33:03 2016

vlan 1
!
vlan 101
!
vlan 102
!
vlan 103
!
vlan 104
!
vlan 105
!
vlan dot1q tag native

!Command: show running-config int po
!Time: Mon Aug 22 18:33:03 2016

interface Port-channel 1
 description Insight port-channel on MM1
 shutdown
!
interface Port-channel 2
 description Insight port-channel on MM2
 shutdown
!
!Command: config
 int po 10
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 101-105
 switchport trunk tag native-vlan ; no shut
!Time: Mon Aug 22 18:33:03 2016


!Command: show running-config int po
!Time: Mon Aug 22 18:33:04 2016

interface Port-channel 1
 description Insight port-channel on MM1
 shutdown
!
interface Port-channel 2
 description Insight port-channel on MM2
 shutdown
!
interface Port-channel 10
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 101-105
```

```
 switchport trunk tag native-vlan
 no shutdown
!

!Command: config
 int eth 0/4
 channel-group 10 mode active type standard
 no shut
!Time: Mon Aug 22 18:33:04 2016


!Command: show running-config int eth 0/4
!Time: Mon Aug 22 18:33:04 2016

interface Ethernet 0/4
 channel-group 10 mode active type standard
 lacp timeout long
 no shutdown
!

!Command: config
 int eth 0/5
 channel-group 10 mode active type standard
 no shut
!Time: Mon Aug 22 18:33:04 2016


!Command: show running-config int eth 0/5
!Time: Mon Aug 22 18:33:05 2016

interface Ethernet 0/5
 channel-group 10 mode active type standard
 lacp timeout long
 no shutdown
!

<output truncated>
```

The following example launches the Python shell to test an event-handler script-file.

> **NOTE**
>
> For more information, refer to the "Python Event-Management and Scripting" > "Guidelines for writing Python scripts" topic in the *Extreme SLX-OS Management Configuration Guide*.

```
device# python script.py --raslog-triggers {"SH-1002":" Event: exit, Status: success,
Info: User [admin] successfully exited from SLXVM Linux shell. Exit Time: Thu Apr 12 17:29:44 2018"}
```

qos cos

Changes the interface default Class of Service (CoS) value.

Syntax

qos cos *cos_value*

Command Default

The default is 0.

Parameters

value

Specifies the CoS value. Valid values range from 0 through 7.

Modes

Interface configuration mode

Examples

To set the CoS value to 2 on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos cos 2
```

To set the CoS value to 2 on a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos cos-mutation

Applies a user configured QoS CoS-to-CoS mutation map to an interface.

Syntax

qos cos-mutation *cos_map_name*

Command Default

No explicit QoS CoS-to-CoS mutation map is applied; the inbound CoS equals the outbound CoS.

Parameters

cos_map_name
The name of the CoS mutation map.

Modes

Interface configuration mode

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a QoS CoS-to-CoS mutation map to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos cos-mutation cos_mutation_map
```

To apply a QoS CoS-to-CoS mutation map to a specific port -channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos-mutation cos_mutation_map
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos cos-traffic-class

Applies a Quality of Service (QoS) CoS-to-traffic class mutation map on an interface.

Syntax

qos cos-traffic-class *cos_map_name*

Command Default

No explicit QoS CoS-to-traffic class mutation map is applied; the inbound CoS equals the outbound CoS.

Parameters

cos_tc_map_name
The name of the CoS-to-traffic class mutation map.

Modes

Interface configuration mode.

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

To activate a QoS CoS-to-traffic class mutation map named `cosMutMap` on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos cos-mutation cosMutMap
```

To activate a QoS CoS-to-traffic class mutation map from a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos-mutation cosMutMap
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos cpu slot

Use this command to configure the traffic manager (TM) CPU port shaper rate (all towers) to the line card (LC) CPU.

Syntax

qos cpu slot *slot_id* { **group** *group_id* { **prio** { *priority* | **all** } | **shaper rate** *shaper_rate* **burst** *burst_size* | **wfq weight** *weight_value* }

qos cpu slot *slot_id* { **port shaper rate** *shaper_rate* **burst** *burst_size* }

no qos cpu slot *slot_id* { **group** *group_id* { **prio** { *priority* | **all** } | **shaper rate** *shaper_rate* **burst** *burst_size* | **wfq weight** *weight_value* }

no qos cpu slot *slot_id* { **port shaper rate** *shaper_rate* **burst** *burst_size* }

Command Default

The TM CPU group or port shaper rate is not set.

Parameters

slot_id
The slot values are 0 on Pizzabox platforms, 1 through 4 on F4 platforms and, 1 through 8 on F8 platforms.

group *group_id*
Configures a CPU group.

shaper rate *shaper_rate*
Configures the TM CPU shaper rate (all towers) to LC CPU for CPU groups. The rate is in kilo bits per second (Kbps) with a range from 0 through 100000.

prio *priority*
C onfigures the TM CPU shaper rate (all towers) to line card CPU for individual priority VoQs within a CPU group. The priority value ranges from 0 through 7.

burst *burst_size*
Configures the CPU burst size in kbytes (KBs). For a group,enter an integer from 1 through 64 KB. For a port, enter an integer from 1 to 31.

wfq weight *weight_value*
Configures the CPU group's weighted fair queue value (all towers). The weight value ranges from 1 through 128. Higher value.

port
Configures a CPU port.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command removes the QoS CPU shaper configuration.

Examples

Set the TM CPU port shaper on slot 1 to priority 5, rate of 4500 Kbps, and a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 port shaper rate 4000 burst 1
```

Set the TM CPU port shaper on slot 1 to 4000 Kbps w/ a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 port shaper rate 4000 burst 1
```

Set the TM CPU on slot 1 group 1 priority to 5, shaper to 4500 Kbps, and a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 group 1 priority 5 shaper rate 4500 burst 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos dscp-cos

Applies a user configured QoS DSCP-to-CoS mutation map to an interface.

Syntax

qos dscp-cos *dscp_cos_map_name*

Command Default

No explicit QoS DSCP-to-CoS mutation map is applied.

Parameters

dscp_cos_map_name
Name of DSCP-to-COS mutation map

Modes

Interface configuration mode.

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a user configured QoS DSCP-to-COS mutation map named `dscpMap` to a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# qos dscp-cos dscpMap
```

Follow this example to apply a user configured QoS DSCP-to-COS mutation map named `dscpMap` to a specific port channel interface.

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-cos dscpMap
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos dscp-mutation

Applies a user configured QoS DSCP mutation map to an interface.

Syntax

qos dscp-mutation *dscp_map_name*

Command Default

No explicit user configured QoS DSCP-to-DSCP mutation map is applied; the inbound DSCP equals the outbound DSCP.

Parameters

dscp_map_name
The name of the DSCP mutation map

Modes

Interface subtype configuration mode

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a QoS DSCP-to-DSCP mutation map to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos dscp-mutation dscp_mutation_map
```

To apply a QoS DSCP-to-DSCP mutation map to a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-mutation dscp_mutation_map
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos dscp-traffic-class

Applies a user configured QoS DSCP-to-traffic- class mutation map to an interface.

Syntax

qos dscp-traffic-class *dscp_tc_name*

Command Default

No explicit user configured QoS DSCP-to-traffic class map is enabled on the interface.

Parameters

dscp_tc_name
Name of DSCP-to-traffic class map

Modes

Interface configuration mode

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a QoS DSCP-to-traffic class mutation map to a specific 40-gigabit Ethernet interface

```
device# configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# qos dscp-traffic-class dscp_tc_map
```

Follow this example to apply a QoS DSCP-to-traffic class mutation map to a specific port channel interface

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-traffic-class dscp_tc_map
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos flowcontrol

Configures link level flow control (IEEE 802.3x Flow Control) in the transmission and reception direction on an interface.

Syntax

qos flowcontrol tx { **on** | **off** } **rx** { **on** | **off** }

no qos flowcontrol

Command Default

By default, link level flow control (LLFC) reception is enabled.

Parameters

tx { **on** | **off** }
: Activates or deactivates the transmission portion of flow control.

rx { **on** | **off** }
: Activates or deactivates the reception portion of flow control.

Modes

Interface configuration mode

Usage Guidelines

LLFC alleviates system congestion by pausing data transmission. LLFC allows a congested receiver to communicate a PAUSE frame to a transmitter to stop data transmission until the congestion is cleared.

The device supports the transmission (Tx) and reception (Rx) of PAUSE frames for each physical interface or port channel.

LLFC can be configured only at the interface level.

Before configuring LLFC on an interface, stop the traffic on the interface.

Use the **no** form of this command to reset the default behavior.

Examples

The following example configures flow control on an interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-eth-1/4)# qos flowcontrol tx on rx on
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos map cos-mutation

Creates a QoS map for performing CoS-to-CoS mutation.

Syntax

qos map cos-mutation *name cos0 cos1 cos2 cos3 cos4 cos5 cos6 cos7*

no qos map cos-mutation *name*

Command Default

No CoS-to-CoS mutation QoS maps are defined.

Parameters

name

Specifies a unique name across all CoS-to-CoS mutation QoS maps defined within the system. If the named CoS-to-CoS mutation QoS map does not exist, then it is created. If the named CoS-to-CoS mutation QoS map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the QoS map.

cos#

Specifies the outbound CoS value.

CoS value	Description
cos0	Sets the outbound CoS value for all packets with inbound CoS 0.
cos1	Sets the outbound CoS value for all packets with inbound CoS 1.
cos2	Sets the outbound CoS value for all packets with inbound CoS 2.
cos3	Sets the outbound CoS value for all packets with inbound CoS 3.
cos4	Sets the outbound CoS value for all packets with inbound CoS 4.
cos5	Sets the outbound CoS value for all packets with inbound CoS 5.
cos6	Sets the outbound CoS value for all packets with inbound CoS 6.
cos7	Sets the outbound CoS value for all packets with inbound CoS 7.

Modes

Global configuration mode

Usage Guidelines

A CoS-to-CoS mutation takes an inbound CoS value and maps it to an outbound CoS value. The inbound CoS value is the user priority after any interface ingress QoS trust and Interface default CoS policy have been applied. The outbound CoS value is used in selecting Traffic Class and egress packet marking.

Enter **no qos map cos-mutation** *name* command to delete the named CoS-to-CoS mutation QoS map. A QoS map can only be deleted if it is not bound to any interface.

Examples

To create a CoS-to-CoS QoS mutation map to swap CoS 4 and CoS 5 and apply it on an interface, for example having inbound CoS 4 mapped to outbound CoS 5 and inbound CoS 5 mapped to outbound CoS 4; but all other CoS values go through unchanged:

```
device# configure terminal
device(config)# qos map cos-mutation cosMap 0 1 2 3 5 4 6 7
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# qos cos-mutation cosMap
```

To delete a CoS-to-CoS QoS mutation map:

```
device# configure terminal
device(config)# no qos map cos-mutation cosMap
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos map cos-traffic-class

A QoS CoS-to-traffic class mutation map can be configured using the following command syntax

Syntax

qos map cos-traffic-class *name*

no qos map cos-traffic-class *name*

Command Default

If CoS-to-traffic class mutation map is not defined, the default CoS-to-traffic class map is used, which is a one-to-one map for each priority.

Parameters

name

Specifies a unique name for the CoS-to-traffic class mutation QoS map. If the named map does not exist, then it is created. If the map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the map.

Modes

Global configuration mode

Usage Guidelines

A CoS-to-traffic class mutation map takes an inbound CoS value and maps it to an outbound traffic class (priority queue) value. The inbound CoS value is the user priority after any interface ingress QoS trust and Interface default CoS policy have been applied.

The drop-precedence parameter is optional.

Enter **no qos map cos-traffic-class** *name* command to delete the named QoS CoS-to-traffic class mutation map.

A QoS map can only be deleted if it is not bound to an interface.

Examples

To create a QoS CoS-to-traffic class mutation map use the following command

```
device# configure terminal
device(config)# qos map cos-traffic-class cosTC1
device(cos-traffic-class-cosTC1)# map cos 4 to traffic-class 3 drop-precedence 0
device(cos-traffic-class-cosTC1)# map cos 5 to traffic-class 5 drop-precedence 1
device(cos-traffic-class-cosTC1)# map cos 6 to traffic-class 6 drop-precedence 0
device(cos-traffic-class-cosTC1)# map cos 7 to traffic-class 6 drop-precedence 1
device(cos-traffic-class-cosTC1)# interface ethernet 1/1
device(conf-if-eth-1/1)# qos cos-traffic-class cosTC1
```

To delete a QoS CoS-to-traffic class mutation map that is bound to an interface follow this example.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no qos cos-traffic-class cosTC1
device(conf-if-eth-1/1)# exit
device(config)# no qos map cos-traffic-class cosTC1
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos map dscp-cos

Creates a QoS map where the ingress DSCP value is mapped to outgoing 802.1P values. This configures a DSCP-to-CoS map on the ingress interface.

Syntax

qos map dscp-cos *name*

no qos map dscp-cos *name*

map dscp *ingress dscp values* **to cos** *cos*

Command Default

DSCP-to-CoS mutation is not enabled.

Parameters

name
Name of DSCP-to-CoS map

map dscp
Ingress DSCP values.

cos
Egress CoS values.

ingress dscp values
Input DSCP values. The range of ingress DSCP values is 0 through 63.

cos
CoS value. The range is 0 through 7.

Modes

dscp-cos mode for the QoS **map dscp** commands

Global configuration mode

Usage Guidelines

This command remaps the incoming DSCP values of the ingress packet to egress CoS 802.1P values.

When you enter **qos map dscp-cos**, the system is placed in dscp-cos mode for the configured map. At this point, you can map ingress DSCP values to egress CoS values using the **map dscp** command.

Enter **qos dscp-cos** *name* while in configuration mode for a specific interface to apply the DSCP-to-CoS map to that interface.

Enter **no qos dscp-cos** *name* while in the interface configuration mode to remove the DSCP-to-CoS map from the interface.

Enter **no map dscp-cos** *name* while in global configuration mode to remove the DSCP-to-CoS map.

Examples

To create a QoS DSCP-to-CoS map and place system into dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)#
```

To map an ingress DSCP value to egress CoS value while in dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)# map dscp 43 to cos 4
```

To map multiple ingress DSCP values to egress CoS values while in dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)# map dscp 43 to cos 4
device(dscp-cos-test)# map dscp 63 to cos 6
device(dscp-cos-test)# map dscp 53 to cos 5
device(dscp-cos-test)# map dscp 23 to cos 2
```

To remove a QoS DSCP-CoS map while in global configuration mode:

```
device# configure terminal
device(config)# no qos map dscp-cos test
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos map dscp-mutation

Creates a DSCP mutation by mapping the incoming DSCP value of the ingress packet to outgoing DSCP values.

Syntax

qos map dscp-mutation *name*

no map qos dscp-mutation *name*

map dscp *ingress dscp values* **to dscp** *egress dscp value*

Command Default

DSCP mutation is not enabled.

Parameters

name
Name of DSCP mutation map

map dscp
Inbound DSCP values.

ingress dscp values
The ingress DSCP values. The range is from 0 through 63.

dscp
Outbound DSCP values.

egress dscp values
The egress DSCP value. The range is from 0 through 63.

Modes

dscp-mutation mode for the DSCP mutation map

Global configuration mode

Usage Guidelines

Enter **qos dscp-mutation** *name* while in configuration mode for a specific interface to apply the DSCP mutation map to that interface. When you enter **qos map dscp-mutation**, the system is placed in dscp-mutation mode for the configured map. At this point, you can map ingress DSCP values to egress DSCP values using the **dscp map** command.

Enter **no qos dscp-mutation** *name* while in interface configuration mode to remove the DSCP mutation map from that interface.

Enter **no map dscp-mutation** *name* while in global configuration mode to remove the DSCP mutation map.

Examples

To create a QoS DSCP mutation map and place system into dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)#
```

To map an ingress DSCP value to egress DSCP values while in dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)# map dscp 1,3,5,7 to dscp 40
```

To map multiple ingress DSCP values to egress DSCP values while in dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)# map dscp 60 to dscp 40
device(dscp-mutation-test)# map dscp 24 to dscp 50
device(dscp-mutation-test)# map dscp 33 to dscp 35
device(dscp-mutation-test)# map dscp 53 to dscp 61
```

To remove a QoS DSCP mutation map while in global configuration mode:

```
device# configure terminal
device(config)# no qos map dscp-mutation test
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos map dscp-traffic-class

Creates a QoS map for performing DSCP-to-traffic class mapping. This creates a DSCP-to-traffic class map on the ingress interface. You can configure an interface with either a DSCP-to-traffic class map or a CoS-to-traffic class map.

Syntax

qos map dscp-traffic-class *name*

no qos map dscp-traffic-class *name*

map dscp *ingress dscp values* **to traffic-class** *traffic class* [**drop-precedence** *out drop precedence*]

Command Default

DSCP-to-traffic class mutation is not enabled.

Parameters

name
Name of the QoS DSCP-to-traffic clas map.

map dscp
Ingress DSCP values. The range of ingress DSCP values is 0 through 63.

traffic-class
Egress traffic class values. The range of ingress traffic class values is from 0 through 7.

drop-precedence
Drop precedence value given egress packets. The range is 0 through 3.

ingress dscp values
Range of input DSCP values. The range is 0 through 63.

traffic class
The traffic class value. the range is from 0 through 7.

out drop precedence
Value of the output drop precedence. The range is 0 through 3.

Modes

dscp-traffic-class mode for the DSCP-to-traffic class map

Global configuration mode

Usage Guidelines

Enter **qos dscp-traffic-class** *name* while in configuration mode for a specific interface to apply the QoS DSCP-Traffic-Class map to that interface. When you enter **qos map dscp-traffic-class**, the system is placed in dscp-traffic-class mode for the configured map. At this point, you can map ingress DSCP values to traffic class values using the **mark** command.

Enter **no qos dscp-traffic-class** *name* while in the interface mode to remove the map from that interface.

Examples

To create a QoS DSCP-to-traffic class map and place system into dscp-traffic-class mode:

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)#
```

To map ingress DSCP values to a traffic class while in dscp-traffic-class mode:

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)# map dscp 1,3,5,7 to traffic-class 1 drop-precedence 1
```

To map multiple ingress DSCP values to traffic classes and drop precedence while in dscp-traffic-class mode:

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)# map dscp 10 to traffic-class 3 drop-precedence 1
device(dscp-traffic-class-test)# map dscp 40 to traffic-class 4 drop-precedence 1
device(dscp-traffic-class-test)# map dscp 45 to traffic-class 5 drop-precedence 0
device(dscp-traffic-class-test)# map dscp 52 to traffic-class 3 drop-precedence 1
```

To remove a QoS DSCP-traffic class map while in global configuration mode:

```
device# configure terminal
device(config)# no qos map dscp-traffic-class test
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos map traffic-class-cos

A QoS traffic class-to-CoS mutation map can be configured to create a priority mapping table using a traffic-class-cos map. The traffic class-to-CoS map is then applied to an egress interface to effect the priority re-mapping.

Syntax

qos map traffic-class-cos name

no qos map traffic-class-cos *name*

Command Default

If a QoS traffic class-to-CoS mutation map is not defined, the default traffic class-to-CoS map is used, which is a one-to-one map for each priority.

Parameters

name

Specifies a unique name for the QoS traffic class-to-CoS mutation map. If the named map does not exist, then it is created. If the map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the map.

Modes

Global configuration mode

Usage Guidelines

A traffic class can be mapped to the outgoing PCP value when a packet egresses the switch. You can create a priority mapping table using a traffic class-to-CoS map. This traffic class-to-CoS map can then be applied to an egress interface to effect the priority re-mapping. This feature only maps the internal traffic class to outgoing priority.

Enter **no qos map traffic-class-cos** *name* command to delete the named QoS traffic class-to-CoS mutation map.

A QoS map can only be deleted if it is not bound to an interface.

Examples

To create and apply a QoS traffic class-to-CoS mutation map use the following command:

```
device# configure terminal
device(config)# qos map traffic-class-cos CoSMap
device(traffic-class-cos-CoSMap)# map traffic-class 3 drop-precedence 1 to cos 2
device(traffic-class-cos-CoSMap)# map traffic-class 4 drop-precedence 1 to cos 3
device(traffic-class-cos-CoSMap)# map traffic-class 5 drop-precedence 2 to cos 4
device(conf-if-eth-1/4)# qos traffic-class-cos tcCos1
```

To delete a QoS traffic class-to-CoS mutation map that is bound to an interface follow this example.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# no qos traffic-class-cos CoSMap
device(conf-if-eth-1/4)# exit
device(config)# no qos map traffic-class-cos CoSMap
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos random-detect traffic-class

Configures Random Early Detect (RED) profile on a traffic class of an interface

Syntax

qos random-detect traffic-class *traffic-class* [**drop-precedence** *value*] **red-profile-id** *ID*

no qos random-detect traffic-class *traffic-class* [**drop-precedence**]

Parameters

traffic-class
Specifies the traffic class to apply the RED profile. Enter an integer from 0 through 7.

drop-precedence *value*
Optionally, specifies the drop precedence value for the traffic class. Enter an integer from 1 from 3.

red-profile-id *ID*
Specifies the RED profile to assign to traffic class on the interface. Enter the identifier for a configured profile.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of the command to remove the RED profile from the interface or the drop precedence for the traffic class on the interface.

Examples

The following example configures an RED profile on an interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# qos random-detect traffic-class 1 red-profile-id 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos red-profile

Configures a weighted random early detection (WRED) profile which includes the setting of the thresholds and drop probability by percentage.

Syntax

qos red-profile *profile-ID* **min-threshold** *min-percentage* **max-threshold** *max-percentage* **drop-probability** *percentage*

no qos red-profile *profile-ID*

Parameters

profile-ID
Specifies the profile identifier. Enter an integer from 0 to 383.

min-threshold *min-percentage*
Specifies the minimum average queue size in percentage for randomly dropping packets. Enter an integer from 0 through 100.

max-threshold *max-percentage*
Specifies the maximum average queue size in percentage which all packets are accepted by the device. Enter an integer from 0 through 100.

drop-probability *percentage*
Specifies the drop probability in percentage when the queue size is at the maximum. Enter an integer from 0 through 100.

Modes

Global configuration mode

Usage Guidelines

You can configure a maximum on 256 profiles.

After configuring the profile, apply it to an interface with the **qos random-detect traffic-class** command.

Use the **no** form of this command to delete the profile.

Examples

The following example is a WRED configuration.

```
device# configure terminal
device(config)# qos red-profile 1 min-threshold 30 max-threshold 60 drop-probability 44
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos rx-queue cos-threshold

Configures the QoS ingress queue cost of service (CoS) thresholds.

Syntax

qos rx-queue cos-threshold *threshold_value_0 threshold_value_1 threshold_value_2 threshold_value_3 threshold_value_4 threshold_value_5 threshold_value_6 threshold_value_7*

[no] qos rx-queue cos-threshold

Command Default

The CoS threshold values for the ingress queue are not configured.

Parameters

threshold_value_n

There are eight entries for this parameter with each entry representing a percentage. Each position matches a specific inbound CoS with the first position (**cos_threshold_0**) representing CoS 0, the second CoS 1, and so on.

Modes

Ethernet interface configuration mode.

Usage Guidelines

The total of all the entries cannot exceed 100%.

A 0 may be entered for any of the values.

Examples

Follow this example to configure the QoS ingress queue CoS thresholds on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# qos rx-queue cos-threshold 10 10 10 10 10 20 20 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos rx-queue multicast

Configures the multicast packet handling on an interface for virtual output queueing.

Syntax

qos rx-queue multicast { **best-effort-rate** | **guarantee-rate** } *kbps*

qos rx-queue multicast traffic class *number* **min-queue-size** *Mbytes* **max-queue-size** *Mbytes*

no qos rx-queue multicast best-effort-rate | **guarantee-rate**

no qos rx-queue multicast traffic class *number* **min-queue-size** *Mbytes* **max-queue-size** *Mbytes*

Parameters

best-effort-rate *kbps*
: Specifies the multicast best effort data rate in kilobits per second (kbps). Enter an integer from 704 through 600000000.

guarantee-rate *kbps*
: Specifies the multicast data guarantee data rate in kilobits per second (kbps). Enter an integer from 704 through 600000000.

traffic class *number*
: Specifies the traffic class on the interface. Enter an integer from 0 to 7.

min-queue-size *Mbytes*
: Specifies the minimum queue size in megabytes per second. Enter an integer from 0 through 1024.

max-queue-size *Mbytes*
: Specifies the maximum queue size in megabytes per second. Enter an integer from 0 through 2048.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of this command to remove the packet handling configuration.

Examples

The following example configures the multicast packet handling on the interface for virtual output queueing.

```
device# configure terminal
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# qos rx-queue multicast best-effort-rate 3000
device(conf-if-eth-1/2)# qos rx-queue multicast guarantee-rate 30000
device(conf-if-eth-1/2)# qos rx-queue multicast traffic-class 3 min-queue-size 512 max-queue-size 1024
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos rx-queue unicast traffic-class

Configures the ingress queue unicast packet traffic class parameter on an Ethernet interface.

Syntax

qos rx-queue unicast traffic-class *traffic_class* **min-queue-size** *minimum_size* **max-queue-size** *maximum_size*

no qos rx-queue unicast traffic class *number* **min-queue-size** *Mbytes* **max-queue-size** *Mbytes*

Parameters

traffic class *number*
Specifies the traffic class on the interface. Enter an integer from 0 to 7.

min-queue-size *Mbytes*
Specifies the minimum queue size in megabytes per second. Enter an integer from 0 through 1024.

max-queue-size *Mbytes*
Specifies the maximum queue size in megabytes per second. Enter an integer from 0 through 2048.

Modes

Ethernet interface configuration mode

Examples

The following example configures tan Ethernet interface ingress queue minimum and maximum queue size by a traffic class. .

```
device# configure terminal
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# qos rx-queue unicast traffic-class 3 min-queue-size 128 max-queue-size 1024
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos service-policy

Applies a policy map to all inbound traffic.

Syntax

qos service-policy in *service_policy_name*

no qos service-policy in *service_policy_name*

Parameters

in

Applies the service policy to inbound traffic.

service_policy_name

The name of the policy map.

Modes

Global configuration mode.

Usage Guidelines

The policy map has been preconfigured.

Enter **no qos service-policy in** *service_policy_name* to return to the default.

Examples

This example binds a service policy to inbound traffic at the system level.

```
device# configure terminal
device(config)# qos service-policy in policyMap1
device(config-service-policy-in/policyMap1)# end
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos traffic-class

Applies a QoS default traffic class value to an interface.

Syntax

qos traffic-class *default_tc_value*

Command Default

No explicit user configured QoS default traffic class priority value is configured.

Parameters

default_tc_value

The assigned traffic class priority value. The traffic class priority values range from 0 through 7.

Modes

Interface configuration mode

Examples

Follow this example to apply a default traffic class value to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos traffic-class 3
```

Follow this example to apply a default traffic class value to a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos traffic-class 3
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos traffic-class-cos

Applies a user configured QoS traffic class-to-CoS mutation map to an interface.

Syntax

qos traffic-class-cos *tc_cos_map*

Command Default

No explicit user configured QoS traffic class-to-CoS mutation maps are applied. The outbound traffic class equals the inbound traffic class.

Parameters

tc_cos_map

The name of the user configured QoS traffic class-to-CoS mutation map.

Modes

Interface configuration mode.

Usage Guidelines

The mutation maps are preconfigured.

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a user configured QoS traffic class-to-CoS mutation map to an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# qos traffic-class-cos tc_cos_map
```

Follow this example to apply a user configured QoS traffic class-to-CoS mutation map) to a port channel interface.

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos traffic-class-cos tc_cos_map
```

History

Release version	Command history
18x.1.00	This command was introduced.

qos tx-queue scheduler strict-priority

Configures the strict priority (SP) value for the egress queue traffic class scheduler and assigns a deficit weighted round robin (DWRR) weight.

Syntax

qos tx-queue scheduler strict-priority *traffic_class* dwrr *dwrr_weight*

[no] qos tx-queue scheduler strict-priority *traffic_class* dwrr *dwrr_weight*

Command Default

The SP value for the egress queue traffic class scheduler is not configured.

Parameters

tarffic_class

There are eight raffic class values:

Value	Traffic class
0	No strict priority queue.
1	Traffic class 7 strict priority queue.
2	Traffic class 6 through 7 strict priority queues.
3	Traffic class 5 through 7 strict priority queues.
4	Traffic class 4 through 7 strict priority queues.
5	Traffic class 3 through 7 strict priority queues.
6	Traffic class 2 through 7 strict priority queues.
7	Traffic class 1 through 7 strict priority queues.

dwrr *dwrr_weight*

Configure the DWRR queue weights. There are eight entries for this parameter with each entry representing a percentage. Tthe total of all the entries cannot exceed 100%. Each entry position represents a specific traffic class:

Place	Assignment
1	Traffic class 0 DWRR weight.
2	Traffic class 1 DWRR weight.
3	Traffic class 2 DWRR weight.
4	Traffic class 3 DWRR weight.
5	Traffic class 4 DWRR weight.
6	Traffic class 5 DWRR weight.
7	Traffic class 6 DWRR weight.
8	Traffic class 7 DWRR weight.

Modes

Global configuration mode

Usage Guidelines

The no form, of the command removes the SP value for the egress queue traffic class scheduler.

Examples

Use the following command to assign traffic classes 6 through 7 to a SP queue and assign DWRR weights.

```
device# configure terminal
device(config)# qos tx-queue scheduler strict-priority 2 dwrr 20 5 5 5 20 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

Commands R - Sh

radius-server host

Specifies a Remote Authentication Dial-In User Service (RADIUS) server, including the VRF to use for communication with the server, and enters RADIUS server host VRF configuration mode.

Syntax

radius-server host { *ip-address* | *host_name* } [**use-vrf** [*vrf-name*]]

no radius-server host { *hostname* | *ip-address* } [**use-vrf** [*vrf-name*]]

Command Default

A RADIUS server is not configured.

Parameters

ipaddr

Specifies the RADIUS server in IP addess format. Both IPv4 and IPv6 addresses are supported.

host_name

Specifies the RADIUS server in hostname format. The maximum supported length for the RADIUS server hostname is 40 characters.

use-vrf

(Optional) Causes communication with the RADIUS server through a specific VRF and enters configuration mode for RADIUS server communications through that VRF.

vrf-name

(Optional) Specifies a VRF through which to communicate with the RADIUS server. By default and when a VRF is not specified, the management VRF (mgmt-vrf) is used for communication with the RADIUS server.

Modes

Global configuration mode

Usage Guidelines

When a RADIUS server with the specified IP address or hostname does not exist, it is added to the server list. When the RADIUS server already exists, this command modifies the configuration.

The **no radius-server host** command removes the RADIUS server configuration.

NOTE

When only one RADIUS is configured, you can remove the RADIUS server configuration only when both login (EXEC) and command accounting are disabled by using, for example, the **no aaa accounting** command.

Examples

The following example shows how to configure a RADIUS server.

```
device# configure terminal
device(config)# radius-server host 10.24.65.6
device(config-radius-server-10.24.65.6/mgmt-vrf)#
```

The following example shows how to configure a RADIUS server and specifies that communication with the server takes place through the green-vrf.

```
device# configure terminal
device(config)# radius-server host 10.24.65.6 use-vrf green-vrf
device(config-radius-server-10.24.65.6/green-vrf)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

raslog-duration

Configures the interval between RASLog messages that are sent when a port is disabled by the loop detection (LD) protocol.

Syntax

raslog-duration {*minutes* }

no raslog-duration

Command Default

See the Usage Guidelines.

Parameters

minutes

Message interval in minutes. Range is from 10 through 1440. The default is 10.

Modes

Protocol Loop Detection configuration mode

Usage Guidelines

Use the **no** form of this command to revert to the default interval.

Examples

To specify a RASLog message interval of 20 minutes:

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# raslog-duration
```

To revert to the default interval:

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# no raslog-duration 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

rd (EVPN VLAN/BD)

Configures a Virtual Private Network (VPN) route distinguisher for a VLAN/bridge domain (BD) in an Ethernet VPN (EVPN) default instance.

Syntax

rd { *admin-value*:*arbitrary-value* | *IP-address*:*arbitrary-value* }

Parameters

admin-value

The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2-byte number (from 0 through 65535) or a 4-byte number (from 0 through 4294967295).

arbitrary-value

An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is is an IP address or a 2 byte ASN. The range is 0 through 4294967295 if the ASN is a 4 byte ASN.

IP-address

An IPv4 or IPv6 address.

Modes

EPVN VLAN/BD configuration mode

Usage Guidelines

Examples

The following example configures an RD and assigns the local ASN number 200:1.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain 200
device(config-bridge-domain-200)# rd 200:1
```

The following example configures an RD and assigns the IP address 10.1.1.1:1.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain 200
device(config-bridge-domain-200)# rd 10.1.1.1:1
```

History

Release version	Command history
18x.1.00	This command was introduced.

rd auto (EVPN)

Enables auto-generation of a route distinguisher (RD) for an Ethernet Virtual Private Network (EVPN) default instance.

Syntax

rd auto

no rd auto

Command Default

Disabled.

Modes

EVPN configuration mode

Usage Guidelines

Use the **no** form of this command to disable autogeneration of an RD.

Examples

The following example enables autogeneration of an RD on an EVPN default instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# rd auto
```

History

Release version	Command history
18x.1.00	This command was introduced.

region

Assigns a name to a Multiple Spanning Tree Protocol (MSTP) region.

Syntax

region *region-name*

no region

Parameters

region-name

Assigns a name to an MSTP region.

Modes

Spanning tree MSTP configuration mode

Usage Guidelines

The *region-name* string must be between 1 and 32 ASCII characters in length, and is case-sensitive.

Enter **no region** to delete the region name.

Examples

To assign a name to an MSTP region named extreme1:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# region extreme1
```

History

Release version	Command history
18x.1.00	This command was introduced.

remote-mep

Associates an action profile to a RMEP for a scheduled Two-Way ETH-SLM or Two-Way ETH-DM.

Syntax

remote-mep *rmep-id* **action-profile** *profile-name*

no remote-mep

Parameters:

rmep-id
Specifies the RMEP ID.

action-profile
Specifies the action profile.

profile-name
Specifies the profile name.

Modes

config-cfm-md-ma-mep configuration mode

Usage Guidelines

Use the **no** form of the command delete the RMEP action profile associations.

Examples

This example shows how to associate an action profile to a RMEP for a scheduled Two-Way ETH-SLM.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain-name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
device(config-cfm-md-ma-ma1)# mep 1 down Ethernet 1/2
device(config-cfm-md-ma-mep-1)#  remote-mep 2
device(config-cfm-md-ma-mep-1)#  remote-mep 2 action-profile my_action_profile
```

History

Release version	Command history
18x.1.00	This command was introduced.

rename

Renames a file in the device flash memory.

Syntax

rename *current_name new_name*

Parameters

current_name
Specifies the file name you want to change.

new_name
Specifies the new file name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

System configuration files cannot be renamed. If you try to rename a system file, a warning message is displayed.

Examples

The following example renames a file in the flash memory.

```
device# rename myconfig myconfig_20101010
```

History

Release version	Command history
18x.1.00	This command was introduced.

resequence access-list

Reassigns sequence numbers to entries of an existing MAC, IPv4, or IPv6 access list.

Syntax

resequence access-list { **ip** | **ipv6** | **mac** } *name seq_num increment*

Parameters

ip | **ipv6** | **mac**

Specifies the Layer 2 or Layer 3 ACL bound to an interface.

name

Specifies the name of a standard or an extended ACL. A maximum of 63 characters is allowed.

seq_num

Specifies the starting sequence number in the ACL. Valid values range from 1 through 65535.

increment

Specifies a value to increment the sequence number between rules. Valid values range from 1 through 65534.

Modes

Privileged EXEC mode

Usage Guidelines

Reordering the sequence numbers is useful when you need to insert rules into an existing ACL and there are not enough sequence numbers available. When all sequence numbers between rules are exhausted, this feature allows the reassigning of new sequence numbers to entries of an existing access list.

Examples

The following example reorders the rules in a MAC ACL.

```
device# show running-config mac access-list test
!
mac access-list standard test
 seq 1 permit 0011.2222.3333
 seq 2 permit 0011.2222.4444
 seq 3 permit 0011.2222.5555
 seq 4 deny 0011.2222.6666
!
device# resequence access-list mac test 10 10

device# show running-config mac access-list test
!
mac access-list standard test
 seq 10 permit 0011.2222.3333
 seq 20 permit 0011.2222.4444
 seq 30 permit 0011.2222.5555
 seq 40 deny 0011.2222.6666
!
```

The following example reorders the rules in an IPv6 ACL.

```
device# show running-config ipv6 access-list distList
!
ipv6 access-list standard distList
 seq 10 deny 2001:125:132:35::/64
 seq 20 deny 2001:54:131::/64
 seq 30 deny 2001:5409:2004::/64
 seq 40 permit any!
device# resequence access-list ipv6 distList 100 100

device# show running-config ipv6 access-list distList
!
ipv6 access-list standard distList
 seq 100 deny 2001:125:132:35::/64
 seq 200 deny 2001:54:131::/64
 seq 300 deny 2001:5409:2004::/64
 seq 400 permit any
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

retain route-target all

Configures a route reflector (RR) to accept all route targets (RTs).

Syntax

retain route-target all

no retain route-target all

Command Default

This feature is disabled.

Modes

BGP address-family EVPN configuration mode

Usage Guidelines

The **no** form of the command disables the retaining of all RTs.

Examples

The following example configures a RR to accept all RTs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# retain route-target all
```

History

Release version	Command history
18x.1.00	This command was introduced.

retries

Configures the number of retries allowed to establish a connection with the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

retries *num*

no retries

Command Default

The number of retries allowed is 5.

Parameters

num

Specifies the number of retries allowed to connect to a RADIUS server. The range is from 0 through 100. The default value is 5.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to set the number of retries allowed (to establish a connection with the RADIUS server) to 10.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# retries 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

revision

Assigns a version number to the Multiple Spanning Tree Protocol (MSTP) configuration.

Syntax

revision *number*

no revision

Command Default

The default is 0.

Parameters

number

Specifies the revision or version number of the MSTP region. Valid values range from 0 through 255.

Modes

]Spanning tree MSTP configuration mode

Usage Guidelines

Enter **no revision** to return to the default setting.

Examples

To set the configuration revision to 1:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# revision 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

rfc1583-compatibility (OSPF)

Configures compatibility with RFC 1583.

Syntax

rfc1583-compatibility

no rfc1583-compatibility

Command Default

OSPF is compatible with RFC 1583 (OSPFv2).

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

OSPF is compatible with RFC 1583 (OSPFv2) and maintains a single best route to an autonomous system (AS) boundary router in the OSPF routing table. Disabling this compatibility causes the OSPF routing table to maintain multiple intra-AS paths, which helps prevent routing loops.

Enter **no rfc1583-compatibility** to disable compatibility with RFC 1583.

Examples

The following example disables compatibility with RFC 1583.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# no rfc1583-compatibility
```

History

Release version	Command history
18x.1.00	This command was introduced.

rib-route-limit

Limits the maximum number of BGP Routing Information Base (RIB) routes that can be installed in the Routing Table Manager (RTM).

Syntax

rib-route-limit *num*

no rib-route-limit

Command Default

No maximum number of RIB routes is set.

Parameters

num

Decimal value for the maximum number of RIB routes to be installed in the RTM. Valid values range from 1 through 4294967295.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

This command controls the number of routes installed by BGP, irrespective of whether those BGP routes are the preferred routes in the system. BGP locally tracks the number of routes installed and the number of routes withdrawn from RIB. If the total number of routes installed exceeds the value specified by *num*, routes will not be installed.

If *num* is increased, route calculation is automatically triggered.

If *num* is decreased, the user is prompted to clear the BGP RTM.

Examples

The following example configures the device to limit the maximum number of BGP4 RIB routes that can be installed in the RTM.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# rib-route-limit 10000
```

The following example configures the device to limit the maximum number of BGP4+ RIB routes that can be installed in the RTM.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# rib-route-limit 32000
```

History

Release version	Command history
18x.1.00	This command was introduced.

rmon alarm

Sets the RMON alarm conditions.

Syntax

rmon alarm *index snmp_oid* **interval** *seconds* [**absolute** | **delta**] **rising-threshold** *value* **event** *number* [**falling-threshold** *value* **event** *number* [**owner** *name*]

no rmon alarm

Command Default

No alarms are configured.

Parameters

index
Specifies the RMON alarm index. Valid values range from 1 through 65535.

snmp_oid
Specifies the MIB object to monitor. The variable must be in the SNMP OID format, for example, 1.3.6.1.2.1.16.1.1.1.5.65535. The object type must be a counter32.

interval *seconds*
Specifies the RMON alarm sample interval in seconds. Valid values range from 1 through 2147483648.

absolute
Sets the sample type as absolute.

delta
Sets the sample type as delta.

rising-threshold *value*
Specifies the RMON alarm rising threshold. Valid values range from 0 through 4294967295.

event *number*
Specifies the event for the rising alarm. Valid values range from 1 through 65535.

falling-threshold *value*
Specifies the RMON alarm falling threshold. Valid values range from 0 through 4294967295.

event *number*
Specifies the event for the rising alarm. Valid values range from 1 through 65535.

owner *name*
Specifies the identity of the owner. The maximum number of characters is 32.

Modes

Global configuration mode

Usage Guidelines

Enter **no rmon alarm** to disable the alarm conditions.

Examples

To set RMON alarm conditions:

```
device# configure terminal
device(config)# rmon alarm 100 1.3.6.1.2.1.16.1.1.1.5.65535 interval 5 absolute rising-threshold 10000
event 100 falling-threshold 1000 event 101 owner admin
```

History

Release version	Command history
18x.1.00	This command was introduced.

rmon collection history

Collects Ethernet group statistics for later retrieval.

Syntax

rmon collection history *number* [**buckets** *bucket_number* | **interval** *seconds* | **owner** *name*]

no romn collection history *number*

Command Default

RMON history collection is not enabled.

Parameters

number

Specifies the RMON collection control index value. Valid values range from 1 through 65535.

buckets *bucket_number*

Specifies the maximum number of buckets for the RMON collection history. Valid values range from 1 through 65535.

interval *seconds*

Specifies the alarm sample interval in seconds. Valid values range from 1 through 3600. The default value is 1800.

owner *name*

Specifies the identity of the owner. The maximum number of characters is 15.

Modes

Interface subtype configuration mode

Usage Guidelines

This command collects periodic statistical samples of Ethernet group statistics on a specific interface for later retrieval.

Enter **no rmon collection history** *number* to disable the history of statistics collection.

Examples

To collect RMON statistics, with an RMON collection control index value of 5 for the owner named admin, on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# rmon collection history 5 owner admin
```

History

Release version	Command history
18x.1.00	This command was introduced.

rmon collection stats

Collects Ethernet group statistics n a specific interface.

Syntax

rmon collection stats *number* [**owner** *name*]

no rmon collection stats *number*

Command Default

RMON statistic collection is not enabled.

Parameters

number

Specifies the RMON collection control index value. Valid values range from 1 through 65535.

owner *name*

Specifies the identity of the owner.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no rmon collection stats** *number* to disable the collection of statistics.

Ethernet group statistics collection is not supported on ISL links.

Examples

The following example shows how to collect RMON statistics, with an RMON collection control index value of 2 for the owner named admin, on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# rmon collection stats 2 owner admin
```

History

Release version	Command history
18x.1.00	This command was introduced.

rmon event

Adds or removes an event in the RMON event table associated to the RMON alarm number.

Syntax

rmon event *index* [**description** *word* | **log** | **owner** *name* | **trap** *word*]

no rmon event

Command Default

No events are configured.

Parameters

index
Specifies the RMON event number. Valid values range from 1 through 65535.

description *word*
Specifies a description of the event.

log
Generates an RMON log when an event is triggered.

owner *name*
Specifies the owner of the event. The *name* string must be between 1 and 32 characters in length.

trap *word*
Specifies the SNMP community or string name to identify this trap.

Modes

Global configuration mode

Usage Guidelines

Enter **no rmon event** to remove the event configuration.

Examples

To configure an RMON event:

```
device# configure terminal
device(config)# rmon event 2 log description "My Errorstoday" owner gjack
```

History

Release version	Command history
18x.1.00	This command was introduced.

role name

Creates or modifies a non-default role.

Syntax

role name *role_name* [**desc** *description*]

no role name *role_name* [**desc** *description*]

Parameters

role_name
Specifies the name of the role.

desc *description*
Specifies an optional role description.

Modes

Global configuration mode

Usage Guidelines

For each role that you create, you define one or more rules. Each user is associated with one—and only one—role.

Role names are from 4 through 32 characters, must begin with a letter, and can contain alphanumeric characters and underscores. The name cannot be same as that of an existing user.

The description field supports up to 64 characters and can include any printable ASCII character, except for the following characters: single quotation mark (‘), double quotation mark (“), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces, enclose the text in double quotation marks.

The maximum number of roles supported is 64, including the user and admin default roles.

To delete a role description, enter **no role name** *role_name* **desc**.

To delete a role, enter **no role name** *role_name*.

Examples

The following example creates a role.

```
device# configure terminal
device(config)# role name tempAdmin desc "Daily admin functions"
```

The following example deletes the role.

```
device# configure terminal
device(config)# no role name tempAdmin
```

History

Release version	Command history
18x.1.00	This command was introduced.

root access console

Restricts the root access to the device to the console only.

Syntax

root access console

no root access console

Modes

Global configuration mode

Usage Guidelines

The **no root access console** allows root access to the device through all terminals (SSH, Telnet, and console).

Examples

Typical command output:

```
device# configure terminal
device(config)# do show running-config | include root
% No entries found.
device(config)# root access console
device(config)# do show running-config | include root
root access console
device(config)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

root enable

Enables root access to the device following a firmware configuration.

Syntax

root enable

no root enable

Modes

Global configuration mode

Usage Guidelines

The **no root enable** command disables root access to the device.

Examples

Typical command output:

```
device# configure terminal
device(config)# do show running-config | include root
% No entries found.
device(config)# root enable
% Info: Root password is at system default, for better security, you may want to change it.
device(config)# do show running-config | include root
root enable
device(config)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

route-map (BGP)

Creates or modifies a route-map under Border Gateway Protocol (BGP).

Syntax

route-map *name* { **permit** | **deny** } *stanza*

no route-map *name* { **permit** | **deny** } *stanza*

Parameters

name

Specifies the name of the route map. The string must be between 1 and 63 ASCII characters in length.

permit

Allows a matching pattern.

deny

Disallows a matching pattern.

stanza

Specifies the stanza ID. Valid values range from 1 through 65535. A route map can support up to 1024 stanzas.

Modes

Global configuration mode

Usage Guidelines

This command is used in conjunction with the **match** and **set** commands.

The **continue** command configures the route map to continue to evaluate and execute match statements after a successful match occurs. The **continue** statement proceeds to the route map with the specified sequence number. If no sequence number is specified, the statement proceeds to the route map with the next sequence number (as an "implied" continue).

The **no** form of this command deletes a route-map stanza.

Examples

The following example configures a route map that allows a matching pattern.

```
device# configure terminal
device(config)# route-map test permit 5
```

The following example configures continue statements in a route map.

```
device# configure terminal
device(config)# route-map mcontroutemap1 permit 1
device(config-route-map-mycontroutemap/permit/1)# match metric 10
device(config-route-map-mycontroutemap/permit/1)# set weight 10
device(config-route-map-mycontroutemap/permit/1)# match metric 10
device(config-route-map-mycontroutemap/permit/1)# continue 2
device(config-route-map-mycontroutemap/permit/1)# route-map mcontroutemap1 permit 2
device(config-route-map-mycontroutemap/permit/2)# match tag 10
device(config-route-map-mycontroutemap/permit/2)# set weight 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

route-only

Configures VE route-only mode on physical ports and port-channels (LAG ports), to enable the exclusive IP routing of incoming packets. Incoming switching packets on the port are dropped, and outgoing switching packets are forwarded.

Syntax

route-only

no route-only

Command Default

This feature is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to disable this feature.

Examples

To configure VE route-only mode on a physical port.

```
device# configure terminal
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# switchport
device(conf-if-eth-1/2)# switchport mode trunk
device(conf-if-eth-1/2)# switchport mode trunk allowed vlan add 100
device(conf-if-eth-1/2)# route-only
device(conf-if-eth-1/2)# no shutdown
```

To disable VE route-only mode on a physical port.

```
device# configure terminal
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# no route-only
```

To configure VE route-only mode on a LAG port:

```
device# configure terminal
device(config)# interface port-channel 1
device(config-Port-channel-1)# switchport
device(config-Port-channel-1)# switchport mode trunk
device(config-Port-channel-1)# switchport mode trunk allowed vlan add 100,200
device(config-Port-channel-1)# switchport trunk tag native-vlan
device(config-Port-channel-1)# route only
device(config-Port-channel-1)# no shutdown
```

To disable VE route-only mode on a LAG port:

```
device# configure terminal
device(config)# interface port-channel 1
device(config-Port-channel-1)# no route-only
```

History

Release version	Command history
18x.1.00	This command was introduced.

route-precedence

Configures a table that defines the order (precedence) in which multicast routes are selected from the multicast routing table (mRTM) and unicast routing (uRTM) table.

Syntax

route-precedence { [**none** | **uc-default** |**uc-non-default**] | [**uc-default** | **none** |**uc-non-default**] | [**uc-non-default** | **none** |**uc-default**] }

no route-precedence

Command Default

The default route precedence used to select routes is **uc-non-default** followed by **uc-default**.

Parameters

none

Specifies that this type of route is to be ignored. You can specify this option for any of the multicast or unicast route types.

uc-non-default

Specifies the precedence for the non-default unicast route table (uRTM).

uc-default

Specifies the precedence for the default unicast route table (uRTM).

Modes

Router PIM configuration mode

Usage Guidelines

The order in which you place the keywords determines the route precedence.

The **no** form of this command restores the default route precedence settings.

Examples

The following example configures the route precedence.

```
device(config)# router pim
device(config-pim-router)# route-precedence uc-default uc-non-default none
```

History

Release version	Command history
18x.1.00	This command was introduced.

route-target

Configures route-target for distribution of routes between VPN routing tables.

Syntax

route-target { **import** | **export** | **both** } *ASN-nn*

no route-target

Parameters

import
Specifies export.

export
Specifies export.

both
Specifies both export and import.

ASN-nn
Composed of the local ASN number followed by a colon ":" and a unique arbitrary number. For example 3:6.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of the command to delete configuration for the route-target for distribution.

Examples

The following example shows how to configures route-target for distribution of routes between VPN routing tables.

```
device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd1 1:2
device#(config-vrf-vpn1)# vpn-statistics
device#(config-vrf-vpn1)# address-family ipv4 unicast
device#(config-vrf-vpn1-ipv4-unicast)# route-target-import 100:1
device#(config-vrf-vpn1-ipv4-unicast)# route-target-export 100:1
```

History

Release version	Command history
18x.1.00	This command was introduced.

route-target (EVPN)

Enables auto-generation of the import and export route-target community attributes for an Ethernet Virtual Private Network (EVPN) default instance.

Syntax

route-target { **both** | **import** } **auto** [**ignore-as**]

route-target export auto

no route-target { **both** | **import** } **auto** [**ignore-as**]

no route-target export auto

Command Default

Disabled.

Parameters

both auto
Specifies auto-generation of the import and export route-target community attributes.

ignore-as
Specifies that the autonomous system (AS) number be ignored.

export auto
Specifies auto-generation of the export route-target community attribute.

import auto
Specifies auto-generation of the import route-target community attribute.

Modes

EVPN configuration mode

Usage Guidelines

The **no** form of this command removes configured route target parameters.

Examples

The following example configures auto-generation of the import and export route-target community attributes for EVPN default instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# route-target both auto
```

The following example configures auto-generation of the import route-target community attribute and specifies that the AS path be ignored to the route for EVPN default instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# route-target import auto ignore-as
```

The following example configures auto-generation of the export route-target community attribute for EVPN myinstance instance.

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# route-target export auto
```

History

Release version	Command history
18x.1.00	This command was introduced.

route-target (EVPN VLAN/BD)

Enables auto-generation of the import and export route-target community attributes for a VLAN/bridge domain (BD) in an Ethernet Virtual Private Network (EVPN) default instance.

Syntax

route-target { **both** | **import** } **auto** [*admin-value*:*arbitrary-value*]

route-target export auto [*admin-value*:*arbitrary-value*]

no route-target { **both** | **import** } **auto** [**ignore-as**]

no route-target export auto

Command Default

Disabled.

Parameters

both auto
Specifies auto-generation of the import and export route-target community attributes.

export auto
Specifies auto-generation of the export route-target community attribute.

import auto
Specifies auto-generation of the import route-target community attribute.

admin-value
The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2-byte number (from 0 through 65535) or a 4-byte number (from 0 through 4294967295).

arbitrary-value
An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is is an IP address or a 2-byte ASN. The range is 0 through 4294967295 if the ASN is a 4-byte ASN.

Modes

EVPN VLAN/BD configuration mode

Usage Guidelines

The **no** form of this command removes configured route target parameters.

Examples

The following example configures auto-generation of the import and export route-target community attributes for EVPN VLAN/BD 200.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain 200
device(config-bridge-domain-200)# route-target both 200:1
```

History

Release version	Command history
18x.1.00	This command was introduced.

router bgp

Enables BGP routing.

Syntax

router bgp

no router bgp

Command Default

BGP routing is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables BGP routing.

Examples

The following example enables BGP routing.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

router ospf

Enables and configures the Open Shortest Path First version 2 (OSPFv2) routing protocol.

Syntax

router ospf [**vrf** *name*]

no router ospf

Parameters

vrf *name*

Specifies a nondefault VRF.

Modes

Global configuration mode

Usage Guidelines

Use this command to enable the OSPFv2 routing protocol and enter OSPF router or OSPF router VRF configuration mode. OSPFv2 maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

The **no** form of the command deletes all current OSPF configuration and blocks any further OSPFv2 configuration.

Examples

The following example enables OSPFv2 on a default VRF and enters OSPF VRF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)
```

History

Release version	Command history
18x.1.00	This command was introduced.

router pim

Configures basic global protocol-independent multicast (PIM) Sparse parameters on a device within the PIM Sparse domain and enters PIM-router configuration mode.

Syntax

router pim

no router pim

Command Default

PIM Sparse is not configured.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables PIM and removes all configuration for PIM multicast on the device (**router pim** level) only.

You do not need to globally enable IP multicast routing when configuring PIM Sparse.

After you enable IP multicast routing and PIM Sparse at the global level, you must enable it on the individual interfaces connected to the PIM Sparse network.

If you configure PIM Sparse on an interface that is on the border of the PIM Sparse domain, you also must also configure the **ip pim border** command on the interface.

You must configure the **bsr-candidate ethernet** command to identify an interface on at least one device as a candidate PIM Sparse Bootstrap router (BSR) and candidate PIM Sparse Rendezvous Point (RP).

You can configure the **rp-address** command to explicitly identify an RP, including an ACL-based RP, by its IP address instead of having it identified by the RP election process.

Examples

This example configures basic global PIM Sparse parameters.

```
device(config)# router pim
```

History

Release version	Command history
18x.1.00	This command was introduced.

router-interface

Binds a router interface to a tunnel or bridge domain.

Syntax

router-interface ve *num*

no router-interface

Command Default

A router interface is not configured.

Parameters

ve *num*

Specifies a virtual interface number on the router.

Modes

Bridge domain configuration mode

Tunnel interface configuration mode

Usage Guidelines

NOTE

You cannot enable routing on a VPLS instance when the **vc-mode** option on the PW attached to the instance is set to **raw**.

When routing is enabled on a VPLS instance that has only one PW and no local endpoints, the VPLS instance is brought to an active state; this state enables routing when the next hop is the PW endpoint.

The **no** form of the command removes the router interface configuration.

Examples

The following example shows how to attach a virtual router interface to a tunnel.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
```

The following example shows how to bind a virtual router interface to a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 100
device(config-bridge-domain-100)# router-interface ve 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

rp-address

Configures a device interface as a rendezvous point (RP).

Syntax

rp-address *ip-address*

no rp-address *ip-address*

Command Default

The RP is selected by the PIM Sparse protocol's RP election process.

Parameters

ip-address

Specifies the IPv4 address of the RP.

Modes

Router PIM configuration mode

Usage Guidelines

The **no** form of this command restores the default and the RP is selected by the RP election process.

Devices in the PIM Sparse domain use the specified RP and ignore group-to-RP mappings received from the bootstrap router (BSR).

The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse routers learn the addresses of RPs and the groups for which they are responsible from messages that the BSR sends to each of the PIM Sparse routers.

Examples

This example configures the device interface at IP address 4.4.4.4 as the RP for the PIM Sparse domain. The default group range is 224/4.

```
device(config)# router pim
device(config-pim-router)# rp-address 4.4.4.4
```

This example configures the RP with specific group ranges:

```
device(config)# router pim
device(config-pim-router)# rp-address 4.4.4.4 static-rp-plist
device(config)# ip prefix-list static-rp-plist permit 225.1.1.0/24
```

History

Release version	Command history
18x.1.00	This command was introduced.

rp-candidate

Configures a device as a candidate rendezvous point (RP) for all multicast groups with the prefix 224.0.0.0/4, by default, and explicitly adds or deletes groups with other prefixes.

Syntax

rp-candidate [**interface** *interface type* | **prefix** *IP prefix-list name*]

Command Default

The PIM router is not available for selection as an RP.

Parameters

interface *interface type*
Specifies an interface for the candidate RP. Interface types include ethernet, loopback, port-channel, and Ve.

prefix *IP prefix list name*
Specifies the IP prefix list name.

Modes

Router PIM configuration mode

Usage Guidelines

The **no rp-candidate** command makes the PIM router cease to act as a candidate RP.

Configuring the **rp-candidate** command on an Ethernet, loopback, virtual, or tunnel interface, configures the device as a candidate RP for all multicast groups with the prefix 224.0.0.0/4, by default. You can configure the **rp-candidate add** command to add to those a group address or range of group addresses. You can configure the **rp-candidate delete** command to delete a group address or range of group addresses that were added to the default addresses.

NOTE
You cannot delete the default group prefix.

The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse routers learn the addresses of RPs and the groups for which they are responsible from messages that the bootstrap router (BSR) sends to each of the PIM Sparse routers.

Although you can configure the device as only a candidate BSR or an RP, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

Examples

This example configures a physical device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate ethernet 1/1
```

This example configures a loopback interface as a candidate RP:

```
device(config-pim-router)# rp-candidate interface loopback 11
device(config-pim-router)# rp-candidate prefix my-rp-cand-list
device(config)# ip prefix-list my-rp-cand-list permit 226.1.1.0/24
device(config)# ip prefix-list my-rp-cand-list permit 228.1.1.0/24
```

History

Release version	Command history
18x.1.00	This command was introduced.

rpf ecmp rebalance

Enables multicast ECMP load sharing with dynamic rebalancing.

Syntax

rpf ecmp rebalance

no rpf ecmp rebalance

Modes

Router PIM configuration mode

Usage Guidelines

Once you configure ECMP rebalance the existing flows are redistributed among the all available ECMP paths. In addition, whenever a new next-hop is added, some of the existing flows are redistributed to the new path added using the newly added ECMP path.

Examples

The following example enables multicast ECMP load sharing with dynamic rebalancing.

```
device(config)# router pim
devic(config-pim-router)# rpf ecmp rebalance
```

History

Release version	Command history
18x.1.00	This command was introduced.

rule

Creates role-based access permissions (RBAC) associated with a role.

Syntax

rule *index* [**action** { **accept** | **reject** }] [**operation** { **read-only** | **read-write** }] **role** *role_name* **command** *command_name*

no rule *index*

Command Default

The default for **action** is **accept**. The default for **operation** is **read-write**.

Parameters

index
Specifies a numeric identifier for the rule. Valid values range from 1 through 512.

action accept | **reject**
(Optional) Specifies whether the user is accepted or rejected while attempting to execute the specified command. The default value is **accept**.

operation read-only | **read-write**
(Optional) Specifies the type of operation permitted. The default value is **read-write**.

role *role_name*
Specifies the name of the role for which the rule is defined.

command *command_name*
Specifies the command for which access is defined. Separate commands with a space. To display a list of supported commands, type a question mark (?).

Modes

Global configuration mode

Usage Guidelines

For each role that you create, you define one or more rules. Each account is associated with one—and only one—role.

When you create a rule, the *index*, **role**, and **command** operands are mandatory; the **action** and **operation** operands are optional.

The maximum number of rules is 512.

When you modify a rule, all operands except *index* and **role** are optional.

Enter **no rule** *index* to remove the specified rule.

Examples

The following example creates rules enabling the NetworkSecurityAdmin role to create user accounts.

```
device# configure terminal
device(config)# rule 150 action accept operation read-write role NetworkSecurityAdmin command config
device(config)# rule 155 action accept operation read-write role NetworkSecurityAdmin command username
```

The following example deletes a rule.

```
device# configure terminal
device(config)# no rule 155
```

History

Release version	Command history
17s.1.00	This command was introduced.

scheduler

Configures the strict priority queues on an interface for QoS egress scheduling.

Syntax

scheduler strict-priority *traffic-class-queues* **dwrr** *TC0-BW% TC1-BW% TC2-BW% TC3-BW% TC4-BW% TC5-BW% TC6-BW% TC7-BW%*

no scheduler strict-priority

Parameters

traffic-class-queues

Specifies the traffic class strict priority queues. Enter one of the following integers:

- 0—No strict priority queues
- 1—Traffic class 7 strict priority queue
- 2—Traffic class 6 through 7 strict priority queues
- 3—Traffic class 5 through 7 strict priority queues
- 4—Traffic class 4 through 7 strict priority queues
- 5—Traffic class 3 through 7 strict priority queues
- 6—Traffic class 2 through 7 strict priority queues
- 7—Traffic class 1 through 7 strict priority queues

drww *TC0-BW% TC1-BW% TC2-BW% TC3-BW% TC4-BW% TC5-BW% TC6-BW% TC7-BW%*

Configures the Deficit Weighted Round Robin queues in percentage for each traffic class, if the priority is in weighted fair queue (WFQ) mode. Enter an integer from 0 through 100 (*TC0-BW* for traffic class 0 through *TC7-BW* for traffic class 7). The total of all values must equal 100%.

Modes

Policy-map configuration mode

Usage Guidelines

This command is allowed only for the egress direction.

Use the **no** form of this command to remove QoS egress scheduling from the interface.

Examples

The following example configures QoS egress scheduling on an interface.

```
device# configure terminal
device(config)# policy-map policy_1
device(config-policymap)# class default
device(config-policymap-class)# scheduler strict-priority 1 dwrr 25 25 25 10 5 5 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

seq (rules in IPv4 extended ACLs)

Inserts filtering rules in IPv4 extended ACLs. Extended ACLs permit or deny traffic according to source and destination addresses, as well as other parameters.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] { *D_IPaddress mask* | **host** *D_IPaddress* | **any** } [**dscp** *DSCPvalue*] [**dscp-force**] [**drop-precedence-force** *dp-value*] [*destination-operator* [*D_port-numbers*]] [*TCP-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] { *D_IPaddress mask* | **host** *D_IPaddress* | **any** } [**dscp** *DSCPvalue*] [**dscp-force**] [**drop-precedence-force** *dp-value*] [*destination-operator* [*D_port-numbers*]] [*TCP-flags*] [**count**] [**vlan** *vlanID*] [**log**] [**mirror**] [**copy-sflow**]

no { **permit** | **deny** | **hard-drop** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] { *D_IPaddress mask* | **host** *D_IPaddress* | **any** } [**dscp** *DSCPvalue*] [**dscp-force**] [**drop-precedence-force** *dp-value*] [*destination-operator* [*D_port-numbers*]] [*TCP-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

ip-protocol

Indicates the type of IP packet you are filtering. The options are as follows:

<0-255>

Protocol number custom value from 0 through 255.

icmp

Internet Control Message Protocol

ip

Any IP protocol

tcp

(Supported only if the containing ACL is applied to incoming traffic) Transmission Control Protocol

udp

User Datagram Protocol

S_IPaddress

Specifies a source address for which you want to filter the subnet.

mask

Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

host

Specifies a source address.

S_IPaddress

The source address.

any

Specifies all source addresses.

source-operator and *destination-operator*

If you specified **tcp** or **udp** *ip-protocol*, the following optional operators are available:

eq

The policy applies to the TCP or UDP port name or number you enter after **eq**.

gt

The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt**.

lt

The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt**.

neq

The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

range

The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53 (two values separated by a space). The first port number in the range must be lower than the last number in the range.

S_port-numbers and *D_port_numbers*

(Valid only when *ip-protocol* is UDP or TCP) Specifies one or more source or destination port numbers.

D_IPaddress

Specifies a destination address for which you want to filter the sub-net.

mask

Defines a mask, whose effect is to specify a subnet that includes the destination address that you specified. For options to specify the mask, see the Usage Guidelines.

host

Specifies a destination address.

D_IPaddress

The destination address.

any
Specifies all destination addresses.

dscp
Matches *DSCPvalue* against the DSCP value of the packet.

DSCPvalue
From 0 through 63. For additional options, press ?.

dscp-force
(In **permit** rules, for incoming routed packets) Forces the outgoing DSCP value of packets that match the filter.

drop-precedence-force *dp-value*
(In **permit** rules for incoming traffic) Sets the force drop precedence by the specified value.

vlan *vlanID*
Specifies a VLAN interface to which the ACL is bound.

TCP-flags
If you specify **tcp** *ip-protocol*, one or more of the following flags are available:

ack
Filters packets for which the **ack** (acknowledge) flag is set.

fin
Filters packets for which the **fin** (finish) flag is set.

rst
Filters packets for which the **rst** (reset) flag is set.

sync
Filters packets for which the **syn** (synchronize) flag is set.

urg
Filters packets for which the **urg** (urgent) flag is set.

push
Filters packets for which the **psh** (push) flag is set.

count
Enables statistics for the rule.

log
Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

mirror
(Supported for rules in ACLs applied on physical interfaces to inbound traffic. Not supported for PBR, rACLs, or ACL-RL.) Mirrors packets matching the rule.

copy-sflow
(Not currently supported) Sends matching inbound packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. (For details, refer to the *Extreme SLX-OS QoS and Traffic Management Configuration Guide*.)

- Because ACLs applied for QoS use implement a unified counter for all rules in an ACL, rule-level **count** keywords are ignored.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not applied.

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL, from an interface-subtype configuration mode you use the { **ip** | **ipv6** | **mac** } **access-group** command.
- To apply a receive-path ACL, from global configuration mode, you use the { **ip** | **ipv6** } **receive access-group** command.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** followed by the full syntax without **seq** *seq-value*.

Examples

The following example creates an IPv4 extended ACL and defines rules.

```
device(config)# ip access-list extended extdACL5
device(conf-ipacl-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
device(conf-ipacl-ext)# seq 7 deny tcp any any eq 80
device(conf-ipacl-ext)# seq 10 deny udp any any range 10 25
device(conf-ipacl-ext)# seq 15 permit tcp any any
```

The following example creates an IPv4 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ip access-list extended ipv4-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20.0.0.1 count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq bgp count
device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.3 host 224.0.0.1 count
device(conf-ipacl-ext)# exit
device(config)# ip receive access-group ipv4-receive-acl-example
```

History

Release version	Command history
18x.1.00	This command was introduced.

seq (rules in IPv4 standard ACLs)

Inserts filtering rules in IPv4 standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**log**] [**copy-sflow**]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**log**] [**copy-sflow**]

no { **permit** | **deny** | **hard-drop** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**log**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

S_IPaddress

Specifies a source address for which you want to filter the subnet.

mask

Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

host

Specifies a source address.

S_IPaddress

The source address.

any

Specifies all source addresses.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

copy-sflow
(Currently not supported) (For incoming traffic) Sends matching packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. For details, refer to the *Extreme SLX-OS QoS and Traffic Management Configuration Guide*.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a "pass-through": For a match, QoS action defined for that class is not applied.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without **seq** *seq-value*.

Examples

The following example shows how to create a IPv4 standard ACL, define rules for it, and apply the ACL to an interface:

```
device# configure
device(config)# ip access-list standard stdACL3
device(conf-ipacl-std)# seq 5 permit host 10.20.33.4
device(conf-ipacl-std)# seq 15 deny any
device(conf-ipacl-std)# exit
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# ipv4 access-group stdACL3 in
```

History

Release version	Command history
18x.1.00	This command was introduced.

seq (rules in IPv6 extended ACLs)

Inserts filtering rules in IPv6 extended ACLs. IPv6 extended ACLs permit or deny traffic according to source address, as well as other parameters.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] { **any** | *D_IPaddress* **/** *prefix_len* | **host** *D_IPaddress* } [*destination-operator* [*D_port-numbers*]] [**dscp** *DSCPvalue*] [**dscp-force**] [**drop-precedence-force** *dp-value*] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] { **any** | *D_IPaddress* **/** *prefix_len* | **host** *D_IPaddress* } [*destination-operator* [*D_port-numbers*]] [**dscp** *DSCPvalue*] [**dscp-force**] [**drop-precedence-force** *dp-value*] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] { **any** | *D_IPaddress* **/** *prefix_len* | **host** *D_IPaddress* } [*destination-operator* [*D_port-numbers*]] [**dscp** *DSCPvalue*]] [**dscp-force**] [**drop-precedence-force** *dp-value*] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

ip-protocol

Indicates the type of IP packet you are filtering. The options are as follows:

<0-255>

Protocol number custom value from 0 through 255.

ipv6-icmp

Internet Control Message Protocol

ipv6

Any IP protocol

tcp
Transmission Control Protocol

udp
User Datagram Protocol

any
Specifies all source addresses.

S_IPaddress
Specifies a source address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

prefix_len
Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

host
Specifies a source address.

S_IPaddress
The specific address. For options to abbreviate the address, see the Usage Guidelines.

source-operator
If you specified **tcp** or **udp** *ip-protocol*, the following optional operators are available:

eq
The policy applies to the TCP or UDP port name or number you enter after **eq**.

gt
The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt**.

lt
The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt**.

neq
The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

range
The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53 (two values separated by a space). The first port number in the range must be lower than the last number in the range.

S_port-numbers
(Valid only when *ip-protocol* is UDP or TCP) Specify one or more port numbers.

any
Specifies all destination addresses.

D_IPaddress
Specifies a destination address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

prefix_len
Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

host
Specifies a destination address.

D_IPaddress
The destination address. For options to abbreviate the address, see the Usage Guidelines.

destination-operator
Specifies one of the following destination operators:

eq
The policy applies to the TCP or UDP port name or number you enter after **eq**.

gt
The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt**.

lt
The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt**.

neq
The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

range
The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53. The first port number in the range must be lower than the last number in the range.

D_port_numbers
(Valid only when *ip-protocol* is UDP or TCP) Specify one or more destination port numbers.

dscp
Matches *DSCPvalue* against the DSCP value of the packet.

DSCPvalue
From 0 through 63.

dscp-force
(In **permit** rules, for routed packets) Forces the outgoing DSCP value of packets that match the filter.

drop-precedence-force *dp-value*
(In **permit** rules) Sets the force drop precedence by the specified value.

vlan *vlanID*
Specifies a VLAN interface to which the ACL is bound.

tcp/udp-flags
If you specify **tcp** or **udp** *ip-protocol*, one or more of the following flags are available:

ack
Filters packets for which the **ack** (acknowledge) flag is set.

fin
Filters packets for which the **fin** (finish) flag is set.

rst
Filters packets for which the **rst** (reset) flag is set.

sync
Filters packets for which the **syn** (synchronize) flag is set.

urg
Filters packets for which the **urg** (urgent) flag is set.

push
Filters packets for which the **psh** (push) flag is set.

count
Enables statistics for the rule.

log
Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

mirror
(Supported for rules in ACLs applied on physical interfaces to inbound traffic. Not supported for PBR, rACLs, or ACL-RL.) Mirrors packets matching the rule.

copy-sflow
(Currently not supported) Sends matching inbound packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

An IPv6 ACL can only be applied to incoming traffic.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

You can abbreviate an IPv6 address by using one or more of the following rules:

- Remove one or more leading zeros from one or more groups of hexadecimal digits; this is usually done to either all or none of the leading zeros. (For example, convert the group 0042 to 42.)
- Omit consecutive sections of zeros, using a double colon (::) to denote the omitted sections. The double colon may only be used once in any given address, as the address would be indeterminate if the double colon were used multiple times. A double colon may not be used to denote an omitted single section of zeros. (For example, 2001:db8::1:2 is valid, but 2001:db8::1::2 or 2001:db8::1:1:1:1:1 are not permitted.)

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** followed by the full syntax except for **seq** *seq-value*.

Examples

The following example creates an IPv6 extended ACL, defines a rule for it, and applies the ACL to an interface.

```
device# configure
device(config)# ipv6 access-list extended ip_acl_1
device(conf-ip6acl-ext)# seq 10 deny ipv6 2001:2002:1234:1::/64 2001:1001:1234:1::/64 count
device(conf-ip6acl-ext)# exit
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# ipv6 access-group ip_acl_1 in
```

History

Release version	Command history
18x.1.00	This command was introduced.

seq (rules in IPv6 standard ACLs)

Inserts filtering rules in IPv6 standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *S_IPaddress* } [**count**] [**log**] [**copy-sflow**]

no seq *seq-value*

{ **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *SIP_address* | *SIP_addressmask* } [**count**] [**log**] [**copy-sflow**]

no { **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *SIP_address* | *SIP_addressmask* } [**count**] [**log**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

any

Specifies all source addresses.

S_IPaddress

Specify a source address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

prefix_len

Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

host

Specifies a source address.

SIP_address

The source address. For options to abbreviate the address, see the Usage Guidelines.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

copy-sflow

(Not currently supported) Sends matching inbound packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

An IPv6 ACL can only be applied to incoming traffic.

You can abbreviate an IPv6 address by using one or more of the following rules:

- Remove one or more leading zeros from one or more groups of hexadecimal digits; this is usually done to either all or none of the leading zeros. (For example, convert the group 0042 to 42.)
- Omit consecutive sections of zeros, using a double colon (::) to denote the omitted sections. The double colon may only be used once in any given address, as the address would be indeterminate if the double colon were used multiple times. A double colon may not be used to denote an omitted single section of zeros. (For example, 2001:db8::1:2 is valid, but 2001:db8::1::2 or 2001:db8::1:1:1:1:1 are not permitted.)

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value*.

Examples

The following example shows how to create an IPv6 standard ACL and define rules for it.

```
device# configure terminal
device(config)# ipv6 access-list standard ipv6-std-acl
device(conf-ip6acl-std)# seq 10 permit host 0:1::1
device(conf-ip6acl-std)# seq 20 deny 0:2::/64
device(conf-ip6acl-std)# seq 30 hard-drop any count
```

History

Release version	Command history
18x.1.00	This command was introduced.

seq (rules in MAC extended ACLs)

Inserts filtering rules in Layer 2 (MAC) extended access control lists (ACLs).

Syntax

[**seq** *seq-value*] **permit** { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**vlan** { **any** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-guard**] | **fcoe** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**pcp-force** *out-pcp-value*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

[**seq** *seq-value*] **permit** { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**vlan-tag-format** { **untagged vlan** *vlan-id* | **single-tagged vlan** { **any** | *vlan-id* [*vlan-id-mask*] }] [*custom-EtherType* | **arp** [**arp-guard**] | **fcoe** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**pcp-force** *out-pcp-value*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

[**seq** *seq-value*] { **deny** | **hard-drop** } { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**vlan** { **any** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-guard**] | **fcoe** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

[**seq** *seq-value*] { **deny** | **hard-drop** } { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**vlan-tag-format** { **untagged vlan** *vlan-id* | **single-tagged vlan** { **any** | *vlan-id* [*vlan-id-mask*] }] [*custom-EtherType* | **arp** [**arp-guard**] | **fcoe** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no seq *seq-value*

no permit { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**vlan** { **any** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-guard**] | **fcoe** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**pcp-force** *out-pcp-value*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no permit { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**vlan-tag-format** { **untagged vlan** *vlan-id* | **single-tagged vlan** { **any** | *vlan-id* [*vlan-id-mask*] }] [*custom-EtherType* | **arp** [**arp-guard**] | **fcoe** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**pcp-force** *out-pcp-value*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no { **deny** | **hard-drop** } { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**vlan** { **any** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-guard**] | **fcoe** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no { **deny** | **hard-drop** } { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**vlan-tag-format** { **untagged vlan** *vlan-id* | **single-tagged vlan** { **any** | *vlan-id* [*vlan-id-mask*] }] [*custom-EtherType* | **arp** [**arp-guard**] | **fcoe** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**count**] [**log**] [**mirror**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny
Specifies rules to deny traffic.

hard-drop
Overrides the trap behavior for control frames and data frames such as echo request (ping). However, hard-drop does not override a permit for this address in a preceding rule.

any
Specifies any source MAC addresses.

SMAC-address
Specifies a source MAC address and a comparison mask.

mask
Specifies the mask using Fs and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host *SMAC-address*
Specifies a source MAC address. Use the format HHHH.HHHH.HHHH.

any
Specifies any destination MAC addresses.

DMAC-address
Specifies a destination MAC address and a comparison mask.

mask
Specifies the mask using Fs and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host *DMAC-address*
Specifies a destination MAC address. Use the format HHHH.HHHH.HHHH.

vlan
Specifies VLANs to which the ACL is bound.

any
Specifies any VLAN.

vlanID
Specifies a VLAN.

vlan-tag-format
Specifies **untagged** or **single-tagged** VLAN traffic.

untagged
Specifies traffic with no VLAN tag.

vlan
Specifies a VLAN or any VLAN.

any
Specifies any VLAN.

vlanID
Specifies a VLAN or range of VLANs.

single-tagged
Specifies traffic with a single VLAN, a range of VLANs, or any VLAN.

vlan
Specifies a VLAN or any VLAN.

any
Specifies any VLAN.

vlanID [*vlan-id-mask*]
Specifies a VLAN or range of VLANs. Optionally, you can use a 12-bit hex value to specify a range of VLANs. For example, 0x0FFF specifies all VLANs for which the last 8 bits are 0.

double-tagged
Not supported for the current release.

custom-EtherType
Specifies a custom EtherType value for which to set the permit or deny conditions. Valid values range from 1536 through 65535.

arp
Specifies to permit or deny the ARP protocol (0x0806).

arp-guard
Enables ARP Guard.

fcoe
Specifies to permit or deny the FCOE EtherType (0x8906).

ipv4
Specifies to permit or deny the IPv4 protocol (0x0800).

ipv6
Specifies to permit or deny the IPv6 protocol (0x86dd).

pcp *pcp-match-value*
Filters by PCP priority value. Permitted values are 0 through 7.

pcp-force *out-pcp-value*
(In permit rules applied to incoming traffic) Modifies the PCP priority value to the specified value. Permitted values are 0 through 7.

drop-precedence-force *dp-value*
(In permit rules applied to incoming traffic) Sets the force drop precedence by the specified value. Permitted values are 0 through 2.

count
Enables statistics for the rule.

log
Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

mirror
(Supported for rules in ACLs applied on physical interfaces to inbound traffic) Mirrors packets matching the rule.

copy-sflow
(Currently not supported) (Supported for incoming traffic) Sends matching packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source and destination MAC addresses and protocol type. You can also enable counters, logging, and mirroring.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The following guidelines apply to rules that contain one of the **vlan-tag-format** options:

- Supported only when an ACL containing such rules is applied to physical or port-channel interfaces for ingress traffic. Ignored for ACLs applied to egress traffic and for ACLs applied to VLANs.
- An implicit LACP BPDU **permit** rule precedes the implicit **deny** rule. But to avoid port-channel interface flap for VPLS endpoints over dynamic LAGs, make sure that the LACP BPDUs do not match any of the configured **deny** rules.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value*.

Examples

The following example creates a rule in a MAC extended ACL to deny IPv4 traffic from the source MAC address 0022.3333.4444 to the destination MAC address 0022.3333.5555 and enable packet counting.

```
device# configure terminal
device(config)# mac access-list extended ACL1
device(conf-macl-ext)# seq 100 deny 0022.3333.4444 0022.3333.5555 ipv4 count
```

The following example creates rule in a MAC extended ACL to filter permit traffic by VLAN tag types and enable packet counting.

```
device# configure terminal
device(config)# mac access-list extended ACL1
device(conf-macl-ext)# permit host 0001.0001.0001 any vlan-tag-format untagged vlan 100 count
device(conf-macl-ext)# permit host 0002.0002.0002 any vlan-tag-format single-tagged vlan 200 count
device(conf-macl-ext)# permit host 0001.0001.0004 any vlan-tag-format untagged vlan 100 0x0fff count
```

The following example deletes a rule from a MAC extended ACL.

```
device# configure terminal
device(config)# mac access-list extended ACL1
device(conf-macl-ext)# no seq 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

seq (rules in MAC standard ACLs)

Inserts filtering rules in Layer 2 (MAC) standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**] [**copy-sflow**]

no seq *seq-value*

{ **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**] [**copy-sflow**]

no seq { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

any

Specifies all source MAC addresses.

SMAC_address

Specifies a source MAC address and a comparison mask.

mask

Specify the mask using F's and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host

Specifies a source MAC address.

SMAC_address

Use the format HHHH.HHHH.HHHH.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

copy-sflow
(Currently not supported) Sends matching inbound packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source MAC address. You can also enable counters and logging.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax, without **seq** *seq-value*.

Examples

The following command creates statistic-enabled rules in a MAC standard ACL.

```
device# configure terminal
device(config)# mac access-list standard ACL1
device(conf-macl-std)# seq 100 deny host 0022.3333.4444 count
device(conf-macl-std)# seq 110 permit host 0011.3333.5555 count
```

The following command deletes a rule in a MAC standard ACL, by specifying the **seq** number.

```
device# configure terminal
device(config)# mac access-list standard ACL1
device(conf-macl-std)# no seq 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

service password-encryption

Enables a global password encryption policy that overrides **username** encryption settings.

Syntax

service password-encryption

no service password-encryption

Command Default

Global password encryption policy is enabled.

Modes

Global configuration mode

Usage Guidelines

If global password encryption policy is enabled, it overrides **username** encryption settings.

To disable global password encryption policy, enter the **no** form of this command.

Even if global password encryption policy is disabled, the following **username** syntax does encrypt that user's password: **encryption-level 7**.

Examples

The following example enables global password encryption policy.

```
device# configure terminal
device(config)# service password-encryption
```

The following example disables global password encryption policy.

```
device# configure terminal
device(config)# no service password-encryption
```

History

Release version	Command history
18x.1.00	This command was introduced.

service-policy (interface)

Binds a policy map as a service policy to an interface.

Syntax

service-policy in | **out** *policy-mapname*

no service-policy in | **out**

Command Default

No service policy is created.

Parameters

in
Binds policy map to inbound traffic.

out
Binds policy map to outbound traffic.

policy-mapname
Name of the policy map.

Modes

Interface configuration mode

Usage Guidelines

This command applies a policy-map containing a class-map with specific Policer parameters and match critters to a switch interface. The policy map must be configured before you can apply it (refer to the description of the **policy-map** command).

The **no** form of this command removes the service policy.

Examples

To create a service policy for outbound traffic on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
device(conf-if-eth-2/8)# service-policy out policymap1
```

To remove a service policy for outbound traffic from a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
device(conf-if-eth-2/8)# no service-policy out
```

To remove a service-policy for inbound traffic on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
device(conf-if-eth-2/8)# no service-policy in
```

History

Release version	Command history
18x.1.00	This command was introduced.

set extcommunity

Sets an extended BGP community attribute in a route-map instance.

Syntax

set extcommunity { **rt** *extcommunity value* | **soo** *extcommunity value* }

no set extcommunity

Command Default

No extended BGP community attribute is set.

Parameters

rt

Specifies the route target (RT) extended community attribute.

soo

Specifies the site of origin (SOO) extended community attribute.

extcommunity value

Specifies the value. The value can be one of the following:

ASN:nn—autonomous-system-number:network-number

Autonomous system (AS) number and network number.

IPAddress:nn—ip-address:network-number

IP address and network number.

Modes

Route-map configuration mode.

Usage Guidelines

Enter **no set extcommunity** to delete an extended community set statement from the configuration file.

Examples

The following example sets the route target to extended community attribute 1:1 for routes that are permitted by the route map.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# set extcommunity rt 1:1
```

The following example sets the site of origin to extended community attribute 2:2 for routes that are permitted by the route map.

```
device# configure terminal
device(config)# ip community-list extended 1 permit 123:2
device(config)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# set extcommunity soo 2:2
```

History

Release version	Command history
18x.1.00	This command was introduced.

sflow agent-address

Configures the sFlow agent-ID address.

Syntax

sflow agent-address { **ipv4** | **ipv6** [**ethernet** *slot/plot* | **loopback** *loopback-number* | **management** *slot* | **ve** *ve-inteface*] }

no sflow agent-address

Command Default

By default the sflow agent address is not configured.

Parameters

ipv4
Specifies an agent-address configuration for IPv4 collectors.

ipv6
Specifies an agent-address configuration for IPv6 collectors.

ethernet *slot/plot*
Specifies an Ethernet slot and port..

loopback *loopback-number*
Specifies a loopback interface. Valid values range from 1 through 255.

management *slot*
Specifies a management interface.

ve *ve-inteface*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove the sFlow agent address configuration.

Examples

The following example configures the sFlow agent-address globally. That is, it applies to all IPv4 collectors..

```
device# configure terminal
device(config)# sflow agent-address ipv4 ethernet 2/5
```

History

Release version	Command history
18x.1.00	This command was introduced.

sflow collector

Configures the forwarding of sFLow datagrams to collectors.

Syntax

sflow collector { *IPv4address* | *IPv6address* } [**use-vrf** *vrf-name*]

no sflow collector { *IPv4address* | *IPv6address* } [**use-vrf** *vrf-name*]

Parameters

IPv4address
Specifies an IPv4 address in dotted-decimal format for the collector.

IPv6address
Specifies an IPv6 address for the collector.

use-vrf *vrf-name*
Specifies a VRF through which to connect to the collector. See the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

You can only specify up to five sFlow collectors; this includes all VRFs.

Use the **no** form of this command to reset the specified collector address to a null value.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

To specify the sFlow collectors for an IPv4 address with the default port on the management VRF:

```
device# configure terminal
device(config)# sflow collector 192.10.138.176
```

To specify the sFlow collectors for an IPv4 address with a nondefault port on a user-specified VRF:

```
device# configure terminal
device(config)# sflow collector 192.10.138.176 50 use-vrf myvrf
```

To specify the sFlow collectors for an IPv6 address with a nondefault port on the management VRF:

```
device# configure terminal
device(config)# sflow collector 3ff3:1900:4545:3:200:f8ff:fe21:67cf:6343 50
```

History

Release version	Command history
18x.1.00	This command was introduced.

sflow enable (global version)

Enables sFlow globally.

Syntax

sflow enable

no sflow enable

Command Default

sFlow is disabled on the system.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disable sFlow globally.

Examples

To enable sFlow globally:

```
device# configure terminal
device(config)# sflow enable
```

History

Release version	Command history
18x.1.00	This command was introduced.

sflow polling-interval (global version)

Configures the polling interval globally.

Syntax

sflow polling-interval *interval_value*

no sflow polling-interval

Parameters

interval_value

Specifies a value in seconds to set the polling interval. Valid values range from 1 through 65535 seconds.

Command Default

The default is 20.

Modes

Global configuration mode

Usage Guidelines

The interval is the maximum number of seconds between successive samples of counters to be sent to the collector.

The **no** form of this command restores the default value.

Examples

To set the polling interval to 135 seconds:

```
device# configure terminal
device(config)# sflow polling-interval 135
```

History

Release version	Command history
18x.1.00	This command was introduced.

sflow sample-rate (global version)

Sets the number of packets that are skipped before the next sample is taken.

Syntax

sflow sample-rate *samplerate*

no sflow sample-rate

Command Default

The default is 32768.

Parameters

samplerate

Specifies the sampling rate value in packets. Valid values range from 2 through 16777215 packets.

Modes

Global configuration mode

Usage Guidelines

Sample-rate is the average number of packets skipped before the sample is taken.

The **no** form of this command restores the default sampling rate.

Examples

To change the sampling rate to 4096:

```
device# configure terminal
device(config)# sflow sample-rate 4096
```

History

Release version	Command history
18x.1.00	This command was introduced.

shutdown (link-oam)

Allows you to enable or disable the link-oam protocol.

Syntax

shutdown

no shutdown

Command Default

This command is executed on the local switch.

Modes

Link OAM configuration mode

Usage Guidelines

By default, link oam protocol is enabled when protocol link-oam is configured. Using this command, the protocol can be disabled or enabled.

Examples

```
device(config-link-oam)# shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

shutdown (STP)

Disables Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), Per-VLAN Spanning Tree+ (PVST+), or Rapid PVST+ (R-PVST+) globally.

Syntax

shutdown

no shutdown

Command Default

STP is not enabled as it is not required in a loop-free topology.

Modes

Any of the supported spanning tree configuration modes (STP, RSTP, MSTP, PVST+, R-PVST+)

Usage Guidelines

Enter **no shutdown** to re-enable any of the supported versions of STP.

Examples

To disable RSTP globally:

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# shutdown
```

To enable MSTP globally:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# no shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

shutdown-time

Configures the interval after which an interface that is shut down by loop detection (LD) protocol is automatically reenabled.

Syntax

shutdown-time *minutes*

no shutdown-time

Command Default

See the Usage Guidelines.

Parameters

minutes

The interval in minutes. Range is from 0 through 1440. The default is 0. (The interface is not automatically reenabled.)

Modes

Protocol Loop Detect configuration mode.

Usage Guidelines

Use the **no** form of this command to revert to the default interval and prevent the interface from being automatically reenabled.

Examples

To specify a shutdown time of 20 minutes:

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# shutdown-time 20
```

To revert to the default interval and prevent the interface from being automatically reenabled:

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# no shutdown-time
```

History

Release version	Command history
18x.1.00	This command was introduced.

Show A through Show I

show access-list

For an ACL type and inbound/outbound direction, displays ACL information. You can show information for a specific ACL or only for that ACL on a specific interface. You can also display information for all ACLs bound to an interface.

Syntax

show access-list { **ip** | **ipv6** | **mac** }

show access-list { **ip** | **ipv6** | **mac** } *acl-name* { **in** | **out** }

show access-list interface { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id* | **vlan** *vlan_id* } { **in** | **out** }

show access-list interface management *slot* **/** *port* **in**

show access-list mac *acl-name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan_id* } { **in** | **out** }

show access-list { **ip** | **ipv6** } *acl-name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id* } { **in** | **out** }

show access-list { **ip** | **ipv6** } *acl-name* **interface management** *slot* **/** *port* **in**

show access-list receive { **ip** | **ipv6** }

Parameters

ip
Specifies the IPv4 Layer 3 network protocol.

ipv6
Specifies the IPv6 Layer 3 network protocol.

mac
Specifies the medium access control (MAC) Layer 2 network protocol.

overlay transit
Not supported for this release.

uda
Not supported for this release.

in
Specifies incoming binding direction.

out
Specifies outgoing binding direction.

acl-name
Specifies the ACL name.

interface
Filters by interface.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *index*
Specifies a port-channel interface.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface.

vlan *vlan_id*
Specifies a VLAN interface.

management *slot / port*
Specifies a management interface.

receive
Specifies an ACL that applies to device recieve-path traffic.

Modes

Privileged EXEC mode

Usage Guidelines

You can show information for a specified ACL or only for that ACL on a specified interface. You can also display information for all ACLs bound to a specified physical interface, port-channel, VLAN or VE.

The command also displays information for receive-path ACLs.

Command Output

The **show access-list** command displays the following information:

Output field	Description
Active	The rule is active and implements the configured action.
Partial	The rule is partially programmed, with the configured action implemented in some cases. This is typically seen for logical interfaces like VLAN, which span multiple hardware resources.
In progress	The rule is currently being programmed into the hardware.
Inactive	The rule is inactive and is not programmed in the hardware. This is typically seen when the hardware resources limit is reached.

Examples

The following example displays the names of IPv4 ACLs applied to the device, interfaces to which they are applied, and the incoming/outgoing direction.

```
device# show access-list ip
Interface Ve 171
   Inbound access-list is not set
   Outbound access-list is IPV4_ACL_000 (From User)
Interface Ethernet 0/2
   Inbound switched access-list is IP_ACL_STD_EXAMPLE (From User)
   Outbound access-list is IP_ACL_EXT_EXAMPLE (From User)
```

The following example displays all interfaces on which an IPv4 ACL is applied in the outgoing direction.

```
device# show access-list ip IPV4_ACL_000 out
ip access-list IPV4_ACL_000 on Ve 171 at Egress (From User)
    seq 10 deny ip host 0.0.0.0 host 10.0.0.0 (Active)
```

The following example displays all interfaces on which an IPv6 ACL is applied in the incoming direction.

```
device# show access-list ipv6 distList in
ipv6 access-list distList on Ethernet 0/4 at Ingress (From User)
    seq 10 deny 2001:125:132:35::/64 (Active)
    seq 20 deny 2001:54:131::/64 (Active)
    seq 30 deny 2001:5409:2004::/64 (Active)
    seq 40 permit any (Active)
```

The following example displays all ACLs applied on a specified interface in the incoming direction.

```
device# show access-list interface ethernet 0/4 in
ipv6 access-list ipv6-std-acl on Ethernet 0/4 at Ingress (From User)
    seq 10 permit host 0:1::1 (Active)
    seq 20 deny 0:2::/64 (Active)
    seq 30 hard-drop any count (Active)
```

The following example displays IPv6 receive-path ACL information.

```
device# show access-list receive ipv6
ipv4 access-list extended ipv6-receive-acl-example
seq 76 deny ip 10.10.95.10 0.0.0.0 any count (Active)

ipv6 access-list extended ipv6-receive-acl-example
seq 10 deny ipv6 3001:2010:145:35::/64 any count (Active)
```

History

Release version	Command history
18x.1.00	This command was introduced.

show access-list-log buffer

Displays the contents of the log buffer for all ACLs, or for a specified interface.

Syntax

show access-list-log buffer [**interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* }]

Parameters

interface
Filters by interface.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

port-channel *index*
Specifies a port-channel interface.

Modes

Privileged EXEC mode

Command Output

The **show access-list log buffer** command displays the following information:

Output field	Description
Frames Logged on interface	Accumulated number of packets matching ACL rules applied to the interface
Ethernet Src, Dst; Internet proto, Src, Dst	Information for matched buffered packets for the specified source and destination addresses

Examples

Sample terminal output:

```
device# show access-list-log buffer
Frames Logged on interface 0/2 :
--------------------------------
Frame Received Time : Fri Dec 9 3:8:48 2011
Ethernet,       Src : (00:34:56:78:0a:ab), Dst: (00:12:ab:54:67:da)
  Ethtype           : 0x8100
  Vlan tag type     : 0x800
  VlanID            : 0x1
Internet proto, Src : 192.85.1.2, Dst: 192.0.0.1
  Interface         :
  Type of service   : 0
  Length            : 110
  Identification    : 0
  Fragmentation     : 00 00
  TTL               : 255
  protocol          : 253
  Checksum          : 39 3a
  Payload type      :
packet(s) repeated  : 30
Ingress Deny Logged
-------------------------------------------------------------------------
```

History

Release version	Command history
18x.1.00	This command was introduced.

show access-list-log buffer config

Displays the configuration of the ACL buffer.

Syntax

show access-list-log buffer config

Modes

Privileged EXEC mode

Command Output

The **show access-list log buffer config** command displays the following information:

Output field	Description
ACL Logging is	Displays "enabled" or "disabled".
Buffer exists	Displays interfaces buffered.
Buffer type is	Displays "circular" or "linear".

Examples

The following example displays the configuration of the ACL buffer.

```
device# show access-list-log buffer config
ACL Logging is enabled
Buffer exists for interface Eth 0/11
Buffer type is Circular and size is 512
```

History

Release version	Command history
18x.1.00	This command was introduced.

show arp

Displays the Address Resolution Protocol (ARP) entries.

Syntax

show arp { **ethernet** *slot* **/** *port* | **ve** *ve_id* } [**vrf** *name*]

show arp ip *ip-address* [**vrf** *name*]

show arp [**dynamic** | **static**] [**summary**] [**vrf** *name*]

Parameters

vrf *name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

ve *ve_id*
Specifies a virtual Ethernet (VE) interface.

ip *ip-address*
Specifies a next-hop IP address.

dynamic
Displays all the dynamic ARP entries in the ARP table.

static
Displays all the static ARP entries in the ARP table.

summary
Displays a summary of the ARP table.

Modes

Privileged EXEC mode

Command Output

The **show arp** command displays the following information:

Output field	Description
Address	Displays the IP address.
Mac-address	Displays the MAC address or "UnResolved".
L3 Interface	Displays the VE interface.

Output field	Description
L2 Interface	Displays the Layer 2 interface.
Age	In hh:mm:ss format, displays the time since the most recent renewal of a dynamic entry. For a static entry, displays "Never".
Type	Displays "Dynamic", "Static", "Bgp-Evpn", or "PreArp". ("PreArp" is ARP triggered other than by the data traffic, for example, by the static route.)

Examples

The following example displays the output of the basic **show arp** command.

```
device# show arp
Total Entries in VRF default-vrf : 606
Address    Mac-address     L3 Interface  L2 Interface  Age    Type
-------------------------------------------------------------------
10.17.0.1  0010.1768.f101  Ve 1017       Po 58.1017    Never  Bgp-Evpn
```

History

Release version	Command history
18x.1.00	This command was introduced.

show arp access-list

Displays one or all Address Resolution Protocol (ARP) access control lists (ACLs) available on a device, including permit statements.

Syntax

show arp access-list [*acl-name*]

Parameters

acl-name

Specifies the name of an ARP ACL defined on the device.

Modes

Privileged EXEC mode

Examples

The following example displays the name and permit statements of an ARP ACL named "list1".

```
device# show arp access-list list1
ARP access list list1
     permit ip host 192.85.1.2 mac host 0010.9400.0002
     permit ip host 192.85.1.3 mac host 0010.9400.0003
     permit ip host 196.2.1.2 mac host 0020.3200.0008
```

The following example displays the name and permit statements of all ARP ACLs.

```
device# show arp access-list
ARP access list list1
     permit ip host 192.85.1.2 mac host 0010.9400.0002
     permit ip host 192.85.1.3 mac host 0010.9400.0003
     permit ip host 196.2.1.2 mac host 0020.3200.0008
ARP access list list2
     permit ip host 20.20.20.1 mac host 0011.9400.0001
     permit ip host 30.30.30.1 mac host 0011.9400.0002
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn l2route

Displays BGP EVPN Layer 2 route information in the MAC VRF table.

Syntax

show bgp evpn l2route [**type** { **inclusive-multicast** | **mac** } [**detail**]]

Modes

Privileged EXEC mode

Examples

The following example shows routes in the VPN table.

```
device# show bgp evpn l2route
Total number of BGP EVPN Routes : 5
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
Route Distinguisher: 3.3.100.3:1
*>  IMR:[50][IPv4:3.3.100.3]
                       0.0.0.0         0          100        0      ?
*>i IMR:[50][IPv4:4.4.100.4]
                       4.4.100.4       0          100        0      ?
*>i IMR:[50][IPv4:5.5.100.5]
                       5.5.100.5       0          100        0      ?
*>  MAC:[50][0000.0300.0050]
                       0.0.0.0         0          100        0      ?
*>i MAC:[50][0000.0400.0050]
                       4.4.100.4       0          100        0      ?
```

The following example displays details for inclusive-multicast routes. In this example, the EVPN instance is configured with route-targets configured automatically.

```
device# show bgp evpn l2route type inclusive-multicast detail
Total number of BGP EVPN IMR Routes : 3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 3.3.100.3:1
1       Prefix: IMR:[50][IPv4:3.3.100.3],  Status: BL,  Age: 0h8m46s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type: 0x00000006 Tunnel-
IP: 3.3.100.3
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
2       Prefix: IMR:[50][IPv4:4.4.100.4],  Status: BI,  Age: 0h2m43s
         NEXT_HOP: 4.4.100.4, Learned from Peer: 4.4.100.4 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 25600:838860816 RT 100:50
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type: 0x00000006 Tunnel-
IP: 4.4.100.4
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
3       Prefix: IMR:[50][IPv4:5.5.100.5],  Status: BI,  Age: 0h2m37s
         NEXT_HOP: 5.5.100.5, Learned from Peer: 5.5.100.5 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 25600:838860816 RT 100:50
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type: 0x00000006 Tunnel-
IP: 5.5.100.5
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
```

The following example displays details for inclusive-multicast routes. In this example, the EVPN instance is configured with route-targets configured explicitly.

```
device# show bgp evpn l2route type inclusive-multicast detail
Total number of BGP EVPN IMR Routes : 2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 3.3.100.3:1
1       Prefix: IMR:[50][IPv4:3.3.100.3],  Status: BL,  Age: 0h4m17s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type: 0x00000006 Tunnel-
IP: 3.3.100.3
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
2       Prefix: IMR:[50][IPv4:4.4.100.4],  Status: BI,  Age: 0h3m31s
         NEXT_HOP: 4.4.100.4, Learned from Peer: 4.4.100.4 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 50:1
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type: 0x00000006 Tunnel-
IP: 4.4.100.4
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
```

The following example displays details for MAC routes. **BI** indicates that the route is "Best" and "Installed." This ensures that it is downloaded into the system.

```
device# show bgp evpn l2route type mac detail
Total number of BGP EVPN MAC Routes : 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 01:00:04:03:02:01:01:00
1       Prefix: MAC:[100][1111.2222.3333],  Status: BI,  Age: 0h6m17s
         NEXT_HOP: 10.20.30.40, Learned from Peer: 10.0.0.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:08:00 RT 25600:1677721600
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 100
            ESI : 00.00000000000000000
            RD: 01:00:04:03:02:01:01:00
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn l3vni

Displays BGP EVPN information for Layer 3 virtual network identifiers (VNIs).

Syntax

show bgp evpn l3 vni { **all-vrfs** | **vrf** *name* }

Parameters

all-vrfs

Specifies all VRFs.

vrf *name*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows Layer 3 VNI information for all VRFs.

```
device# show bgp evpn l3vni all-vrfs

------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (2)
------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3 VNI  Link UP          : True
Source VTEP              : 0x06000006
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (2)
------------------------------------------------------------------------
Address Family under BGP : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (3)
------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3 VNI  Link UP          : True
Source VTEP              : 0x06000006
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (3)
------------------------------------------------------------------------
Address Family under BGP : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (4)
------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3 VNI  Link UP          : True
Source VTEP              : 0x06000006
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (4)
------------------------------------------------------------------------
Address Family under BGP : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
```

```
Router mac Exists        : True
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (5)
------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3 VNI  Link UP          : True
Source VTEP              : 0x06000006
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (5)
------------------------------------------------------------------------
Address Family under BGP : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3VNI Active             : Active
```

The following example shows Layer 3 VNI information for a specified VRF.

```
device# show bgp evpn l3vni vrf red

------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (red)
------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
IRB I/F Configured        : True (0x48000064)
IRB I/F Status            : False
IRB EVID Conigured        : True (100)
Router mac Exists        : True
Source VTEP              : 40.40.40.1
VTEP Active              : Active
IPv4 L3VNI Active             : Active
IPv6 L3VNI Active             : Inactive


------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (red)
------------------------------------------------------------------------
Address Family under BGP : True
IRB I/F Configured       : True (0x48000064)
IRB EVID Configured      : True (100)
Router mac Exists        : True
IPv4 L3VNI Active             : Active
IPv6 L3VNI Active             : Inactive
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn neighbors

Displays configuration information for BGP EVPN neighbors of the device.

Syntax

show bgp evpn neighbors [*ip-addr* | *ipv6-addr* | **routes-summary**]

Parameters

ip-addr
Specifies the IPv4 address of a neighbor.

ipv6-addr
Specifies the IPv6 address of a neighbor.

routes-summary
Displays routes received, routes accepted, number of routes advertised by peer, and so on.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP EVPN neighbors of the device. Output shows all configured parameters for the neighbors.

Examples

The following example shows sample output from the show bgp evpn neighbors command.

```
device# show bgp evpn neighbors
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn neighbors advertised-routes

Displays information about the routes that the device has advertised to the specified neighbor during the current BGP EVPN session.

Syntax

show bgp evpn neighbors { *ip address* | *ipv6 address* } **advertised-routes** [**detail** [*type*] | *type*]

Parameters

ip-addr
Specifies the IPv4 address of a neighbor.

ipv6-addr
Specifies the IPv6 address of a neighbor.

detail *type*
Specifies detailed information be given for the designated route type.

type
Specifies the type of route.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segment (ES) routes.

inclusive-multicast
Specifies inclusive multicast routes.

ipv4-prefix
Specifies IPv4 prefix routes.

ipv6-prefix
Specifies IPv6 prefix routes.

mac
Specifies MAC routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn neighbors advertised-routes detail** command.

```
device# show bgp evpn neighbors 2.0.0.2 advertised-routes detail

       There are 5812 routes advertised to neighbor 2.0.0.2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
1       Prefix: ARP:[0][0000.abba.baba]:[IPv4:2.29.1.254],  Status: BE,  Age: 1d6h1m40s
         NEXT_HOP: 19.0.0.19, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            Extended Community: ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT
65003:29 RT 2:2 RT 65003:20 ExtCom:06:03:50:eb:1a:13:17:9a
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 29 L3_vni: 20 Router Mac : 50:eb:1a:13:17:9a
            ESI : 00.0000000000000000000
2       Prefix: ND:[0][0000.abba.abba]:[IPv6:2:29:1::254],  Status: BE,  Age: 1d6h1m40s
         NEXT_HOP: 19.0.0.19, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            Extended Community: ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT
65003:29 RT 2:2 RT 65003:20 ExtCom:06:03:50:eb:1a:13:17:9a
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 29 L3_vni: 20 Router Mac : 50:eb:1a:13:17:9a
            ESI : 00.0000000000000000000
3       Prefix: MAC:[0][50eb.1a13.8074],  Status: BE,  Age: 1d6h1m35s
         NEXT_HOP: 76.0.0.76, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65003:136
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 136
            ESI : 00.0000000000000000000
4       Prefix: MAC:[0][0000.abba.baba],  Status: BE,  Age: 1d6h1m35s
         NEXT_HOP: 76.0.0.76, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65003:136
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 136
            ESI : 00.0000000000000000000
5       Prefix: MAC:[0][0000.abba.abba],  Status: BE,  Age: 1d6h1m35s
         NEXT_HOP: 76.0.0.76, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65003:136
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 136
            ESI : 00.0000000000000000000
…
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn neighbors routes

Displays routes of specified types received from designated BGP EVPN neighbors, for example, best BGP EVPN routes to their destination.

Syntax

show bgp evpn neighbors { *ip address* | *ipv6 address* } **routes** [*type*] | **best** [*type*] | **detail** [*type*] | **not-installed-best** [*type*] | **unreachable** [*type*]]

Parameters

type
Specifies the type of route.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segments (ES) routes.

inclusive-multicast
Specifies inclusive multicast routes.

mac
Specifies MAC routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn neighbors routes best** command.

```
device# show bgp evpn neighbors 2.0.0.2 routes best

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      IMR:[0][IPv4:57.0.0.57]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
         L2_vni: 22
2      ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
3      ND:[0][0000.abba.abba]:[IPv6:2:22:1::254]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
4      ND:[0][0027.f8ca.76ba]:[IPv6:fe80::227:f8ff:feca:76ba]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
5      MAC:[0][0000.abba.abba]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
         L2_vni: 22
         ESI : 00.000000000000000000
…
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes

Displays EVPN routes in the VPN table. Routes are imported into the MAC VRF table if those routes are imported.

Syntax

show bgp evpn routes

Modes

Privileged EXEC mode

Examples

The following example shows routes in the VPN table.

```
device# show bgp evpn routes
Total number of BGP EVPN Routes : 5
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
Route Distinguisher: 3.3.100.3:32818
*>  IMR:[0][IPv4:3.3.100.3]
                         3.3.100.3       0          100        0      ?
*>  MAC:[0][0000.0300.0050]
                         3.3.100.3       0          100        0      ?
Route Distinguisher: 4.4.100.4:32818
*>i IMR:[0][IPv4:4.4.100.4]
                         4.4.100.4       0          100        0      ?
*>i MAC:[0][0000.0400.0050]
                         4.4.100.4       0          100        0      ?
Route Distinguisher: 5.5.100.5:32818
*>i IMR:[0][IPv4:5.5.100.5]
                         5.5.100.5       0          100        0      ?
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes best

Displays information for BGP EVPN routes that were selected as best routes.

Syntax

show bgp evpn routes best

show bgp evpn routes best [**type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** }]

Parameters

type
Specifies the type of route.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segments (ES) routes.

inclusive-multicast
Specifies inclusive multicast routes.

ipv4-prefix
Specifies IPv4 prefix routes.

ipv6-prefix
Specifies IPv6 prefix routes.

mac
Specifies MAC routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes best** command.

```
device# show bgp evpn routes best

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      IMR:[0][IPv4:57.0.0.57]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
         L2_vni: 22
2      ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
3      ND:[0][0000.abba.abba]:[IPv6:2:22:1::254]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
4      ND:[0][0027.f8ca.76ba]:[IPv6:fe80::227:f8ff:feca:76ba]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
5      MAC:[0][0000.abba.abba]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
         L2_vni: 22
         ESI : 00.000000000000000000
6      MAC:[0][0000.abba.baba]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
         L2_vni: 22
         ESI : 00.000000000000000000
…
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes detail

Displays detailed BGP EVPN route information.

Syntax

show bgp evpn routes detail

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes detail** command.

```
device# show bgp evpn routes detail
Total number of BGP EVPN Routes : 12136
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 6.0.0.6:32790
1       Prefix: IMR:[0][IPv4:57.0.0.57],  Status: BE,  Age: 1d9h20m9s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 2.0.0.2 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 65006:22
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000016 Tunnel-Type: 0x00000006 Tunnel-
IP: 57.0.0.57
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 22
2       Prefix: IMR:[0][IPv4:57.0.0.57],  Status: E,  Age: 1d9h20m9s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 3.0.0.3 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 65006:22
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000016 Tunnel-Type: 0x00000006 Tunnel-
IP: 57.0.0.57
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 22
3       Prefix: ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254],  Status: BE,  Age: 1d9h19m42s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 2.0.0.2 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT
65006:22
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 22 L3_vni: 0
            ESI : 00.0000000000000000000
4       Prefix: ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254],  Status: E,  Age: 1d9h19m42s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 3.0.0.3 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT
65006:22
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 22 L3_vni: 0
            ESI : 00.0000000000000000000
5       Prefix: ND:[0][0000.abba.abba]:[IPv6:2:22:1::254],  Status: BE,  Age: 1d9h19m42s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 2.0.0.2 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT
65006:22
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 22 L3_vni: 0
            ESI : 00.0000000000000000000
…
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes local

Displays information about BGP EVPN local routes.

Syntax

show bgp evpn routes local

show bgp evpn routes local type [**auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac**]

Parameters

type
Specifies the type of route.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segments (ES) routes.

inclusive-multicast
Specifies inclusive multicast routes.

ipv4-prefix
Specifies IPv4 prefix routes.

ipv6-prefix
Specifies IPv6 prefix routes.

mac
Specifies MAC routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes local** command.

```
device# show bgp evpn routes local

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: AD:[00.000000000000989900][4294967295],  Status: BL,  Age:
1d23h
50m9s
         NEXT_HOP: 78.0.0.78, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:06:01:00:00:00:00:00:00 ExtCom:03:0c:
00:0
0:00:00:00:08
            ESI Label Ext Community: 0     All-Active
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 0
2       Prefix: ESR:[00.000000.000000.989900][IPv4:7.0.0.7],  Status: BL,
Age:
1d23h50m9s
         NEXT_HOP: 78.0.0.78, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:06:02:00:00:00:98:99:00 ExtCom:03:0c:
00:0
0:00:00:00:08
        RT Import 0:10000640
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 0
3       Prefix: IP4Prefix:[0][21.1.1.0/24],  Status: BL,  Age: 1d23h36m46s
         NEXT_HOP: 78.0.0.78, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 1:1 ExtCom:06:03:50:eb:1a:14:07:67 ExtCom:
03:                                                                          0c:
00:00:00:00:00:08
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 0
            L3_vni: 10020 Router Mac : 50:eb:1a:14:07:67
4       Prefix: IP4Prefix:[0][22.1.1.0/24],  Status: BL,  Age: 1d23h36m46s
         NEXT_HOP: 78.0.0.78, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 1:1 ExtCom:06:03:50:eb:1a:14:07:67 ExtCom:
03:                                                                          0c:
00:00:00:00:00:08
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 0
            L3_vni: 10020 Router Mac : 50:eb:1a:14:07:67
…
```

This example shows output for the **show bgp evpn routes local** command when the **type** and **mac** keywords are used.

```
device# show bgp evpn routes local type mac

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: MAC:[0][0000.abba.abba],  Status: BL,  Age: 1d9h36m12s
         NEXT_HOP: 109.0.0.109, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65009:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 3,  Admin distance 0
            L2_vni: 22
            ESI : 00.000000000000000000
2       Prefix: MAC:[0][0000.abba.baba],  Status: BL,  Age: 1d9h36m12s
         NEXT_HOP: 109.0.0.109, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65009:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 3,  Admin distance 0
            L2_vni: 22
            ESI : 00.000000000000000000
3       Prefix: MAC:[0][0027.f8fd.274b],  Status: BL,  Age: 1d9h36m32s
         NEXT_HOP: 109.0.0.109, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65009:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 3,  Admin distance 0
            L2_vni: 22
            ESI : 00.000000000000000000
   …
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes next-hop

Displays information for BGP EVPN routes received from the specified next-hop.

Syntax

show bgp evpn routes next-hop { *ipv4-address* | *ipv6-address* } **type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** }

Parameters

ipv4-address
Specifies an IPv4 address.

ipv6-address
Specifies an IPv6 address.

type
Specifies the type of route.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segments (ES) routes.

inclusive-multicast
Specifies inclusive multicast routes.

ipv4-prefix
Specifies IPv4 prefix routes.

ipv6-prefix
Specifies IPv6 prefix routes.

mac
Specifies MAC routes.

Modes

Privileged EXEC mode

Examples

```
device# show bgp evpn routes next-hop 57.0.0.57 type mac
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes no-best

Displays information for BGP EVPN routes that were selected as not best routes.

Syntax

show bgp evpn routes no-best

show bgp evpn routes no-best [**type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** }]

Parameters

type
Specifies the type of route.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segments (ES) routes.

inclusive-multicast
Specifies inclusive multicast routes.

ipv4-prefix
Specifies IPv4 prefix routes.

ipv6-prefix
Specifies IPv6 prefix routes.

mac
Specifies MAC routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes no-best** command.

```
device# show bgp evpn routes no-best

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      IMR:[0][IPv4:57.0.0.57]
                           57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
         L2_vni: 22
2      ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254]
                           57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
3      ND:[0][0000.abba.abba]:[IPv6:2:22:1::254]
                           57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
4      ND:[0][0027.f8ca.76ba]:[IPv6:fe80::227:f8ff:feca:76ba]
                           57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
5      MAC:[0][0000.abba.abba]
                           57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
         L2_vni: 22
         ESI : 00.000000000000000000
6      MAC:[0][0000.abba.baba]
                           57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
         L2_vni: 22
         ESI : 00.000000000000000000
…
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes not-installed-best

Displays information for BGP EVPN best routes that are not installed.

Syntax

show bgp evpn routes not-installed-best

show bgp evpn routes not-installed-best [**type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** }]

Parameters

type
Specifies the type of route.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segments (ES) routes.

inclusive-multicast
Specifies inclusive multicast routes.

ipv4-prefix
Specifies IPv4 prefix routes.

ipv6-prefix
Specifies IPv6 prefix routes.

mac
Specifies MAC routes.

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes rd

Displays information for BGP EVPN routes with the specified route distinguisher (RD).

Syntax

show bgp evpn routes rd *ID*

Parameters

ID

Identifying number assigned to the route.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes rd** command.

```
device# show bgp evpn routes rd 6.0.0.6:32790

Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
*>  IMR:[0][IPv4:57.0.0.57]
                       57.0.0.57                  100        0      65002 65006 ?
*   IMR:[0][IPv4:57.0.0.57]
                       57.0.0.57                  100        0      65002 65006 ?
*>  ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254]
                       57.0.0.57                  100        0      65002 65006 ?
*   ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254]
                       57.0.0.57                  100        0      65002 65006 ?
*>  ND:[0][0000.abba.abba]:[IPv6:2:22:1::254]
                       57.0.0.57                  100        0      65002 65006 ?
*   ND:[0][0000.abba.abba]:[IPv6:2:22:1::254]
                       57.0.0.57                  100        0      65002 65006 ?
*>  ND:[0][0027.f8ca.76ba]:[IPv6:fe80::227:f8ff:feca:76ba]
                       57.0.0.57                  100        0      65002 65006 ?
*   ND:[0][0027.f8ca.76ba]:[IPv6:fe80::227:f8ff:feca:76ba]
                       57.0.0.57                  100        0      65002 65006 ?
*>  MAC:[0][0000.abba.abba]
                       57.0.0.57                  100        0      65002 65006 ?
*   MAC:[0][0000.abba.abba]
                       57.0.0.57                  100        0      65002 65006 ?
*>  MAC:[0][0000.abba.baba]
                       57.0.0.57                  100        0      65002 65006 ?
*   MAC:[0][0000.abba.baba]
                       57.0.0.57                  100        0      65002 65006 ?
*>  MAC:[0][0027.f8ca.76ba]
                       57.0.0.57                  100        0      65002 65006 ?
*   MAC:[0][0027.f8ca.76ba]
                       57.0.0.57                  100        0      65002 65006 ?
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes rd type

Displays information for BGP EVPN routes, filtered based on a specified route type, with the specified route distinguisher (RD).

Syntax

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** } **detail**

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type auto-discovery esi-value** *value* **ethernet-tag** *tag-id*

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type ethernet-segment esi-value** *value* { **ipv4-address** *address* | **ipv6-address** *address* }

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type inclusive-multicast ethernet-tag** *tag-id* **ipv4-address** *address* [**l2-vni** *number*

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type ipv4-prefix** *ip address/mask* **tag** *tag-id* [**l3vni** *value*]

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type ipv6-prefix** *ipv6 address/mask* **tag** *tag-id* [**l3vni** *value*]

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type mac** *mac address***ethernet-tag** *tag-id* [**l2-vni** *number*]

Parameters

admin-value

The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2-byte number (from 0 through 65535) or a 4-byte number (from 0 through 4294967295).

arbitrary-value

An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is 2 byte, or from 0 through 4294967295 if the ASN is 4 byte.

type

Specifies a route type.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segment (ES) information.

inclusive-multicast

Specifies inclusive multicast information.

ipv4-prefix

Specifies IPv4 prefix information information.

ipv6-prefix

Specifies IPv6 prefix information information.

mac

Specifies Media Access Control (MAC) information.

detail

Displays detailed information.

mac *mac address*
Specifies a MAC address. The valid format is HHHH.HHHH.HHHH.

ethernet-tag *tag-id*
Specifies an Ethenet tag. Valid values range from 1 through 4294967295.

l2-vni *number*
Specifies a layer 2 virtual network identifier (VNI). Valid values range from 1 through 16777215.

esi-value *value*
Specifies a 10 byte Ethernet Segment Identifier (ESI) value in the form of hexadecimal characters (HH.HH.HH.HH.HH.HH.HH.HH.HH.HH).

ipv4-address *address*
Specifies an IPv4 address.

ipv6-address *address*
Specifies an IPv6 address.

ip address/mask
Specifies an IPv4 address and mask.

ipv6 address/mask
Specifies an IPv6 address and mask.

tag *tag-id*
Specifies an Ethenet tag. Valid values range from 1 through 4294967295.

l3vni *value*
Specifies a Layer 3 virtual network identifier (VNIs). Valid values range from 1 through 6777215.

Modes

Privileged EXEC mode

Examples

The following example shows detailed MAC information for a BGP EVPN route with the RD 6.0.0.6:32790.

```
device# show bgp evpn routes rd 6.0.0.6:32790 type mac detail

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: MAC:[0][0000.abba.abba],  Status: BE,  Age: 1d7h26m34s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 2.0.0.2 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65006:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 22
            ESI : 00.000000000000000000
2       Prefix: MAC:[0][0000.abba.abba],  Status: E,  Age: 1d7h26m34s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 3.0.0.3 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65006:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 22
            ESI : 00.000000000000000000
3       Prefix: MAC:[0][0000.abba.baba],  Status: BE,  Age: 1d7h26m34s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 2.0.0.2 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65006:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 22
            ESI : 00.000000000000000000
4       Prefix: MAC:[0][0000.abba.baba],  Status: E,  Age: 1d7h26m34s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 3.0.0.3 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65006:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 22
            ESI : 00.000000000000000000
5       Prefix: MAC:[0][0027.f8ca.76ba],  Status: BE,  Age: 1d7h27m2s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 2.0.0.2 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:06:00:01:00:00:00:00:00 ExtCom:03:0d:00:00:00:00:00:00 ExtCom:
03:0c:00:00:00:00:00:08 RT 65006:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 22
            ESI : 00.000000000000000000
…
```

The following example shows detailed inclusive multicast information for a BGP EVPN route with the RD 6.0.0.6:32790.

```
device# show bgp evpn routes rd 6.0.0.6:32790 type inclusive-multicast detail

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: IMR:[0][IPv4:57.0.0.57],  Status: BE,  Age: 1d7h34m37s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 2.0.0.2 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 65006:22
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000016 Tunnel-Type: 0x00000006 Tunnel-
IP: 57.0.0.57
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 22
2       Prefix: IMR:[0][IPv4:57.0.0.57],  Status: E,  Age: 1d7h34m37s
         NEXT_HOP: 57.0.0.57, Learned from Peer: 3.0.0.3 (65002)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65002 65006
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 65006:22
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000016 Tunnel-Type: 0x00000006 Tunnel-
IP: 57.0.0.57
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 22
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes type

Displays EVPN routes in the VPN table by type. Routes are imported into the MAC VRF table if those routes are imported.

Syntax

show bgp evpn routes type arp [*IPv4_address* | **mac** *MAC_address* | **brief** | **detail**]

show bgp evpn routes type auto-discovery [**brief** | **detail** | **esi-value**]

show bgp evpn routes type ethernet-segment [**brief** | **detail** | **esi-value** *ESI*]

show bgp evpn routes type inclusive-multicast [**brief** | **detail** | **ethernet-tag**]

show bgp evpn routes type ipv4-prefix [*IPv4_address/mask* | **brief** | **detail** | **l3-label**]

show bgp evpn routes type ipv6-prefix [*IPv6_address/mask* | **brief** | **detail** | **l3-label**]

show bgp evpn routes type mac [*MAC_address* | **brief** | **detail**]

show bgp evpn routes type nd [*IPv6_address* | **brief** | **detail**]

Parameters

arp
Specifies ARP details.

IPv4_address
Specifies an IPv4 address in A.B.C.D format.

mac *MAC_address*
Specifies a MAC address in HHHH.HHHH.HHHH format.

brief
Specifies brief information.

detail
Specifies detailed information.

auto-discovery
Specifies auto-discovery details.

esi-value *ESI*
Specifies an Ethernet Segment Indicator in the following hexadecimal format:
HH:HH:HH:HH:HH:HH:HH:HH:HH , HH.

ethernet-segment
Specifies Ethernet Segment details.

inclusive-multicast
Specifies inclusive multicast details.

ethernet-tag *tag*
Specifies an Ethernet tag ID. Range is from 0 through 4294967295.

ipv4-prefix *IPv4_address/mask*
Specifies an IPv4 prefix and mask length in A.B.C.D/L format.

l3-label *number*
Specifies a Layer 3 Virtual Network Identifier (VNI). Range is from 1 through 16777215.

ipv6-prefix *IPv6_address/mask*
Specifies an IPv6 prefix and mask length in A:B::C:D/L format.

l3-label *number*
Specifies a Layer 3 Virtual Network Identifier (VNI). Range is from 1 through 16777215.

mac *MAC_address*
Specifies a MAC address in HHHH.HHHH.HHHH format.

nd *IPv6_address*
Specifies a BGP Neighbor Discovery IPv6 address in A:B::C:D format.

Modes

Privileged EXEC mode

Examples

The following example displays information related to ARP routes.

```
device# show bgp evpn route type arp
Total number of BGP EVPN ARP Routes : 4 Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP
D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
Route Distinguisher: 40.40.100.50:32869
1      ARP:[0][0000.0a0a.0a0b]:[IPv4:10.10.10.11]
                          0.0.0.0         0          100        0      BL
         AS_PATH:
            L2 Label: 101 L3 Label: 100
         ESI : 00.000000000000000000
2      ARP:[0][609c.9f5a.4715]:[IPv4:15.143.15.1]
                          0.0.0.0         0          100        0      BL
         AS_PATH:
            L2 Label: 101 L3 Label: 100
         ESI : 00.000000000000000000
Route Distinguisher: 40.40.100.50:33769
3      ARP:[0][609c.9f5a.4715]:[IPv4:14.13.15.1]
                          0.0.0.0         0          100        0      BL
         AS_PATH:
            L2 Label: 1001 L3 Label: 100
         ESI : 00.000000000000000000
Route Distinguisher: 40.40.100.60:32869
4      ARP:[0][609c.9f5a.8d15]:[IPv4:6.6.2.5]
                          40.40.40.2      0          100        0      BE
         AS_PATH: 1000
            L2 Label: 101 L3 Label: 0
         ESI : 00.000000000000000000
```

The following example displays brief information related to IPv4 prefix routes.

```
device# show bgp evpn route type ipv4-prefix brief
Total number of BGP EVPN Ipv4Prefix Routes : 4 Status codes: s suppressed, d damped, h history, *
valid, > best, i internal, S stale Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
Route Distinguisher: 5:50
*>  IP4Prefix:[0][14.13.15.0/24]
                       0.0.0.0         0          100        0      ?
*>  IP4Prefix:[0][15.143.15.0/24]
                       0.0.0.0         0          100        0      ?
*>  IP4Prefix:[0][16.16.16.0/24]
                       0.0.0.0         0          100        0      ?
Route Distinguisher: 5:100
*>  IP4Prefix:[0][17.17.17.0/24]
                       40.40.40.2      0          100        0      1000 ?
```

The following example displays information for inclusive multicast routes.

```
device# show bgp evpn routes type inclusive-multicast
Total number of BGP EVPN IMR Routes : 9
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
Route Distinguisher: 23.23.23.23:32868
1      IMR:[0][IPv4:23.23.23.23]
                          0.0.0.0         0          100        0      BL
         AS_PATH:
         L2 Label: 100 (EVI)
Route Distinguisher: 23.23.23.23:32969
2      IMR:[0][IPv4:23.23.23.23]
                          0.0.0.0         0          100        0      BL
         AS_PATH:
         L2 Label: 201 (EVI)
Route Distinguisher: 23.23.23.23:32970
3      IMR:[0][IPv4:23.23.23.23]
                          0.0.0.0         0          100        0      BL
         AS_PATH:
         L2 Label: 202 (EVI)
Route Distinguisher: 24.24.24.24:32868
4      IMR:[0][IPv4:11.11.11.11]
                          11.11.11.11      none      100        0      BE
         AS_PATH: 20 11
         L2 Label: 100 (VNI)
5      IMR:[0][IPv4:11.11.11.11]
                          11.11.11.11      none      100        0      E
         AS_PATH: 21 11
         L2 Label: 100 (VNI)
Route Distinguisher: 24.24.24.24:32969
6      IMR:[0][IPv4:11.11.11.11]
                          11.11.11.11      none      100        0      BE
         AS_PATH: 20 11
         L2 Label: 201 (VNI)
7      IMR:[0][IPv4:11.11.11.11]
                          11.11.11.11      none      100        0      E
         AS_PATH: 21 11
         L2 Label: 201 (VNI)
Route Distinguisher: 24.24.24.24:32970
8      IMR:[0][IPv4:11.11.11.11]
                          11.11.11.11      none      100        0      BE
         AS_PATH: 20 11
         L2 Label: 202 (VNI)
9      IMR:[0][IPv4:11.11.11.11]
                          11.11.11.11      none      100        0      E
         AS_PATH: 21 11
         L2 Label: 202 (VNI)
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes type igmp-join-sync

Displays information for BGP EVPN routes to join IGMP sync.

Syntax

show bgp evpn routes type igmp-join-sync

show bgp evpn routes type igmp-join-sync brief

show bgp evpn routes type igmp-join-sync detail

Parameters

brief

Displays summary information.

detail

Displays detailed information.

Modes

Privileged EXEC mode

Examples

The following example shows routes to join IGMP sync:

```
Total number of BGP EVPN Igmp Join Sync Routes : 2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
Route Distinguisher: 19.1.2.3:32868
1      IGMPJoinSyncPrefix4:[0](100.1.2.3,234.1.2.3):19.1.2.3 (esi 00.010203040506070809)
                          19.1.2.3        0          100        0      BI
         AS_PATH:
2      IGMPJoinSyncPrefix6:[0](2001::4,ff03::1):19.1.2.3 (esi 02.010203040506070809)
                          19.1.2.3        0          100        0      BI
         AS_PATH:
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes type igmp-leave-sync

Displays BGP EVPN routes to leave IGMP sync.

Syntax

show bgp evpn routes type igmp-leave-sync

show bgp evpn routes type igmp-leave-sync brief

show bgp evpn routes type igmp-leave-sync detail

Parameters

brief

Displays summary information.

detail

Displays detailed information.

Modes

Privileged EXEC mode

Examples

The following example shows routes to leave IGMP sync:

```
Total number of BGP EVPN Igmp Leave Sync Routes :
2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP
D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-
MULTIPATH
       S:SUPPRESSED F:FILTERED
s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight
Status
Route Distinguisher:
19.1.2.3:32868
1      IGMPLeaveSyncPrefix4:[0](101.1.2.3,235.1.2.3):19.1.2.3 (esi
01.010203040506070809)
                          19.1.2.3        0          100        0
BI
         AS_PATH:
2      IGMPLeaveSyncPrefix6:[0](2002::5,ff04::3):19.1.2.3 (esi 03.010203040506070809)
                          19.1.2.3        0          100        0      BI
         AS_PATH:
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn routes unreachable

Displays route information about BGP EVPN routes whose destinations are unreachable through any of the paths in the BGP EVPN route table.

Syntax

show bgp evpn routes unreachable

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes unreachable** command.

```
device# show bgp evpn routes unreachable

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      AD:[00.000000000000989900][4294967295]
                          78.0.0.78       0          100        0      BME
         AS_PATH: 2 3
2      AD:[00.000000000000989900][4294967295]
                          78.0.0.78       0          100        0      ME
         AS_PATH: 2 3
3      ESR:[00.000000.000000.989900][IPv4:8.0.0.8]
                          78.0.0.78       0          100        0      BE
         AS_PATH: 2 3
4      ESR:[00.000000.000000.989900][IPv4:8.0.0.8]
                          78.0.0.78       0          100        0      E
         AS_PATH: 2 3
5      IP4Prefix:[0][11.1.1.0/24]
                          78.0.0.78       0          100        0      BE
         AS_PATH: 2 3
         L3_vni: 10020 Router Mac : 50:eb:1a:13:ce:f5
6      IP4Prefix:[0][11.1.1.0/24]
                          78.0.0.78       0          100        0      E
         AS_PATH: 2 3
         L3_vni: 10020 Router Mac : 50:eb:1a:13:ce:f5
7      IP4Prefix:[0][12.1.1.0/24]
                          78.0.0.78       0          100        0      BE
         AS_PATH: 2 3
         L3_vni: 10020 Router Mac : 50:eb:1a:13:ce:f5
8      IP4Prefix:[0][12.1.1.0/24]
                          78.0.0.78       0          100        0      E
         AS_PATH: 2 3
         L3_vni: 10020 Router Mac : 50:eb:1a:13:ce:f5
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bgp evpn summary

Displays the EVPN neighbors configured on the router, including how many routes have been received, sent, and filtered.

Syntax

show bgp evpn summary

Modes

Privileged EXEC mode

Examples

The following example displays summarized information for EVPN neighbors.

```
device# show bgp evpn summary
  BGP4 Summary
  Router ID: 3.3.100.3   Local AS Number: 100
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 3, UP: 2
  Number of Routes Installed: 5, Uses 625 bytes
  Number of Routes Advertising to All Neighbors: 6 (2 entries), Uses 120 bytes
  Number of Attribute Entries Installed: 7, Uses 805 bytes
  '+': Data in InQueue '>': Data in OutQueue '-': Clearing
  '*': Update Policy 'c': Group change 'p': Group change Pending
  'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  4.4.100.4         100         ESTAB     0h 4m49s    2        0        2        0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show bridge-domain

Displays information about Virtual Private LAN Services (VPLS) bridge domains.

Syntax

show bridge-domain [*id* [**logical-interface** [*id*]]]

show bridge-domain brief [{ **p2mp** | **p2p** }]

show bridge-domain vc-peer

Parameters

id

Specifies the bridge-domain identifier. The range is from 1 through 4096.

logical-interface

Causes the display of the ifindex and operational information for logical interfaces configured under the bridge domain.

id

Specifies a logical interface instance ID.

brief

Causes the display of summary bridge-domain information.

p2mp

Causes the display of multipoint service information.

p2p

Causes the display of multi-point cross-connect service information.

vc-peer

Causes the display of summary virtual connection (VC) peer information for the bridge domain.

Modes

Privileged EXEC mode.

Usage Guidelines

To display information about all bridge domains, specify the **bridge-domain** option without a bridge-domain identifier.

To display information about all logical interfaces configured under a specific bridge domain, specify the **logical-interface** option without a logical-interface identifier.

Command Output

The following table describes elements of information displayed in output from the **show bridge-domain** command:

Output field	Description
Assigned LSPs	Assigned label-switched paths.

Output field	Description
AC LIF Count	Number of attachment circuit (AC) logical interfaces in the bridge-domain.
bpdu-drop-enable	Indicates whether dropping Layer 2 (L2) bridge protocol data units (BPDUs) is enabled (TRUE) or disabled (FALSE) for the bridge domain.
Bridge-domain Type	Bridge-domain type. Type can be multipoint service (MP) or multi-point cross-connect (P2P).
Cos Enabled	Indicates whether Cost of Service (CoS) is enabled (True) or disabled (False) for a peer device in the bridge domain.
Load-balance	Indicates whether load balancing is enabled (True) or disabled (False) for a peer device in the bridge domain.
Local switching	Indicates whether local switching is enabled (TRUE) or disabled (FALSE) for the bridge domain.
Local VC lbl	Local virtual connection label (for the pseudowire that corresponds with the peer).
Local MTU	Local maximum transmission unit configuration (for the pseudowire that corresponds with the peer).
Local VC-Type	Local virtual connection mode configuration (for the pseudowire that corresponds with the peer).
Macs Dynamically learned	MAC addresses learned dynamically from traffic on the interface part of the bridge domain.
Macs statically configured	Number of MAC addresses configured statically over interfaces associated with the bridge domain.
MCT Enabled	Whether the bridge domain is configured under the MCT cluster. If it is, the field displays TRUE. Otherwise, the field displays FALSE.
Number of configured end-points	Number of endpoints that are configured for the bridge domain.
Number of Active end-points	Number of endpoints that are active in the bridge domain.
PW-profile	Pseudowire profile that is associated the bridge domain.
Remote VC lbl	Remote virtual connection label (for the pseudowire that corresponds with the peer).
Remote VC MTU	Remote maximum transmission unit configuration (for the pseudowire that corresponds with the peer).
Remote VC-Type	Remote virtual connection mode configuration (for the pseudowire that corresponds with the peer).
Total number of VC peers	Number of remote VPLS provider-edge (PE) devices that this node is peered with. (This is the same as the number of remote VPLS peers.)
Total VPLS peers	Number of remote VPLS provider-edge (PE) devices that this node is peered with.
Tunnel cnt	The number of MPLS tunnels that are selected by the pseudowire (corresponding to the peer).
VC id	Virtual connection identifier.
VE if-indx	Routing interface (virtual switching interface) index.
VFI LIF Count:	Number of virtual forwarding interfaces (VFI) in the bridge-domain.

Examples

The following example shows the information displayed by the **show bridge-domain** command.

```
device# show bridge-domain

Total Number of bridge-domains: 3
Number of bridge-domains: 3

Bridge-domain 1
-------------------------------
Bridge-domain Type: mp , VC-ID: 5, MCT Enabled: TRUE
Number of configured end-points:  5 , Number of Active end-points: 4
VE if-indx: 1207959555, Local switching: TRUE, bpdu-drop-enable:TRUE
PW-profile: 1, mac-limit: 128000
Number of Mac's learned:90000,     Static-mac count: 10,
VLAN: 100, Tagged ports: 2(2 up), Un-tagged ports: 0 (0 up)
Tagged ports: Eth 0/2/6, eth 0/2/8
Un-tagged ports:

Total PW peers: 2 (2 Operational)
Peer address: 12.12.12.12, State: Operational, Uptime: 2 hr 55 min
      Load-balance: True , Cos enabled:False,
      Assigned LSP;s:
      Tnnl in use: tnl2[RSVP]
      Local VC lbl: 983040, Remote VC lbl: 983040
      Local VC MTU: 1500, Remote VC MTU: 1500,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 15.15.15.15, State: Operational, Uptime: 2 hr 55 min
         Load-balance: False , Cos enabled:False,
      Assigned LSP's: lsp1, lsp2
      Tnnl in use: tnl1[MPLS]
      Local VC lbl: 983041, Remote VC lbl: 983043
      Local VC MTU: 1500, Remote VC MTU: 1500 ,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)

Bridge-domain 2
-------------------------------
Bridge-domain Type: mp , VC-ID: 100, MCT Enabled: FALSE
Number of configured end-points:  5 , Number of Active end-points: 4
VE if-indx:  NA, Local switching: FALSE, bpdu-drop-enable:FALSE
PW-profile: profile_1, mac-limit: 262144
Number of Mac's learned:90000,     Static-mac count: 10,
VLAN: 100, Tagged ports: 2(1 up), Un-tagged ports: 0 (0 up)
      Tagged ports: eth 0/2/10, eth 0/1/10
      Un-tagged ports:
VLAN: 150, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
      Tagged ports: eth 0/1/5
      Un-tagged ports:

Bridge-domain 3
-------------------------------
Bridge-domain Type: mp , VC-ID: 200, MCT Enabled: FALSE
Number of configured end-points:  5 , Number of Active end-points: 4
VE if-indx: 120793855, Local switching: FALSE, bpdu-drop-enable:FALSE
PW-profile: 2, mac-limit: 262144
Number of Mac's learned:90000,     Static-mac count: 10,
Local switching: TRUE,
VLAN: 500, Tagged ports: 2(2 up), Un-tagged ports: 2 (1 up)
Tagged ports:     eth 0/11/6, eth 0/4/3
Un-tagged ports:

Total VPLS peers: 3 (2 Operational)
Peer address: 5.5.5.5, State: Operational, Uptime: 2 hr 35 min
         Load-balance: False , Cos enabled:False,
      Assigned LSP;s:
      Tnnl in use: tnl2[RSVP]
      Local VC lbl: 983050, Remote VC lbl: 983050
      Local VC MTU: 1500,Remote VC MTU: 1500,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 20.20.20.20, State: Operational, Uptime: 0 hr 18 min
```

```
         Load-balance: False , Cos enabled:True,
      Assigned LSP's:
      Tnnl in use: NA,
      Local VC lbl: NA, Remote VC lbl: NA
      Local VC MTU: 1500,Remote VC MTU: 1500,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 10.10.10.10, State: Not-Operational (Tunnel Not Available),
         Load-balance: True , Cos enabled:False,
      Assigned LSP's: lsp10, lsp15
      Tnnl in use: NA,
      Peer Index:2
      Local VC lbl: NA, Remote VC lbl: NA
      Local VC MTU: 1500,Remote VC MTU: NA ,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: NA
```

The following example shows information about a bridge domain (501) in which the **load-balance** and **cos** options are configured for the peer device 10.9.9.9.

```
device# show bridge-domain 501

Bridge-domain 501
------------------------------
Bridge-domain Type: MP , VC-ID: 501, MCT Enabled: FALSE
Number of configured end-points:  2 , Number of Active end-points: 2
VE if-indx: 0, Local switching: TRUE, bpdu-drop-enable: TRUE
PW-profile: default, mac-limit: 0
VLAN: 501, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
Tagged Ports: eth1/6.501
Un-tagged Ports:
Total VPLS peers: 1 (1 Operational):

VC id: 501, Peer address: 10.9.9.9, State: Operational, uptime: 2 min
      Load-balance: True , Cos Enabled: True ,
      Tunnel cnt: 16
      rsvp  p101(cos_enable:True cos_value:1)
      rsvp  p102(cos_enable:True cos_value:1)
      rsvp  p103(cos_enable:True cos_value:1)
      rsvp  p104(cos_enable:True cos_value:1)
      rsvp  p105(cos_enable:True cos_value:1)
      rsvp  p106(cos_enable:True cos_value:1)
      rsvp  p107(cos_enable:True cos_value:1)
      rsvp  p108(cos_enable:True cos_value:1)
      rsvp  p109(cos_enable:True cos_value:1)
      rsvp  p110(cos_enable:True cos_value:1)
      rsvp  p111(cos_enable:True cos_value:1)
      rsvp  p112(cos_enable:True cos_value:1)
      rsvp  p113(cos_enable:True cos_value:1)
      rsvp  p114(cos_enable:True cos_value:1)
      rsvp  p115(cos_enable:True cos_value:1)
      rsvp  p116(cos_enable:True cos_value:1)
      Assigned LSPs count:0 Assigned LSPs:
      Local VC lbl: 989046, Remote VC lbl: 983040,
      Local VC MTU: 1500, Remote VC MTU: 1500,
      Local VC-Type: 5, Remote VC-Type: 5
```

The following example shows information about bridge domain 501 in which the **load-balance** option, **cos** option and three assigned label-switched paths (p1001, p1002, and p1003) are configured for the peer device 10.9.9.9.

```
device# show bridge-domain 501

Bridge-domain 501
-----------------------------
Bridge-domain Type: MP , VC-ID: 501, MCT Enabled: FALSE
Number of configured end-points:  2 , Number of Active end-points: 2
VE if-indx: 0, Local switching: TRUE, bpdu-drop-enable: TRUE
PW-profile: default, mac-limit: 0
VLAN: 501, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
Tagged Ports: eth1/6.501
Un-tagged Ports:
Total VPLS peers: 1 (1 Operational):

VC id: 501, Peer address: 10.9.9.9, State: Operational, uptime: 19 sec
      Load-balance: True , Cos Enabled: True ,
      Tunnel cnt: 2
      rsvp  p1001(cos_enable:True cos_value:1)
      rsvp  p1002(cos_enable:True cos_value:1)
      Assigned LSPs count:3 Assigned LSPs:p1001 p1002 p1000
      Local VC lbl: 989047, Remote VC lbl: 983040,
      Local VC MTU: 1500, Remote VC MTU: 1500,
      Local VC-Type: 5, Remote VC-Type: 5
```

The following example shows the information displayed by the **show bridge-domain brief** command.

```
device# show bridge-domain brief

Total Number of bridge-domains configured:  3
Number of VPLS bridge-domains: 3
Macs Dynamically learned: 100, Macs statically configured: 200

Name    ID(VC-ID) TYPE   Intf(up)   PWs(up)  macs
------- -------    ------ --------- ------       ------
1          3000      MP     5(3)             -           5000
2          5000      MP     2(1)             -           80
3       8000         MP     1(1)          3(2)     100000
```

History

Release version	Command history
18x.1.00	This command was introduced.

show capabilities

Displays whether a variety of network services are enabled ("true") or not ("false").

Syntax

show capabilities

Modes

Privileged EXEC mode

Usage Guidelines

Enter **?** to view available options.

Examples

The following example displays the status of all network services:

```
device# show capabilities
capabilities mqc span true
capabilities qos system-rx-queue-limit false
capabilities qos system-tx-queue-limit true
capabilities qos show-rx-queue-interface false
capabilities qos conf-rx-queue-interface false
capabilities qos cee nas false
capabilities qos cpu slot false
capabilities qos cpu queue false
capabilities l2 port_profile true
capabilities l2 overlap_vlan true
capabilities l2 rspan false
capabilities l2 mac_move true
capabilities l2 consistency_check false
capabilities l2 learning_mode true
capabilities l2 priority_tag true
capabilities l2 internal_nsm true
capabilities l2 lif_untagged_vlan_id false
capabilities l2 bridgedomain_local_switching false
capabilities l2 dot1x false
capabilities l3 ip_mtu true
capabilities ipv6 ipv6Raguard false
capabilities ssm aclTrafficType true
capabilities lag PortchannelRedundancy false
capabilities bgp next-hop-mpls false
capabilities bgp redistribute-isis false
capabilities license eula_display true
capabilities license dpod_display false
capabilities license slot_display false
capabilities ip igmp false
capabilities ip igmp-snooping igmp-snooping-version false
capabilities tm false
capabilities overlay gre false
capabilities cfm false
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cert-util sshkey

Displays SSH public key information.

Syntax

show cert-util sshkey user *user_acct*

Parameters

user *user_acct*
Specifies a user name.

Modes

Privileged EXEC mode

Examples

The following example shows how to display SSH public key information for the *admin* user.

```
device# show cert-util sshkey user admin
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cert-util syslogca

Displays the syslog Certification Authority (CA) certificate.

Syntax

show cert-util syslogca

Modes

Privileged EXEC mode

Examples

To display the syslog Certification Authority (CA) certificate on the device:

```
device# show cert-util ldapca

syslog CA
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cfm

Displays the current configuration and status of CFM.

Syntax

show cfm [**brief** | **connectivity**]

Parameters

brief

Displays the CFM brief output.

connectivity *session-id*

Dixplays the CFM connectivity configuration

Modes

Privileged EXEC mode

Command Output

The **show cfm** command displays the following information:

Output field	Description
Domain	The Domain is the network or the part of the network for which faults in connectivity are displayed.
Level	The level is the domain level in the range <0-7>.
Maintenance Association	The maintenance association name.
MAID Format	MAID format setting
CCM interval	The time interval between two successive Continuity Check messages (CCMs) that are sent by MEPs in the specified Maintenance Domain.
VLAN ID/ Bridge-Domain ID	The VLAN or Bridge-domain identifier of the maintenance association.
Priority	The priority of the CCM messages, sent by 'MEPs, in the range <0-7>.
MEP	The maintenance end point ID
Direction	Displays the direction the MEP was sent: Up - The MEP direction away from the monitored VLAN. Down - The MEP direction is towards the monitored VLAN.
MAC	Displays the associated MAC address.
PORT	Displays the associated port.
MIP	Displays the associated MIP.

Examples

Typical command output displaying the CFM settings for domain MD1.

```
device# show cfm
Domain: md1
Index: 1
Level: 7
  Maintenance association: ma5
  MA Index: 5
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
  MEP   Direction  MAC              PORT       VLAN         INNER-VLAN   PORT-STATUS-TLV
  ====  =========  =========        ====       ====         ==========   ===============
  1     UP         609c.9f5f.700d   Eth 1/9    50           --           N
```

Typical command output displaying the connectivity information.

```
device# show cfm connectivity
Domain: md1
Index: 1
Level: 7
  Maintenance association: ma5
  MA Index: 5
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
    MEP Id: 1
    MEP Port: Eth 1/9
      RMEP  MAC             VLAN/PEER         INNER-VLAN    PORT      STATE
      ====  ===             =========         ==========    ====      =====
      2     609c.9f5e.4809  19.1.1.1           --            --       OK
```

Typical command output displaying the brief output.

```
device# show cfm brief
Domain: md1
Index: 1
Level: 7  Num of MA: 1
  Maintenance association: ma5
  MA Index: 5
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
  Num of MEP: 1  Num of RMEP: 1
  rmepfail: 0 rmepok: 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cfm y1731 action-profile

Displays the Y.1731 action profile.

Syntax

show cfm y1731 action-profile

Modes

Privileged EXEC mode

Examples

This example displays the Y. 1731 action-profiles.

```
device# show cfm y1731 action-profile
----------------------------------------
  Name                  : a1

  Event                 : CCM Down
  Action(s)             : Interface Down
----------------------------------------
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cfm y1731 delay-measurement

Displays detailed info for all measurement sessions.

Syntax

show cfm y1731 delay-measurement

show cfm y1731 delay-measurement brief

show cfm y1731 delay-measurement session *session-id*

show cfm y1731 delay-measurement statistics

show cfm y1731 delay-measurement statistics brief

show cfm y1731 delay-measurement statistics session *session-id* **brief**

show cfm y1731 delay-measurement statistics session *session-id* **brief**

Parameters

brief
Specifies brief.

session *session-id*
Specifies session and the session ID.

statistics
Specifies statistics.

history*history-index*
Specifies history and the history index..

Modes

Privileged EXEC mode

Examples

This example displays detailed info for all measurement sessions.

```
device# show cfm y1731 delay-measurement statistics brief
------------------------------------------------------------------------------
Session Index : 1
Test Profile Name : my_test_profile2
------------------------------------------------------------------------------
HISTORY TABLE :
-------------------------------------------------------------------------------------------------
Index     Start    Elapsed    Avg Delay(us)   Max Delay(us)   Min Delay(ns)   FDV Avg(ns)     FDV
Max(ns)     FDV Min(ns)
-------------------------------------------------------------------------------------------------
4         03:13:34 00:15:00      33.281      33.542      32.851      39      79      12
3         02:58:34 00:15:00   27.162      27.690      26.745      41      85      13
2         02:43:34 00:15:00   28.260      30.452      27.540      40      83      12
1         02:28:34 00:15:00   29.120      32.164      28.242      41      84      13
-------------------------------------------------------------------------
Session Index : 2
Test Profile Name : my_test_profile2
-------------------------------------------------------------------------------------------------
HISTORY TABLE :
-------------------------------------------------------------------------------------------------
Index     Start    Elapsed    Avg Delay(us)   Max Delay(us)   Min Delay(ns)   FDV Avg(ns)     FDV
Max(ns)     FDV Min(ns)
-------------------------------------------------------------------------------------------------
4         05:12:14 00:15:00  32.180      33.543      31.589      38      79      11
3         04:48:54 00:15:00  29.060      29.950      27.654      41      83      12
2         04:30:40 00:15:00  30.105      30.154      28.764      40      82      12
1         04:15:14 00:15:00  31.234      31.665      29.143      40      81      12
-------------------------------------------------------------------------------------------------
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cfm y1731 synthetic-loss-measurement

Displays detailed info for all measurement sessions.

Syntax

show cfm y1731 synthetic-loss-measurement

show cfm y1731 synthetic-loss-measurement brief

show cfm y1731 synthetic-loss-measurement session *session-id*

show cfm y1731 synthetic-loss-measurement statistics

show cfm y1731 synthetic-loss-measurement statistics brief

show cfm y1731 synthetic-loss-measurement statistics session *session-id* **brief**

show cfm y1731 synthetic-loss-measurement statistics session *session-id* **brief**

show cfm y1731 synthetic-loss-measurement statistics session *session-id* **history** *history-index*

Parameters

brief

Specifies brief.

session *session-id*

Specifies session and the session ID.

statistics

Specifies statistics.

history*history-index*

Specifies history and the history index..

Modes

Privileged EXEC mode

Examples

This example displays detailed info for all measurement sessions.

```
device# show cfm y1731 synthetic-loss-measurement
    SLM Session Index       : 1
Test Profile Name              : my_test_profile1
Status                        : Active
Session Type                  : Initiator
Domain                        : md1
MA                            : ma1
Source MEP                    : 1
Target MEP                    : 2
Cos                           : 5
Start time                    : 19:49:55
Start time type               : Fixed
Stop time                     : 00:00:00
Stop time type                : Fixed
Tx-interval(sec)              : 1
Measurement-interval(min)     : 15
Forward Average (milliPercent) : 4294967295
Forward Max     (milliPercent) : 4294967295
Backward Average(milliPercent) : 1
Backward Max    (milliPercent) : 4
---------------------------------

SLM Session Index              : 2
Test Profile Name               : my_test_profile2
Status                        : Active
Session Type                  : Responder
Domain                        : md2
MA                            : ma2
Source MEP                    : 2
Target MEP                    : 1
Cos                           : 7
Start time                    : 01:30:30
Start time type               : Fixed
Stop time                     : 02:30:30
Stop time type                : Fixed
Tx-interval(sec)              : 2
Measurement-interval(min)     : 10
Forward Average  (milliPercent) : 4294967295
Forward Max      (milliPercent) : 4294967295
Backward Average (milliPercent) : 1
Backward Max     (milliPercent) : 3
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cfm y1731 test-profile

Displays the Y.1731 test profile.

Syntax

show cfm y1731 synthetic-loss-measurement

Modes

Privileged EXEC mode

Examples

This example displays the Y.1731 test profile.

```
-------------------------------------------------
Default Test Profiles:
-------------------------------------------------
  Name                          : 2dm-default-profile
  Type                          : ETH-DM
  Cos Value                     : 7
  Tx-Interval                   : 1 Second
  Tx-Frame-Count                : 10
  Measurement Interval          : 15 Minute(s)
  Threshold Average             : 4294967295 (uSec)
  Threshold Max                 : 4294967295 (uSec)
  Start time                    : 00:05:00 (After)
  Stop time                     : 01:05:00 (After)
  Timeout                       : 1 Second
-------------------------------------------------
-------------------------------------------------
  Name                          : 2slm-default-profile
  Type                          : ETH-SLM
  Cos Value                     : 7
  Tx-Interval                   : 1 Second
  Tx-Frame-Count                : 10
  Measurement Interval          : 15 Minute(s)
  Threshold Backward Average    : 4294967295
  Threshold Backward Max        : 4294967295
  Threshold Forward Average     : 4294967295
  Threshold Forward Max         : 4294967295
  Start time                    : 00:05:00 (After)
  Stop time                     : 01:05:00 (After)
  Timeout                       : 1 Second
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cipherset

Displays the current cipherset status for LDAP and SSH.

Syntax

show cipherset

Modes

Privileged EXEC mode

Examples

To display cipherset status on the device:

```
device# show cipherset

LDAP Cipher List        : !DH:HIGH:-MD5
SSH Cipher List         : 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cli

Displays all the current CLI settings.

Syntax

show cli

Modes

Privileged EXEC mode

Examples

Typical command output display.

```
device# show cli
autowizard            false
complete-on-space     false
history               100
idle-timeout          600
ignore-leading-space  false
output-file           terminal
paginate              true
prompt1               \H\M#
prompt2               \H(\m)#
screen-length         73
screen-width          120
service prompt config true
show-defaults         false
terminal              ansi
```

History

Release version	Command history
18x.1.00	This command was introduced.

show clock

Returns the local time, date, and time zone.

Syntax

show clock

Command Default

The local clock is used.

Modes

Privileged EXEC mode

Usage Guidelines

The command displays the current time for the device.

Examples

The following example shows the clock time.

```
device# show clock
2017-02-28 17:58:30 Etc/GMT
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cluster

Displays the MCT cluster information including client, PW client, member bridge domain, and member VLAN information.

Syntax

show cluster { *cluster-ID* [{ **client** [*client-ID*] } | **member bridge-domain** | **member vlan**

Parameters

cluster-ID

Specifies the cluster ID to display the cluster configuration, peer, PW client, and client information.

client

Specifies the displaying of all clients for the cluster including their names, IDs, local and remote labels, associated interface, and local and remote states.

client-ID

Optionally specifies the cluster client ID to also display the associated VLANs and the deployed and undeployed count. However, local and remote label information are not provided.

member bridge-domain

Specifies the displaying of the member bridge domain for the cluster including the local and remote multicast and unicast labels, and forwarding state.

member vlan

Specifies the displaying of the member VLANs for the cluster including the local and remote multicast and unicast labels.

Modes

Privileged EXEC mode

Usage Guidelines

When you delete an IP router ID that is used as the neighbor ID and IP address on an MCT peer, the **show cluster** command on the MCT peer devices displays inconsistent cluster states.

Command Output

The **show cluster** command displays the following information:

Output field		Description
Cluster		Name of the cluster
	Cluster State	Whether the cluster is deployed or undeployed
	Client Isolation Mode	Client-isolation mode configuration: Strict or Loose.
	DF Hold Time	Designated-forwarder hold timer value.
	Configured Member Vlan Range	Configured VLANs as members to the MCT cluster.

Output field		Description
	Active Member Vlan Range	Active member VLANs.
	Configured Member BD Range	Configured bridge domains as members to the MCT cluster.
	Active Member BD Range	Active member bridge domains.
	No. of Peers	Number of cluster peers.
	No. of Clients	Number of cluster clients.
Peer Info		Peer information
	Peer IP	Configured IP address for the MCT cluster peer.
	State	Whether the peer state is UP or DOWN.
	Peer Interface	Optionally configured peer interface.
	ICL Tunnel Type	State of the VXLAN tunnel to reach the MCT peer.
Client Info		Cluster client information
	Name	Configured client name.
	ID	Configured client ID.
	ESI	Configured 9-byte Ethernet Segment ID (ESI) value or 10-byte auto-generated ESI.
	Interface	Configured interface assigned to the client.
	Local/Remote State	Local and remote state of the client; Up or Down, Deployed (Dep) or Undeployed (UnDep).

Examples

The following example shows the information of the cluster on the SLX-OS device.

```
device# show cluster 1
Cluster c1 1
================
Cluster State: Deployed
Client Isolation Mode: Loose
DF Hold Time: 3
Configured Member Vlan Range: 100-101
Active Member Vlan Range: 100-101
Configured Member BD Range: 1000-1001
Active Member BD Range: 1000-1001
No. of Peers: 1
No. of Clients: 2


 Peer Info:
 ==========
 Peer IP: 10.38.38.38, State: Up
 Peer Interface: Not Configured
 ICL Tunnel Type: VXLAN, State: Up


 Client Info:
 ============
 Name           Id          ESI                Interface               Local/Remote State
 ----          ----       -----------         ---------               ------------------
 c3             3         0:a:b:1:2:3:0:0:0:0    Ethernet 0/11            Up / Up
```

The following example shows the member bridge-domain information.

```
device# show cluster member bridge-domain
 BD-ID     Mcast-label(Lo/Re)     Unicast-label(Lo/Re)     Forwarding state
-------    ------------------     --------------------     ----------------
  1000       822248/ -1                 805864/ 0                 Down
  1001       822249/ -1                 805865/ 0                 Down
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cluster management

Displays the current state of an IP-based management cluster.

Syntax

show cluster management [**detail**]

Parameters

detail

Displays detailed information.

Modes

Privileged EXEC mode

Examples

The following example displays basic information regarding the IP-based management cluster.

```
device# show cluster management
Total Number of Nodes in Cluster   : 2

Node-Id         Switch MAC                  IP Address       Status
-------------------------------------------------------------------------
1               60:9C:9F:5A:CF:14*          10.0.0.47        Connected
2              >60:9C:9F:5A:F1:14           10.0.0.48        Co-ordinator
```

The following example displays detailed information.

```
device# show cluster management detail
Total Number of Nodes in Cluster   : 2
Nodes Disconnected from Cluster    : 0
Node : 1
   Serial Number : Unitialized
   Condition : Good
   Cluster Status : Secondary Connected To Cluster
   Node Id : 1
   Co-ordinator : NO
   Switch MAC : 60:9C:9F:5A:CF:14
   Switch Type : BR-SLX9540
   Firmware version : v17r.2.00slxos17r.2.01_rel_180213_1205
   IP Address : 10.0.0.47
Node : 2
   Serial Number : Unitialized
   Condition : Good
   Cluster Status : Primary
   Node Id : 2
   Co-ordinator : YES
   Switch MAC : 60:9C:9F:5A:F1:14
   Switch Type : BR-SLX9540
   Firmware version : v17r.2.00slxos17r.2.01_rel_180213_1205
   IP Address : 10.0.0.48
```

History

Release version	Command history
18x.1.00	This command was introduced.

show copy-support status

Displays the status of the copy support operation.

Syntax

show copy-support status

Modes

Privileged EXEC mode

Usage Guidelines

The status is indicated by the percentage of completion. NORMAL indicates process is proceeding or completed without errors. FAULTY indicates a faulty blade.

This command is supported only on the local device.

Examples

To display the support upload status:

```
device# show copy-support status
```

History

Release version	Command history
18x.1.00	This command was introduced.

show cpu-interface

Displays information about the CPU Ethernet interface.

Syntax

show cpu-interface { **statistics interface backplane** }

Modes

Privileged EXEC mode

Examples

To display information about the CPU Ethernet interface:

```
device# show cpu-interface statistics interface backplane
Wave Management Interface Does Not Know The Client
```

History

Release version	Command history
18x.1.00	This command was introduced.

show crypto ca

Displays the crypto trust point/certificate information.

Syntax

show crypto ca {**trustpoint** | **certificates**}

Parameters

trustpoint

Displays the trustpoint and associated key pair details.

certificates

Displays the CA certificate and Identity certificate details.

Modes

Privileged EXEC mode

Usage Guidelines

To execute this command from other configuration modes, use the **do** command modifier.

Examples

Typical command display output:

```
device# show crypto ca trustpoint
trustpoint: t1; key-pair: k1
```

Typical command display output for certificates:

```
device# show crypto ca certificates
Trustpoint: t1
certificate:
SHA1 Fingerprint=B7:5B:DB:9B:24:69:40:39:36:66:4D:59:2C:69:83:8E:93:CA:23:0C
Subject: C=US, ST=CA, L=SJ, O=BRC, OU=SFI, CN=10:00:00:27:F8:87:70:29
Issuer: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Not Before: Oct 6 23:44:27 2014 GMT
Not After : Oct 6 23:44:27 2015 GMT
purposes: sslserver
CA certificate:
SHA1 Fingerprint=76:5B:D4:2C:CB:54:FE:6B:C5:E0:E3:FD:11:B0:88:70:80:12:C6:63
Subject: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Issuer: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Not Before: Sep 19 20:56:49 2014 GMT
Not After : Oct 19 20:56:49 2014 GMT
purposes: sslserver
```

History

Release version	Command history
18x.1.00	This command was introduced.

show crypto key

Displays the crypto key pair information for HTTPS.

Syntax

show crypto key mypubkey

Modes

Privileged EXEC mode

Usage Guidelines

To execute this command from other configuration modes, use the **do** command modifier.

Examples

Typical command output:

```
device# show crypto key mypubkey
key type: ecdsa
key label: k1
key size: 384
```

History

Release version	Command history
18x.1.00	This command was introduced.

show debug arp packet

Displays the ARP-packet debug configuration.

Syntax

show debug arp packet [**buffer**]

Parameters

buffer

Displays ARP packets saved in the relevant buffer.

Modes

Privileged EXEC mode

Command Output

The **show debug arp packet** command displays the following information:

Output field	Description
Protocol Type	Displays "ARP".
Package Flow	Displays "Sending" or "Rcvd".
Packet Type	Displays "ARP".
VRF ID	Displays the VRF ID.
Interface Info	Displays the physical or port-channel interface.
ScrMAC	Displays the MAC address of the source.
DstMAC	Displays the MAC address of the destination.
SrcIP	Displays the IP address of the source.
DstIP	Displays the IP address of the destination.

Examples

The following example is a typical output of the **show debug arp packet buffer** option.

```
device# show debug arp packet buffer
 Protocol Type        : ARP
 Packet Flow          : Sending
 Packet Type          : Req
 VRF ID               : 1
 Interface info       : Eth 0/1
 Ethernet,     SrcMAC : 768e.f807.2005, DstMAC: 0000.0000.0000
 Internet proto,SrcIP : 11.1.1.1, DstIP: 11.1.1.1

 Protocol Type        : ARP
 Packet Flow          : Sending
 Packet Type          : Req
 VRF ID               : 1
 Interface info       : Eth 0/1
 Ethernet,     SrcMAC : 768e.f807.2005, DstMAC: 0000.0000.0000
 Internet proto,SrcIP : 11.1.1.1, DstIP: 11.1.1.1

 Protocol Type        : ARP
 Packet Flow          : Rcvd
 Packet Type          : Req
 VRF ID               : 1
 Interface info       : Eth 0/1
 Ethernet,     SrcMAC : 0010.9400.0001, DstMAC: 0000.0000.0000
 Internet proto,SrcIP : 11.1.1.2, DstIP: 11.1.1.1

 Protocol Type        : ARP
 Packet Flow          : Sending
 Packet Type          : Rep
 VRF ID               : 1
 Interface info       : Eth 0/1
 Ethernet,     SrcMAC : 768e.f807.2005, DstMAC: 0010.9400.0001
 Internet proto, SrcIP : 11.1.1.1, DstIP: 11.1.1.2
```

History

Release version	Command history
18x.1.00	This command was introduced.

show debug dhcp packet

Displays the Dynamic Host Control Protocol (DHCP) packet capture configuration for interfaces configured for DHCP packet capturing.

Syntax

show debug dhcp packet

Modes

Privileged EXEC mode

Examples

The following example displays the DHCP packet capture configuration on interfaces.

```
device# show debug dhcp packet
%  DHCP  protocol  RCV debug is enabled on interface Eth 0/18
%  DHCP  protocol  TX debug is enabled on interface Eth 0/18
PCAP Buffer Configuration for Vrf ID 0: Buffer Type is Linear and BufferSize is 2056
```

History

Release version	Command history
18x.1.00	This command was introduced.

show debug dhcp packet buffer

Displays Dynamic Host Configuration Protocol (DHCP) packets saved in the DHCP packet capture buffer for all VRF IDs.

Syntax

show debug dhcp packet buffer

Modes

Privileged EXEC mode

Examples

The following command displays buffer content for all VRF IDs.

```
device# show debug dhcp packet buffer
Protocol Type       : DHCP
Packet Flow         : RX
Src Port            : 68 (DHCP Client)
Dst Port            : 67 (DHCP Server)
Message Type        : 1 (DHCP-Discover)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 0
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 0.0.0.0
Next Server IP      : 0.0.0.0
Relay Agent IP      : 0.0.0.0
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*********************************************
Protocol Type       : DHCP
Packet Flow         : TX
Src Port            : 67 (DHCP Server)
Dst Port            : 68 (DHCP Client)
Message Type        : 2 (DHCP-Offer)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 1
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 10.10.10.30
Next Server IP      : 20.20.20.20
Relay Agent IP      : 10.10.10.10
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*********************************************
Protocol Type       : DHCP
Packet Flow         : RX
Src Port            : 68 (DHCP Client)
Dst Port            : 67 (DHCP Server)
Message Type        : 3 (DHCP-Request)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 0
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 0.0.0.0
Next Server IP      : 0.0.0.0
Relay Agent IP      : 0.0.0.0
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*********************************************
Protocol Type       : DHCP
Packet Flow         : TX
Src Port            : 67 (DHCP Server)
Dst Port            : 68 (DHCP Client)
Message Type        : 5 (DHCP-Ack)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 1
Transaction ID      : 0
```

```
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 10.10.10.30
Next Server IP      : 20.20.20.20
Relay Agent IP      : 10.10.10.10
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
```

History

Release version	Command history
18x.1.00	This command was introduced.

show debug ip bgp all

Displays all BGP4 debugging options that are enabled.

Syntax

show debug ip bgp all

Modes

Privileged EXEC mode

Examples

The following example displays all BGP4 debugging options that are enabled.

```
device# show debug ip bgp all
```

History

Release version	Command history
18x.1.00	This command was introduced.

show debug ip igmp

Displays the Internet Group Management Protocol (IGMP) packets received and transmitted, as well as related events.

Syntax

show debug ip igmp

Modes

Privileged EXEC mode

Examples

The following displays example output.

```
device# show debug ip igmp
IGMP debugging status:

---------------------------------------

 errors          : off

 group           : off

 packets         : off

 query           : off

 report          : off

 direction       : none

 vlan            : none

 l2_port         : none
```

History

Release version	Command history
18x.1.00	This command was modified to include the output example.

show debug ipv6 mld

Displays the IPv6 Multicast Listener Discovery (MLD) packets received and transmitted, as well as related events.

Syntax

show debug ipv6 mld

Modes

Privileged EXEC mode

Examples

The following example displays the output of the **show debug ipv6 mld** command.

```
device# show debug ipv6 mld

MLD debugging status:
---------------------------------------
errors          : on
group           : off
packets         : on
query           : on
report          : on
direction       : none
vlan            : none
l2_port         : none
```

History

Release version	Command history
18x.1.00	This command was introduced.

show debug ipv6 packet

Displays IPv6 packets captured through the packet capture utility on an interface or all interfaces, as well as the packet capture configuration on the device.

Syntax

show debug ipv6 packet [**buffer** [**all** | **interface** [**ethernet** *slot/port*| **ve** *vlan_id*] [**rx** | **tx**]

Parameters

buffer
Specifies IPv6 packets.

all
Specifies all interfaces.

interface
Specifies an interface.

ethernet
Specifies an Ethernet port.

slot
Specifies a valid slot number. This must be **0** for devices that do not support line cards.

port
Specifies a valid port number.

ve*vlan_id*
Specifies a virtual Ethernet interface.

Command Default

None

Modes

Privileged EXEC mode

Examples

The following example displays the current PCAP configuration on the device.

```
device# show debug ipv6 packet
```

The following example displays IPv6 packets captured on all interfaces.

```
device# show debug ipv6 packet buffer all
```

The following example displays IPv6 packets captured on a specific Ethernet interface.

```
device# show debug ipv6 packet buffer interface ethernet 0/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show debug lacp

Displays the status of Link Aggregation Control Protocol (LACP) debugging on the device.

Syntax

show debug lacp

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

show debug lldp

Displays the status of Link Layer Discovery Protocol (LLDP) debugging on the device.

Syntax

show debug lldp

Modes

Privileged EXEC mode

Examples

The following example displays the status of LLDP debugging on the device.

```
device# show debug lldp
 LLDP debugging status:
Interface Eth0/0    : Transmit Receive  Detail
```

History

Release version	Command history
18x.1.00	This command was introduced.

show debug spanning-tree

Displays the status of STP debugging flags on the device.

Syntax

show debug spanning-tree

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

show debug vrrp

Displays the status of Virtual Router Redundancy Protocol (VRRP) debugging on the device.

Syntax

show debug vrrp

Modes

Privileged EXEC mode

Usage Guidelines

This command is for VRRP and VRRP-E. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Examples

If you run this command and the debug parameter has already been set to debug all VRRP events, the following is displayed:

```
device# show debug vrrp
 VRRP event debugging is on
```

History

Release version	Command history
18x.1.00	This command was introduced.

show defaults threshold

Displays the default thresholds for environmental and alert values for small form-factor pluggable (SFP) types.

Syntax

show defaults threshold sfp type *sfp-type*

Parameters

sfp-type

The following SFP types are supported:

1GCOP
— 1G SFP Copper

1GCWDM
— 1G SFP CWDM

1GLR
— 1G SFP LR

1GSR
— 1G SFP SR

10GDWDMT
— 10G SFP+ DWDM Tunable

10GER
— 10G SFP+ ER

10GLR
— 10G SFP+ LR

10GSR
— 10G SFP+ SR

10GUSR
— 10G SFP+ USR

10GZR
— 10G SFP+ ZR

40GER
— 40G QSFP+ ER4

40GESR
— 40G QSFP+ eSR4 INT

40GLM
— 40G QSFP+ LM4

40GLR
— 40G QSFP+ LR4

40GSR
— 40G QSFP+ SR4

40GSRINT
— 40G QSFP+ SR4 INT

100GAOC
— 100G QSFP28 AOC

100GCLR
— 100G QSFP28 CLR4

100GCWDM
— 100G QSFP28 CWDM4

100GESR
— 100G QSFP28 eSR4

100GLR
— 100G QSFP28 LR4

100GLRLT
— 100G QSFP28 LR4 Lite

100GPSM
— 100G QSFP28 PSM4

100GSR
— 100G QSFP28 SR4

Modes

Privileged EXEC mode

Usage Guidelines

You can modify these thresholds with the **threshold-monitor sfp** command.

Examples

The following example displays the default sfp thresholds for 1G SFP Copper.

```
device# show defaults threshold sfp type 1GCOP
Type: 1GCOP
+------------+-------------------------+-------------------------+--------+
|            |     High Threshold      |     Low Threshold       | Buffer |
| Area       | Value | Above  | Below  | Value     |  Below     | Value  |
|            |       | Action | Action |           |  Action    |        |
+------------+-------+--------+--------+-----------+------------+--------+
| Temp C     |    90 | raslog | none   |        -45|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| RXP uWatts |   501 | raslog | none   |          6|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| TXP uWatts |   794 | raslog | none   |         71|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| Current mA |    45 | raslog | none   |          1|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| Voltage mV |  3700 | raslog | none   |       2900|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
```

History

Release version	Command history
18x.1.00	This command was introduced.

show dot1x

Displays 802.1X-related information.

Syntax

show dot1x [**all**]

show dot1x [**interface ethernet** *slot/port*]

show dot1x [**diagnostics** | **session-info** | **statistics**] { **interface ethernet** *slot/port* }

Parameters

all

Displays detailed dot1x information for all of the ports.

interface

Displays the state of a specified interface.

diagnostics

Displays diagnostics information for the authenticator associated with a port.

session-info

Displays all statistical information of an established session.

statistics

Displays the statistics of a specified interface.

Modes

Privileged EXEC mode

Examples

The following example shows the overall state of 802.1X authentication on the system.

```
device# show dot1x
802.1X Port-Based Authentication: Enabled
PAE Capability:                   Authenticator Only
Protocol Version:                 2
Auth Server:                      RADIUS
Readiness test timeout:           10
RADIUS Configuration
--------------------
Position:                1
Server Address:          10.24.65.6
Port:                    1812
Secret:                  xxxxxxxxx
Retry Interval:          5 seconds
```

The following example shows detailed 802.1X authentication information for all of the ports.

```
device# show dot1x all
802.1X Port-Based Authentication: Enabled
PAE Capability:                   Authenticator Only
Protocol Version:                 2
Auth Server:                      RADIUS
Readiness test timeout:           10

RADIUS Configuration
--------------------
Position:                 1
Server Address:           10.20.106.144
Port:                     1812
Secret:                   testing123
Retry Interval:           4 seconds

Position:                 2
Server Address:           10.20.106.189
Port:                     1812
Secret:                   testing123
Retry Interval:           4 seconds

802.1X info for interface Eth 1/31
----------------------------------
Port Control:             Auto
Protocol Version:         2
ReAuthentication:         Enabled
Auth Fail Max Attempts:   0
ReAuth Max:               2
Tx Period:                30 seconds
Quiet Period:             60 seconds
Supplicant Timeout:       30 seconds
Re-Auth Interval:         3600 seconds
Dynamic VLAN assigned:    50
Filter-strict-security:   Enabled
IP ACL assigned (IN|OUT): IPEXT-50 | IPEXT-OUT-50
MAC ACL assigned:         mac-ext
```

The following example shows all diagnostics information for the authenticator associated with a port.

```
device# show dot1x diagnostics interface ethernet 1/2
802.1X Diagnostics for interface Eth 1/2
----------------------------------------
authEnterConnecting:                1
authEaplogoffWhileConnecting:       0
authEnterAuthenticating:            1
authSuccessWhileAuthenticating:     1
authTimeoutWhileAuthenticating:     0
authFailWhileAuthenticating:        0
authEapstartWhileAuthenticating:    0
authEaplogoffWhileAuthenticating:   0
authReauthsWhileAuthenticated:      0
authEapstartWhileAuthenticated:     0
authEaplogoffWhileAuthenticated:    0
BackendResponses:                   11
BackendAccessChallenges:            10
BackendOtherrequestToSupplicant:    11
BackendAuthSuccess:                 1
BackendAuthFails:                   0
```

The following example shows state of a specified interface.

```
device# show dot1x interface ethernet 1/31
802.1X info for interface Eth 1/31
---------------------------------
Port Control:             Auto
Protocol Version:         2
ReAuthentication:         Enabled
Auth Fail Max Attempts:   0
ReAuth Max:               2
Tx Period:                30 seconds
Quiet Period:             60 seconds
Supplicant Timeout:       30 seconds
Re-Auth Interval:         3600 seconds
Dynamic VLAN assigned:    50
Filter-strict-security:   Enabled
IP ACL assigned (IN|OUT): IPEXT-50 | IPEXT-OUT-50
MAC ACL assigned:         mac-ext
```

The following example shows information for all clients on the port.

```
device# show dot1x session-info interface ethernet 1/2
802.1X Session info for interface Eth 1/2
-----------------------------------------
Mac Address: 0021.5ec6.15ce
---------------------------------------
User Name:                md5user2
Session Time:             2 secs
Terminate Cause:          Not terminated yet
Session Status:           Authorized
PAE State:                Authenticated
BE State:                 Idle
VLAN:                     N/A
IP ACL (IN | OUT):        N/A | N/A
MAC ACL:                  N/A
Current Id:               18
Id From Server:           17
```

The following example shows the statistics of a specified interface.

```
device# show dot1x statistics interface ethernet 1/2
802.1X statistics for interface Eth 1/2
---------------------------------------
EAPOL Frames Rx:                    12
EAPOL Frames Tx:                    43
EAPOL Start Frames Rx:              1
EAPOL Logoff Frames Rx:             0
EAP Rsp/Id Frames Rx:               1
EAP Response Frames Rx:             10
EAP Req/Id Frames Tx:               23
EAP Request Frames Tx:              10
Invalid EAPOL Frames Rx:            0
EAPOL Length Error Frames Rx:       0
EAPOL Last Frame Version Rx:        1
Invalid EAP Frames Rx:              0
EAP Length Error Frames Rx:         0
EAPOL Last Frame Src:               0021.5ec6.15ce
```

History

Release version	Command history
18x.1.00	This command was introduced.

show dpod

Displays Dynamic Ports on Demand (DPOD) licensing.

Syntax

show dpod

Modes

Privileged Exec mode

Usage Guidelines

The **show dpod** command displays a summary of POD license status and POD license assignments.

Examples

```
device# show dpod
48 10G ports are available in this switch
6 100G ports are available in this switch
COD license is installed
100G Port Upgrade license is installed
Dynamic POD method is in use

48 10G port assignments are provisioned for use in this switch:
24 10G port assignments are provisioned by the base switch allowance
24 10G port assignments are provisioned by the COD license
2 10G ports are assigned to the base switch allowance or installed licenses:
2 10G ports are assigned to the base switch allowance
0 10G ports are assigned to the COD license
10G ports assigned to the base switch allowance:
0/7, 0/9
10G ports assigned to the COD license:
None
10G ports that are not assigned:
0/1, 0/2, 0/3, 0/4, 0/5, 0/6, 0/8, 0/10, 0/11, 0/12
0/13, 0/14, 0/15, 0/16, 0/17, 0/18, 0/19, 0/20, 0/21, 0/22
0/23, 0/24, 0/25, 0/26, 0/27, 0/28, 0/29, 0/30, 0/31, 0/32
0/33, 0/34, 0/35, 0/36, 0/37, 0/38, 0/39, 0/40, 0/41, 0/42
0/43, 0/44, 0/45, 0/46, 0/47, 0/48
46 10G license reservations are still available for use by unassigned ports

6 100G port assignments are provisioned for use in this switch:
0 100G port assignments are provisioned by the base switch allowance
6 100G port assignments are provisioned by the 100G Port Upgrade license
3 100G ports are assigned to the base switch allowance or installed licenses:
0 100G ports are assigned to the base switch allowance
3 100G ports are assigned to the 100G Port Upgrade license
100G ports assigned to the base switch allowance:
None
100G ports assigned to the 100G Port Upgrade license:
0/49, 0/50, 0/53
100G ports that are not assigned:
0/51, 0/52, 0/54
3 100G license reservations are still available for use by unassigned ports
```

History

Release version	Command history
18x.1.00	This command was introduced.

show environment fan

Displays fan status information.

Syntax

show environment fan

Modes

Privileged EXEC mode

Command Output

The **show environment fan** command displays the following information:

Output field	Description
OK	Fan is functioning correctly at the displayed speed (RPM).
absent	Fan is not present.
below minimum	Fan is present but rotating too slowly or stopped.
above maximum	Fan is rotating too quickly.
unknown	Unknown fan unit installed.
faulty	Fan has exceeded hardware tolerance and has stopped. In this case, the last known fan speed is displayed.
Airflow direction	Port side intake or Port side exhaust. This value is not applicable to modular chassis.
speed	Fan RPM.

Examples

The following example displays fan status information:

```
device# show environment fan

Fan 1 is Ok, speed is 4243 RPM
Fan 2 is Ok, speed is 4249 RPM

Fan 3 is Ok, speed is 4402 RPM
```

History

Release version	Command history
18x.1.00	This command was introduced.

show environment history

Displays the field-replaceable unit (FRU) history log.

Syntax

show environment history

Modes

Privileged EXEC mode

Usage Guidelines

The history log records insertion and removal events for field-replaceable units (FRUs), such as blades, power supplies, fans, and world wide name (WWN) or chassis ID (CID) cards. The type of FRU supported depends on the hardware platform.

Command Output

The **show environment history** command displays the following information:

Output field	Description
Object type	On standalone platforms: FAN, POWER SUPPLY, WWN (WWN card), or UNKNOWN.
Object number	Displays the slot number for blades. Displays the unit number for all other object types.
Event type	Displays Inserted, Removed, or Invalid.
Time of the event	Displays the date in the following format: Day Month dd hh:mm:ss yyyy.
Factory Part Number	Displays the part number (xx-yyyyyyy-zz) or Not available.
Factory Serial Number	Displays the FRU serial number (xxxxxxxxxxx) or Not available.

Examples

The following example displays the FRU history on a device.

```
device# show environment history
POWER SUPPLY  Unit 1  Inserted at Sun Jul 12 21:59:17 2015
Factory Part Number:
Factory Serial Number:

POWER SUPPLY  Unit 2  Inserted at Sun Jul 12 21:59:17 2015
Factory Part Number:
Factory Serial Number:

FAN  Unit 1  Inserted at Sun Jul 12 21:59:17 2015
Factory Part Number:   60-1003113-03
Factory Serial Number: DUX0343K00A

FAN  Unit 2  Inserted at Sun Jul 12 22:02:40 2015
Factory Part Number:   60-1003113-03
Factory Serial Number: DUX0343K00B

FAN  Unit 3  Inserted at Sun Jul 12 22:02:41 2015
Factory Part Number:   60-1003113-03
Factory Serial Number: DUX0343K00C

SFM  Slot S1 Inserted at Sun Jul 12 22:02:41 2015
Factory Part Number:   40-0000155-xx
Factory Serial Number: LU000000000

LC  Slot L4 Inserted at Sun Jul 12 22:02:41 2015
Factory Part Number:   50-1002179-14
Factory Serial Number: BVT0307H00P

CID  Unit 1  Inserted at Sun Jul 12 22:02:43 2015
Factory Part Number:   60-1003219-01
Factory Serial Number: BWF0415K00D

MM  Slot M1 Inserted at Sun Jul 12 22:02:43 2015
Factory Part Number:   60-1003051-02
Factory Serial Number: DCR0341K006

(Output truncated)
```

History

Release version	Command history
18x.1.00	This command was introduced.

show environment power

Displays the type and current status of the switch power supply.

Syntax

show environment power

Modes

Privileged EXEC mode

Command Output

The **show environment power** command displays the following information:

Output field	Description
OK	Power supply is functioning correctly.
absent	Power supply is not present.
unknown	Unknown power supply unit is installed.
predicting failure	Power supply is present but predicting failure. Replace the power supply as soon as possible.
faulty	Power supply is present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).
Airflow	Direction of fan air flow (not applicable to modular chassis).

Examples

The following example displays the power supply status.

```
device# show environment power

Power Supply #1 is OK
DELTA type: A V23.45
Power Supply #2 is OK
DELTA type: A V23.45
Power Supply #3 is absent
Power Supply #4 is absent
Power Supply #5 is absent
Power Supply #6 is absent
```

History

Release version	Command history
18x.1.00	This command was introduced.

show environment sensor

Displays the environment sensor status.

Syntax

show environment sensor

Modes

Privileged EXEC mode

Usage Guidelines

The command output displays the current temperature, fan, and power supply status readings from sensors located on the switch. For an explanation of power supply status values, refer to the **show environment power** topic.

Examples

The following example displays sensor readings on the device:

```
device# show environment sensor
sensor  1: (Temperature) is Ok, value is 31 C
sensor  2: (Temperature) is Ok, value is 53 C
sensor  3: (Temperature) is Ok, value is 52 C
sensor  4: (Temperature) is Ok, value is 37 C
sensor  5: (Temperature) is Ok, value is 32 C

(Output truncated)

sensor 50: (Fan         ) is Ok,speed is 4297 RPM
sensor 51: (Fan         ) is Ok,speed is 4240 RPM
sensor 52: (Fan         ) is Ok,speed is 4350 RPM
sensor 53: (Power Supply) is Ok
sensor 54: (Power Supply) is Ok
sensor 55: (Power Supply) is Absent
sensor 56: (Power Supply) is Absent
sensor 57: (Power Supply) is Absent
sensor 58: (Power Supply) is Absent
```

History

Release version	Command history
18x.1.00	This command was introduced.

show environment temp detail

Displays information pertaining to the environment temperature.

Syntax

show environment temp detail *detail*

Parameters

detail

Specifies to display information in detail.

Modes

Privileged EXEC mode

Examples

This example displays the environment temperature in detail.

```
device# show environment temp detail
Sensor  Slot    State           Blade Name      Sensor name             Centigrade     Fahrenheit
  ID
=============================================================================================================
  1       1     Ok            MM v1             1 - front                  25             77
  2       1     Ok            MM v1             2 - mid-board              29             84
  3       1     Ok            MM v1             3 - backplane connector    36             96
  4       1     Ok            MM v1             4 - PEX die                19             66
=============================================================================================================
  5       2     Ok            MM v2             1 - front                  25             77
  6       2     Ok            MM v2             2 - mid-board              28             82
  7       2     Ok            MM v2             3 - backplane connector    38            100
  8       2     Ok            MM v2             4 - PEX die                19             66
=============================================================================================================
  9       7     Absent
=============================================================================================================
10        8     Ok            SFM4 v4           TEMP0                      61            141
11        8     Ok            SFM4 v4           R-FRONT                    34             93
12        8     Ok            SFM4 v4           L-REAR                     61            141
13        8     Ok            SFM4 v4           R-REAR                     35             95
14        8     Ok            SFM4 v4           FE0                        86            186
=============================================================================================================
15        9     Absent
=============================================================================================================
16       10     Absent
=============================================================================================================
17       11     Absent
=============================================================================================================
18       12     Absent
=============================================================================================================
19        3     Absent
=============================================================================================================
20        4     Absent
=============================================================================================================
21        5     Ok            LC72X10G v1       MB-L-REAR                  30             86
22        5     Ok            LC72X10G v1       MB-R-REAR                  25             77
23        5     Ok            LC72X10G v1       MB-L-FRONT                 24             75
24        5     Ok            LC72X10G v1       MB-R-FRONT                 30             86
25        5     Ok            LC72X10G v1       MB-JERI-1                  43            109
26        5     Ok            LC72X10G v1       MB-JERI-2                  30             86
27        5     Ok            LC72X10G v1       DC-Center                  22             71
=============================================================================================================
28        6     Ok            LC36x100G v1      MB L-REAR                  31             87
29        6     Ok            LC36x100G v1      MB R-REAR                  24             75
30        6     Ok            LC36x100G v1      MB L-FRONT                 31             87
31        6     Ok            LC36x100G v1      MB R-FRONT                 26             78
32        6     Ok            LC36x100G v1      MB JERICHO 1               42            107
33        6     Ok            LC36x100G v1      MB JERICHO 2               30             86
34        6     Ok            LC36x100G v1      MB JERICHO 3               30             86
35        6     Ok            LC36x100G v1      DC L-REAR                  24             75
36        6     Ok            LC36x100G v1      DC R-REAR                  30             86
37        6     Ok            LC36x100G v1      DC L-FRONT                 31             87
38        6     Ok            LC36x100G v1      DC R-FRONT                 31             87
39        6     Ok            LC36x100G v1      DC JERICHO 1               30             86
40        6     Ok            LC36x100G v1      DC JERICHO 1               41            105
41        6     Ok            LC36x100G v1      DC JERICHO 1               30             86
```

History

Release version	Command history
18x.1.00	This command was introduced.

show event-handler activations

Displays operational data of activated event-handlers.

Syntax

show event-handler activations

Modes

Privileged EXEC mode

Command Output

The **show event-handler activations** command displays the following information:

Output field	Description
Event-handler	Displays the event-handler name.
Last Trigger Activation Time	Displays the time of the last trigger activation. If no trigger was activated, displays "Never".
Total Trigger Activations	Displays the total number of trigger activations.
Last Action Completion Time	Displays the completion time of the last event-handler action run. If no event-handler action ran, displays "Never".
Last Action Completion Status. Exit Code =	Displays the status of the last completed event-handler action. If the Python script assigns exit codes, such codes are displayed here. An exit code of `0` indicates one of the following: • No code was assigned to this condition. • The script author assigned `0` to a specified condition.
Total Action Completions	Displays the number of completed event-handler actions.

Examples

The following example displays event-handler operational data.

```
device# show event-handler activations

Event-handler : evh1
Last Trigger Activation Time: 2015-04-30 17:28:12
Total Trigger Activations: 25
Last Action Completion Time: 2015-04-30 17:28:57
Last Action Completion Status: Exit Code = 0
Total Action Completions: 25

Event-handler : evh2
Last Trigger Activation Time: 2015-04-28 22:02:51
Total Trigger Activations: 8
Last Action Completion Time: 2015-04-28 22:02:58
Last Action Completion Status: Exit Code = 0
Total Action Completions: 8
```

show file

Displays the contents of a file in the local flash memory.

Syntax

show file *filename*

Parameters

filename

The name of the file to be displayed.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

Examples

The following example displays the contents of a file in the flash memory.

```
device# show file defaultconfig.cluster
vlan dot1q tag native
!
cee-map default
remap fabric-priority priority 0
remap lossless-priority priority 0
priority-group-table 15.0 pfc off
priority-group-table 1 weight 40 pfc on
priority-group-table 2 weight 60 pfc off
priority-table 2 2 2 1 2 2 2 15.0
!!
port-profile default
vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
!
interface Port-channel 1
vlag ignore-split
  description Homerun port-channel on MM1
  shutdown
!
interface Port-channel 2
  vlag ignore-split
  description Homerun port-channel on MM2
  shutdown
!
protocol lldp
!!
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging auditlog class SECURITY
!
end
```

History

Release version	Command history
18x.1.00	This command was introduced.

show firmwaredownloadhistory

Displays the firmware download history for the device.

Syntax

show firmwaredownloadhistory

Modes

Privileged EXEC mode

Usage Guidelines

The log records the date and time of the firmware download, the device name, slot number, process ID, and firmware version.

Use this command to display information for the local management module only.

Examples

The following example displays the firmware download history.

```
SLX# show firmwaredownloadhistory

Firmware version history

Sno    Date & Time                Switch Name  Slot  PID    OS Version
1      Thu Mar  2 05:52:27 2017   SLX          0     33552  17r.1.00
2      Wed Feb 22 17:10:45 2017   SLX          0     3187   16r.1.00
```

History

Release version	Command history
18x.1.00	This command was introduced.

show firmwaredownloadstatus

Displays the firmware download activity log.

Syntax

show firmwaredownloadstatus [**brief**] [**summary**]

Parameters

brief

Displays only the last entry of the firmware download event log.

summary

Displays a high-level summary of the firmware download status.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display an event log that records the progress and status of events that occur during a firmware download. The event log is created by the **firmware download** command and is retained until you issue another **firmware download** command. A time stamp is associated with each event.

The output of **show firmwaredownloadstatus** and **show firmwaredownloadstatus brief** are equivalent.

The output varies depending on the hardware platform.

Examples

The following example displays the firmware download event log.

```
device# show firmwaredownloadstatus
 [1]: Wed Mar  1 21:58:34 2017
Slot M1: Firmware install begins.

[2]: Wed Mar  1 22:03:59 2017
Slot M1: Firmware install ends.

[3]: Wed Mar  1 22:03:59 2017
Slot M1: Firmware starts to swap.

[4]: Wed Mar  1 22:04:19 2017
Slot M1: Firmware is swapped.

[5]: Wed Mar  1 22:04:20 2017
Slot M1: The blade begins to reboot.

[6]: Wed Mar  1 22:09:03 2017
Slot L2/0: Firmware install begins.

[7]: Wed Mar  1 22:09:08 2017
Slot L4/0: Firmware install begins.

[8]: Wed Mar  1 22:11:37 2017
Slot L2/0: Firmware install ends.

[9]: Wed Mar  1 22:11:37 2017
Slot L2/0: Firmware starts to swap.

[10]: Wed Mar  1 22:11:46 2017
Slot L4/0: Firmware install ends.

(Output truncated)
```

The following example displays a high-level summary of the firmware download status.

```
device# show firmwaredownloadstatus summary
No Firmware Download session in progress.
```

History

Release version	Command history
18x.1.00	This command was introduced.

show hardware profile

Displays details of the current active hardware profile.

Syntax

show hardware profile [**current**]

Parameters

current

Displays current active running profile information. For the current version, the output with or without **current** is equivalent.

Modes

Privileged EXEC mode

Examples

The following example displays details of the current active hardware profile.

```
device# show hardware profile

 switch type: EN-SLX-9030-48T

                       current TCAM profile:    DEFAULT
                                    l2-acl:    502
                                  l3v4-acl:    1526
                                  l3v6-acl:    1014
                             l3v4-acl-vxlan:    0
                                   l2l3v4Of:    0
                                 egrl2-acl:    246
                                 egrl3-acl:    246
                                   l3v6-of:    0
                                  Flex-acl:    0
_____________________________________________________________________

                    current SLX ROUTE profile:    ROUTE-DEFAULT
                                        hwopt:    Disabled
                                    v4FibComp:    Disabled
                                    v6FibComp:    Disabled
_____________________________________________________________________
                       current LAG  profile:    LAG-DEFAULT
                                    max-lag:    64
_____________________________________________________________________

                     current COUNTERS profile:    COUNTERS-DEFAULT
                             InLIF - HitCount:    32768
                              InL4 - HitCount:    16384
                            OutLIF - HitCount:    16384
                             OutL4 - HitCount:    0
_____________________________________________________________________

                           current CAM Share:
                                    l2In-acl:    no
                                  l3v4In-acl:    no
                                    l3v4-pbr:    no
                                  l3v6In-acl:    no
                                    l3v6-pbr:    no
                                        Ofv4:    no
                                      Ofl3v6:    no
_____________________________________________________________________
```

History

Release version	Command history
18x.1.00	This command was introduced.

show history

Displays the history of commands executed on the device during the current session.

Syntax

show history [*number*]

Parameters

number

Specifies the number of commands to display. Values range from 1 through 1000.

Modes

Privileged EXEC mode

Usage Guidelines

If you enter this command without specifying a number, up to 1000 commands are displayed.

Examples

The following command displays the four last commands entered.

```
device# show history 4
12:45:06 -- show hardware port-group
12:45:23 -- show interface switchport
12:45:37 -- show interface stats brief
12:45:45 -- show arp vrf test
```

History

Release version	Command history
18x.1.00	This command was introduced.

show http server status

Displays HTTP and HTTPS server status information.

Syntax

show http server status

Modes

Privileged EXEC mode

Command Output

The **show http server status** command displays the following information:

Output field	Description
VRF-Name	VRF name
Status	HTTP and HTTPS server status (enabled or disabled)

Examples

The following example displays HTTP and HTTPS server status information.

```
 device# show http server status

VRF-Name: mgmt-vrf       Status: HTTP Enabled and HTTPS Disabled
VRF-Name: default-vrf    Status: HTTP Enabled and HTTPS Disabled
```

History

Release version	Command history
18x.1.00	This command was introduced.

show interface

Displays the detailed interface configuration and capabilities of all interfaces or for specified interfaces.

Syntax

show interface [**description**]

show interface [**ethernet** *slot* **/** *port* | **port-channel** *number*] [**switchport**]

show interface loopback *number*

show interface management [*management-id*]

show interface trunk

Parameters

description
For all device interfaces, displays a summary that includes the Description field.

ethernet
Specifies an Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies a port-channel number. Depending on the platform, valid values range from 1 through 1024.

switchport
Specifies Layer 2 interfaces.

loopback *number*
Specifies a loopback interface.

management *management-id*
Specifies a management interface.

trunk
Displays VLANs on the trunk.

Modes

Privileged EXEC mode

Command Output

The **show interface ethernet** command displays the following information:

Output field	Description
Ethernet *slot* / *port*	Displays the port state. The states are "admin down, line protocol is down (admin down)" or "up, line protocol is up (connected)".
Hardware	Displays the MAC address of the Ethernet interface.
Pluggable media	Displays "present" or "not present".
Interface index	Displays the interface index.
MTU	Displays the maximum transmission unit (MTU), in bytes.
*n*G interface	Displays the speed of the Ethernet interface, in Gb.
Transparent phy loopback	If **loopback phy** was configured on the interface, displays "configured". If not configured, this line is not displayed.
LineSpeed Actual	Displays the actual line speed in Mb or "Nil".
LineSpeed Configured	Displays "Auto" or a value in Mb.
Duplex	Displays "Half" or "Full".
Priority Tab	Displays "enable" or "disable".
Forward LACP PDU	Displays "enable" or "disable".
Route Only	Displays "enabled" or "disabled".
Queueing strategy	Displays "FIFO".
Primary Internet Address	Displays the primary Internet address
Broadcast	Displays the broadcast Internet address
Receive Statistics	Displays receive statistics: packets, bytes, unicasts, multicasts, broadcasts, packets by byte size, runts, jabbers, cyclic redundancy check (CRC), overruns, errors, and discards.
Transmit Statistics	Displays transmit statistics: packets, bytes, unicasts, multicasts, broadcasts, underruns, errors, and discards.
Rate info	Displays input and output in Mbits/sec, packets/sec, and percentage of the line rate.
Route-Only Packets Dropped	Displays the number or routing-only packets dropped.

The **show interface loopback** command displays the following information:

Output field	Description
Loopback	Displays the loopback number and state and the line protocol state. The states are "Loopback *nn* is up", "Loopback *nn* is admin down, line protocol is down (admin down). "
Hardware	Displays "is Loopback".
Pluggable media	Displays "present" or "not present".
Interface index	Displays the interface index.
MTU	Displays the maximum transmission unit (MTU), in bytes.
LineSpeed Actual	Displays the actual line speed in Mb or "Nil".
LineSpeed Configured	Displays "Auto" or a value in Mb.
Last clearing of show interface counters:	In days, hours, and minutes, displays how much time elapsed since the last counter clear.
Queueing strategy	Displays "FIFO".
Primary Internet Address	Displays the primary Internet address.

The **show interface ethernet management** command displays the following information:

Output field	Description
LineSpeed Actual	Displays "100000baseT" (100Gb), "40000baseT" (40Gb), "25000baseT" (25Gb), "10000baseT" (10Gb), or "1000baseT" (1Gb).
Duplex	Displays "Half" or "Full".
LineSpeed Configured	Displays "Auto" or a value in Mb.
oper-status	Displays "up" or "down".
ip address	Displays "static" or "dynamic" and the IPv4 address.
ip gateway-address	Displays the IPv4 gateway address.
ipv6 ipv6-address	Displays the IPv6 address.
ipv6 ipv6-gateways	Displays the IPv6 gateway address.

The **show interface ethernet switchport** command displays the following information:

Output field	Description
Interface name	Displays "Ethernet *slot* **/** *port*" or "Port-channel *nn*".
Switchport mode	Displays "access", "trunk", or "trunk-no-default-native".
Ingress filter	Displays "enable".
Acceptable frame types	Displays "vlan-tagged only", "vlan-untagged only", or "all".
Native Vlan	Displays the ID number of the native VLAN.
Active Vlans	Displays ID numbers of the active VLANs.
MAC learn disable Vlans	Displays VLANs for which MAC learning is disabled.

The **show interface trunk** command displays the following information:

Output field	Description
Port	Displays the Ethernet ports by *slot* **/** *port*.
Vlans Allowed on Trunk	Displays "Nil" or a list of the VLANs allowed on the trunk.

Examples

The following example displays detailed information for a specified Ethernet interface.

```
device# show interface ethernet 3/4
Ethernet 3/4 is up, line protocol is up (connected)
Hardware is Ethernet, address is 768d.f804.ca08
    Current address is 768d.f804.ca08
Pluggable media present
Interface index (ifindex) is 207650816
MTU 1548 bytes
IP MTU 1500 bytes
10G Interface
LineSpeed Actual     : 10000 Mbit
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Forward LACP PDU: Disable
Route Only: Disabled
Last clearing of show interface counters: 11:59:37
Queueing strategy: fifo
 Primary Internet Address is 12.2.1.2/24 broadcast is 12.2.1.255
Receive Statistics:
    45756 packets, 34003184 bytes
    Unicasts: 9094, Multicasts: 36650, Broadcasts: 12
    64-byte pkts: 1438, Over 64-byte pkts: 8113, Over 127-byte pkts: 1786
    Over 255-byte pkts: 10132, Over 511-byte pkts: 8432, Over 1023-byte pkts: 15855
    Over 1518-byte pkts(Jumbo): 0
    Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
    Errors: 0, Discards: 0
Transmit Statistics:
    33405 packets, 25357172 bytes
    Unicasts: 10232, Multicasts: 23162, Broadcasts: 10
    Underruns: 0
    Errors: 0, Discards: 0
Rate info:
    Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 0.000333 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Route-Only Packets Dropped: 0
```

The following example displays detailed information for a specified management interface.

```
device# show interface management 1
interface Management 1
 line-speed actual "1000baseT, Duplex: Full"
 line-speed configured Auto
 oper-status up
 ip address "static 10.17.110.59/20"
 ip gateway-address 10.17.114.1
 ipv6 ipv6-address [  ]
 ipv6 ipv6-gateways [ fe80::21b:edff:fe0b:9000 fe80::21b:edff:fe0b:3c00 ]
```

The following example displays detailed information for a specified loopback interface.

```
device# show interface loopback 1
Loopback 1 is up, line protocol is up
Hardware is Loopback
Pluggable media not present
Interface index (ifindex) is 1476395009
IP MTU 1500 bytes
LineSpeed Actual     : Nil
LineSpeed Configured : Auto
Last clearing of show interface counters: 00:00:23
Queueing strategy: fifo
 Primary Internet Address is 50.1.1.1/32
```

The following example displays details of a specified Layer 2 interface.

```
device# show interface switchport 1/15
 Interface name          : Ethernet 1/15
 Switchport mode         : trunk
 Ingress filter          : enable
 Acceptable frame types  : vlan-tagged only
 Native Vlan             : 1
 Active Vlans            : 1-201
 MAC learn disable Vlans : -
```

History

Release version	Command history
18x.1.00	This command was introduced.

show interface stats brief

Displays a brief list of interface statistics.

Syntax

show interface stats brief

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

show interface stats detail

Displays a detailed list of interface statistics.

Syntax

show interface stats detail

show interface stats detail interface { **ethernet** *slot* **/** *port* | **port-channel** *index* }

Parameters

interface

Specifies what type of interface is displayed.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel

Specifies a port channel interface.

index

Specifies the port channel number. Depending on the platform, the number ranges from 1 through 512.

Modes

Privileged EXEC mode

Examples

The following example displays detailed statistics for a specified Ethernet interface.

```
device# show interface stats detail interface ethernet 2/60

 Interface Ethernet 2/60 statistics (ifindex 413007892)
                                RX                              TX
             Packets        15069980                        38855
               Bytes     18850526482                      4892750
            Unicasts        15027331                            1
          Multicasts           42423                        38853
          Broadcasts             210                            1
              Errors               0                            0
            Discards               0                            0
            Overruns               0       Underruns            0
               Runts               0
             Jabbers               0
                 CRC               0
        64-byte pkts               0
   Over 64-byte pkts            7092
  Over 127-byte pkts         1876809
  Over 255-byte pkts         1229162
  Over 511-byte pkts             168
 Over 1023-byte pkts        11956733
 Over 1518-byte pkts               0
           Mbits/Sec        0.174379                     0.001014
          Packet/Sec              94                            0
           Line-rate           0.00%                        0.00%
```

The following example displays detailed statistics for a specified port channel.

```
device# show interface stats detail interface port-channel 2

 Interface Port-channel 2 statistics (ifindex 671088642)
                                RX                              TX
             Packets               0                            0
               Bytes               0                            0
            Unicasts               0                            0
          Multicasts               0                            0
          Broadcasts               0                            0
              Errors               0                            0
            Discards               0                            0
            Overruns               0       Underruns            0
               Runts               0
             Jabbers               0
                 CRC               0
        64-byte pkts               0
   Over 64-byte pkts               0
  Over 127-byte pkts               0
  Over 255-byte pkts               0
  Over 511-byte pkts               0
 Over 1023-byte pkts               0
 Over 1518-byte pkts               0
           Mbits/Sec        0.000000                     0.000000
          Packet/Sec               0                            0
           Line-rate           0.00%                        0.00%
```

History

Release version	Command history
18x.1.00	This command was introduced.

show interface stats utilization-watermark

Displays high and low—incoming and outgoing—current hour, previous hour, current 24-hour, and previous 24-hour traffic watermarks.

Syntax

show interface stats utilization-watermark

show interface stats utilization-watermark interface { **ethernet** *slot* **/** *port* | **port-channel** *index* }

Parameters

interface
Specifies what type of interface to display.

ethernet
Specifies an Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *index*
Specifies a port-channel number. Depending on the platform, valid values range from 1 through 1024.

Modes

Privileged EXEC mode

Usage Guidelines

You can filter the results by interface or by line card.

Command Output

The **show interface stats utilization-watermark** command displays the following information:

Output field	Description
Cur1Hr-InHigh	Displays the high watermark for incoming traffic during the current hour.
Cur1Hr-InLow	Displays the low watermark for incoming traffic during the current hour.
Cur1Hr-OutHigh	Displays the high watermark for outgoing traffic during the current hour.
Cur1Hr-OutLow	Displays the low watermark for outgoing traffic during the current hour.
Last1Hr-InHigh	Displays the high watermark for incoming traffic during the previous hour.
Last1Hr-InLow	Displays the low watermark for incoming traffic during the previous hour.
Last1Hr-OutHigh	Displays the high watermark for outgoing traffic during the previous hour.
Last1Hr-OutLow	Displays the low watermark for outgoing traffic during the previous hour.

Output field	Description
Cur24Hr-InHigh	Displays the high watermark for incoming traffic during the current 24 hours.
Cur24Hr-InLow	Displays the low watermark for incoming traffic during the current 24 hours.
Cur24Hr-OutHigh	Displays the high watermark for outgoing traffic during the current 24 hours.
Cur24Hr-OutLow	Displays the low watermark for outgoing traffic during the current 24 hours.
Last24Hr-InHigh	Displays the high watermark for incoming traffic during the previous 24 hours.
Last24Hr-InLow	Displays the low watermark for incoming traffic during the previous 24 hours.
Last24Hr-OutHigh	Displays the high watermark for outgoing traffic during the previous 24 hours.
Last24Hr-OutLow	Displays the low watermark for outgoing traffic during the previous 24 hours.

Examples

The following example displays utilization watermarks for a specified Ethernet interface.

```
device# show interface stats utilization-watermark interface ethernet 1/1

 Starting time of watermark windows:
 Cur1Hr : Apr  4 08:11:19       Cur24Hr : Apr  4 03:11:18

 Interface eth1/1 statistics watermark
                           Mbits/Sec         Pkts/Sec             Time

    Cur1Hr-InHigh   :        0.000000               0               00:00:00
    Cur1Hr-InLow    :        0.000000               0               00:00:00
    Cur1Hr-OutHigh  :        0.000000               0               00:00:00
    Cur1Hr-OutLow   :        0.000000               0               00:00:00
    Last1Hr-InHigh  :        0.000000               0               00:00:00
    Last1Hr-InLow   :        0.000000               0               00:00:00
    Last1Hr-OutHigh :        0.000000               0               00:00:00
    Last1Hr-OutLow  :        0.000000               0               00:00:00
    Cur24Hr-InHigh  :        0.000000               0               00:00:00
    Cur24Hr-InLow   :        0.000000               0               00:00:00
    Cur24Hr-OutHigh :        0.000000               0               00:00:00
    Cur24Hr-OutLow  :        0.000000               0               00:00:00
    Last24Hr-InHigh :        0.000000               0               00:00:00
    Last24Hr-InLow  :        0.000000               0               00:00:00
    Last24Hr-OutHigh:        0.000000               0               00:00:00
    Last24Hr-OutLow :        0.000000               0               00:00:00
```

History

Release version	Command history
18x.1.00	This command was introduced.

show interface status

Displays the status of all device interfaces.

Syntax

show interface status

Modes

Privileged EXEC mode

Command Output

The **show interface status** command displays the following information:

Output field	Description
Port	Displays the physical port or port channel.
Status	Displays the port status. The states are "adminDown", "notconnected", "connected (up)", or "sfpAbsent".
Mode	Displays "access" or "trunk".
Speed	Displays the speed of the Ethernet interface, in Gb.
Type	Displays 1G-SFP, 10G-SFP-LR, 10G-SFP-SR, 10G-SFP-SX, 40G-QSFP, or 100G.
Description	Displays a Description defined for the port.

Examples

The following example displays the status of all device interfaces.

```
device# show interface status
--------------------------------------------------------------------------------
Port         Status          Mode       Speed    Type            Description
--------------------------------------------------------------------------------
Eth 1/1      adminDown       --         --       --
Eth 1/2      adminDown       --         --       --
Eth 1/3      adminDown       --         --       --
...
Eth 1/15     notconnected    --         --       40G-QSFP                      -
...
Eth 3/4      connected (up)  --         10G      10G-SFP-SR
(output
               truncated)
```

History

Release version	Command history
18x.1.00	This command was introduced.

show inventory

Displays the hardware inventory of the device.

Syntax

show inventory [**chassis** | **fan** | **module** | **powerSupply**]

Parameters

chassis
Displays information about the chassis.

fan
Displays information about the fan.

module
Displays information about the module.

powerSupply
Displays information about the power supply.

Modes

Privileged EXEC mode

Examples

The following is an example of typical command output.

History

Release version	Command history
18x.1.00	This command was introduced.

show ip arp inspection

Displays Dynamic ARP Inspection (DAI) information for one or more VLANs.

Syntax

show ip arp inspection [**vlan** *vlan-range*]

Parameters

vlan *vlan-range*

Specifies a VLAN, multiple VLANs (separated by commas with no spaces), a range of VLANs, or a combination of specified VLANs and ranges of VLANs. Valid values are from 1 through 4090.

Modes

Privileged EXEC mode

Command Output

The **show ip arp inspection** command displays the following information:

Output field	Description
Vlan	Displays the VLAN name.
Configuration	Displays Enabled (**ip arp inspection**) or Disabled (**no ip arp inspection**).
Operation	Displays "Active" if ARP configuration is successfully saved to the database. "Inactive" indicates one of the following conditions: • The "Configuration" value is "Disabled". • There is an internal issue that prevents successful application of ACLs
ACL Match	Displays the name of the ARP ACL that is applied.
ACL Logging	Does not display a value.

Examples

The following example displays DAI information for all VLANs.

```
device# show ip arp inspection
  Vlan  Configuraton     Operation     ACL Match   ACL Logging
-------------------------------------------------------------------------------
     1       Enabled        Active
    10      Disabled      Inactive
   100       Enabled        Active          acl1
    20      Disabled      Inactive
   200      Disabled      Inactive
  2000       Enabled        Active          acl1
```

The following example displays DAI information for specified VLANs and a range of VLANs.

```
device# show ip arp inspection vlan 1,100,200-2000
  Vlan  Configuraton     Operation     ACL Match   ACL Logging
-------------------------------------------------------------------------------
     1       Enabled        Active
   100       Enabled        Active          acl1
  1000       Enabled        Active
   200      Disabled      Inactive
  2000       Enabled        Active          acl1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip arp inspection interfaces

Displays a list of trusted interfaces on VLANs enabled for Dynamic ARP Inspection (DAI).

Syntax

show ip arp inspection interfaces [**ethernet** *slot* **/** *port* | **port-channel** *index*]

Parameters

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel interface.

Modes

Privileged EXEC mode

Usage Guidelines

On VLANs enabled for Dynamic ARP Inspection (DAI), interfaces not listed in the command output are untrusted.

Command Output

The **show ip arp inspection interfaces** command displays the following information:

Output field	Description
Interface	Displays a prefix specifying the interface type, followed by the interface identifier.
Trust State	Displays "Trusted".

Examples

The following example displays all trusted interfaces.

```
device# show ip arp inspection interfaces
Interface     Trust State
--------------------------------------
Po 60        Trusted
Eth 0/1       Trusted
Eth 0/2       Trusted
--------------------------------------

All other interfaces are untrusted.
```

The following example displays the trust state of Ethernet interface 0/1.

```
device# show ip arp inspection interfaces ethernet 0/1
Interface     Trust State
--------------------------------------
Eth 0/1       Trusted
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip arp suppression-cache

Displays IPv4 ARP-suppression information.

Syntax

show ip arp suppression-cache [**summary**]

show ip arp suppression-cache bridge-domain *bridge-domain-id*

show ip arp suppression-cache vlan *vlan-id*

Parameters

summary

Specifies summary format.

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Command Output

The **show ip arp suppression-cache** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
IP	Displays the IP address.
Mac	Displays the MAC address.
Interface	Displays the interface type and ID. "Tu" represents a tunnel interface, followed by the end-point IP.
Age	In hh:mm:ss format, displays the time since the most recent renewal of a dynamic entry. For a static entry, displays "Never".
Flags	Displays "L" (locally learned adjacency), "R" (remote learned adjacency), or RS (remote static adjacency).

Examples

The following example displays the results of the basic form of this command.

```
device# show ip arp suppression-cache
Flags: L  - Locally Learnt Adjacency
       R  - Remote Learnt Adjacency
       RS - Remote Static Adjacency
Vlan/Bd  IP         Mac            Interface                  Age       Flags
-------------------------------------------------------------------------------
4003 (V) 40.3.1.100 00ec.4003.3401 Eth 0/41                   03:09:44  L
4003 (V) 40.3.1.101 00ec.4003.3402 Eth 0/41                   03:09:44  L
4007 (V) 40.7.1.100 00ec.4007.4401 Tu 61441 (114.114.114.114) Never     R
4007 (V) 40.7.1.101 00ec.4007.4402 Tu 61441 (114.114.114.114) Never     R
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip arp suppression-statistics

Displays IPv4 ARP-suppression statistics.

Syntax

show ip arp suppression-statistics

show ip arp suppression-statistics bridge-domain *bridge-domain-id*

show ip arp suppression-statistics vlan *vlan-id*

Parameters

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Command Output

The **show ip arp suppression-statistics** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
Forwarded	Displays the number of packets forwarded.
Suppressed	Displays the number of packets suppressed.
Remote-arp Proxy	Displays the number of packets for which the device has sent proxy-ARP replies.

Examples

The following example displays the results of the basic form of this command.

```
device# show ip arp suppression-statistics
Vlan/Bd       Forwarded     Suppressed    Remote-arp Proxy
-------------------------------------------------------
110 (V)       0             24            0
254 (V)       3             10            0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip arp suppression-status

Displays the IPv4 ARP-suppression status.

Syntax

show ip arp suppression-status

show ip arp suppression-status bridge-domain *bridge-domain-id*

show ip arp suppression-status vlan *vlan-id*

Parameters

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Command Output

The **show ip arp suppression-status** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
Configuration	Displays "Enabled" or "Disabled".
Evpn-Register	Displays "Yes" if the VLAN is extended through EVPN or "No" if it is not extended.
Operation	Displays "Active" or "Inactive".

Examples

The following example displays the results of the basic form of this command.

```
device# show ip arp suppression-status
Vlan/Bd          Configuration   Evpn-Register Operation
-------------------------------------------------------------------------------
4003 (V)         Enabled         Yes           Active
4005 (V)         Disabled        No            Inactive
4006 (V)         Enabled         Yes           Active
4007 (V)         Enabled         Yes           Active
4008 (V)         Disabled        No            Inactive
4013 (V)         Enabled         Yes           Active
4015 (V)         Disabled        No            Inactive
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp

Displays BGP4 route information.

Syntax

show ip bgp

show ip bgp *ip-addr* [*/prefix*]

show ip bgp *ip-addr* [*/prefix*] [**longer-prefixes**] [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation, with an optional mask.

/prefix

IPv4 mask length in CIDR notation.

longer-prefixes

Filters prefixes equal to or greater than that specified by *prefix*.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays sample output from the **show ip bgp** command.

```
device# show ip bgp

Total number of BGP Routes: 4
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
*>i 110.110.110.0/24   50.50.50.10                150        0      i
*x  110.110.110.0/24   20.20.20.10                100        0      200 i
*   110.110.110.0/24   30.30.30.10                100        0      300 i
*   110.110.110.0/24   40.40.40.10                100        0      400 i
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp attribute-entries

Displays BGP4 route-attribute entries that are stored in device memory.

Syntax

show ip bgp attribute-entries [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4 attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4 route-attribute entries that are stored in device memory.

Examples

The following example show sample output for the **show ip bgp attribute-entries** command.

```
device# show ip bgp attribute-entries
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp dampened-paths

Displays all BGP4 dampened routes..

Syntax

show ip bgp dampened-paths [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ip bgp dampened-paths** command.

```
device# show ip bgp dampened-paths

    Status Code  >:best d:damped h:history *:valid
    Network            From            Flaps Since       Reuse       Path
*d  110.110.114.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
*d  110.110.113.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
*d  110.110.112.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
*d  110.110.111.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
*d  110.110.110.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp filtered-routes

Displays BGP4 filtered routes that are received from a neighbor or peer group.

Syntax

show ip bgp filtered-routes [**detail**] [*ip-addr* { **/** *mask* } [**longer-prefixes**]] | **as-path-access-list** *name* | **prefix-list** *name*] [**vrf** *vrf-name*]

Parameters

detail
Optionally displays detailed route information.

ip-addr
IPv4 address of the destination network in dotted-decimal notation.

mask
(Optional) IPv4 mask of the destination network in CIDR notation.

longer-prefixes
Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

as-path-access-list *name*
Specifies an AS-path ACL. The name must be between 1 and 32 ASCII characters in length.

prefix-list *name*
Specifies an IP prefix list. The name must be between 1 and 32 ASCII characters in length.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays BGP4 filtered routes.

```
device# show ip bgp filtered-routes 10.11.12.13 prefix-list myprefixlist
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp flap-statistics

Displays BGP4 route-dampening statistics for all dampened routes with a variety of options.

Syntax

show ip bgp flap-statistics

show ip bgp flap-statistics *ip-addr* { **/** *mask* } [**longer-prefixes** [**vrf** *vrf-name*] | **vrf** *vrf-name*]

show ip bgp flap-statistics neighbor *ip-addr* [**vrf** *vrf-name*]

show ip bgp flap-statistics regular-expression *name* [**vrf** *vrf-name*]

show ip bgp flap-statistics vrf *vrf-name*

Parameters

ip-addr
IPv4 address of a specified route in dotted-decimal notation.

mask
IPv4 mask of a specified route in CIDR notation.

longer-prefixes
Displays statistics for routes that match the specified route or have a longer prefix than the specified route.

vrf *vrf-name*
Specifies a VRF instance.

neighbor
Displays flap statistics only for routes learned from the specified neighbor.

ip-addr
IPv4 address of the neighbor.

regular-expression
Specifies a regular expression in the display output on which to filter.

name
Name of an AS-path filter or regular expression.

Modes

Privileged EXEC mode

Examples

The following example displays flap statistics for a neighbor.

```
device# show ip bgp flap-statistics neighbor 10.11.12.13
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors

Displays configuration information and statistics for BGP4 neighbors.

Syntax

show ip bgp neighbors [*ip-addr*]

show ip bgp neighbors last-packet-with-error [**vrf** *vrf-name*]

show ip bgp neighbors routes-summary [**vrf** *vrf-name*]

show ip bgp neighbors vrf *vrf-name*

Parameters

ip-addr
: Address of a neighbor in IPv4 address format.

last-packet-with-error
: Displays the last packet with an error.

route-summary
: Displays routes received, routes accepted, number of routes advertised by peer, and so on.

vrf *vrf-name*
: Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP4 neighbors of a device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from the default values are shown.

Examples

The following example shows sample output from the **show ip bgp neighbors** command.

```
device# show ip bgp neighbors

    '+': Data in InQueue '>': Data in OutQueue '-': Clearing
    '*': Update Policy 'c': Group change 'p': Group change Pending
    'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

1   IP Address: 60.60.60.20, AS: 200 (IBGP), RouterID: 60.60.60.20, VRF: default-vrf
    State: ESTABLISHED, Time: 4h3m28s, KeepAliveTime: 60, HoldTime: 180
       KeepAliveTimer Expire in 0 seconds, HoldTimer Expire in 159 seconds
    Minimal Route Advertisement Interval: 0 seconds
       RefreshCapability: Received
    Address Family : IPV4 Unicast
       Configured with Add-Path(send receive)capability
       Received Add-Path (send receive)capability in open msg
       Negotiated Add-Path(send receive)capability
    Messages:    Open        Update      KeepAlive   Notification   Refresh-Req
       Sent    : 1           1           275         0              0
       Received: 1           1           275         0              0
    Last Update Time: NLRI       Withdraw          NLRI       Withdraw
                  Tx: 4h3m28s    ---           Rx: 4h3m28s    ---
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors advertised-routes

Displays the routes that the device has advertised to the neighbor during the current BGP4 session.

Syntax

show ip bgp neighbors *ip-addr* **advertised-routes** [**detail** | **/** *mask-bits*] [**vrf** *vrf-name*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

detail
Displays details of advertised routes.

mask-bits
Number of mask bits in CIDR notation.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays the details of advertised routes.

```
device# show ip bgp neighbors 123.123.123.3 advertised-routes

       There are 5 routes advertised to neighbor 123.123.123.3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix           Next Hop        MED        LocPrf     Weight Status
1      110.110.110.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
2      110.110.111.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
3      110.110.112.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
4      110.110.113.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
5      110.110.114.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors flap-statistics

Displays the route flap statistics for routes received from or sent to a BGP4 neighbor.

Syntax

show ip bgp neighbors *ip-addr* **flap-statistics** [**vrf** *vrf-name*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows flap statistics.

```
device# show ip bgp neighbors flap-statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors last-packet-with-error

Displays information about the last packet that contained an error from any of a device's neighbors.

Syntax

show ip bgp neighbors *ip-addr* **last-packet-with-error** [**decode**] [**vrf** *vrf-name*]

Parameters

ip-addr

IP address of a neighbor in dotted-decimal notation.

decode

Decodes last packet that contained an error from any of a device's neighbors.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ip bgp neighbors last-packet-with-error** command when no packet from a specified neighbor contained an error.

```
device# show ip bgp neighbors 123.123.123.3 last-packet-with-error

 Received Message Length: 45
 BGP Message:
  0xffffffff  0xffffffff  0xffffffff  0xffffffff  0x002d0104
  0x014b00b4  0x09090909  0x10020601  0x04010000  0x01020202
  0x00020280  0x00

 BGP Header
  Marker:   0xffffffff  0xffffffff  0xffffffff  0xffffffff
  Message Length: (0x002d) 45
  Message Type: (0x01) OPEN

 OPEN Message
 Version: (0x04) 4
 AS Number: (0x014b) 331
 Hold Time: (0x00b4) 180
 BGP Identifier: (0x09090909) 9.9.9.9
 Optional Parameter length: (0x10) 16

 OPEN message optional parameters
  Parameter Type: (0x02) Capability
  Parameter Length: (0x06) 6
   Capability Type: (0x01) MULTIPROTOCOL EXTENSIONS
   Capability Length: (0x04) 4
   AFI: (0x0100) Unknown(256)
   Reserved: (0x00) 0
   SAFI: (0x01) Unicast

  Parameter Type: (0x02) Capability
  Parameter Length: (0x02) 2
   Capability Type: (0x02) ROUTE REFRESH(new)
   Capability Length: (0x00) 0

  Parameter Type: (0x02) Capability
  Parameter Length: (0x02) 2
   Capability Type: (0x80) ROUTE REFRESH(old)
   Capability Length: (0x00) 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

Syntax

show ip bgp neighbors *ip-addr* **received**

show ip bgp neighbors *ip-addr* **received detail** [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **received prefix-filter** [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **vrf** *vrf-name*

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

detail
Displays detailed information for ORFs received from BGP4 neighbors of the device.

vrf *vrf-name*
Specifies a VRF instance.

prefix-filter
Displays the results for ORFs that are prefix-based.

Modes

Privileged EXEC mode

Examples

The following example displays output for the **show ip bgp neighbors received** command.

```
device# show ip bgp neighbors 10.5.5.6 received
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors received-routes

Lists all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

Syntax

show ip bgp neighbors *ip-addr* **received-routes** [**detail**] [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Displays detailed route information.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays output for the **show ip bgp neighbors received-routes** command.

```
device# show ip bgp neighbors 160.160.160.10 received-routes

       There are 5 received routes from neighbor 160.160.160.10
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      110.110.110.0/24    160.160.160.10   0         100        0      BE
         AS_PATH: 111
2      110.110.111.0/24    160.160.160.10   0         100        0      BE
         AS_PATH: 111
3      110.110.112.0/24    160.160.160.10   0         100        0      BE
         AS_PATH: 111
4      110.110.113.0/24    160.160.160.10   0         100        0      BE
         AS_PATH: 111
5      110.110.114.0/24    160.160.160.10   0         100        0      BE
         AS_PATH: 111
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors rib-out-routes

Displays information about BGP4 outbound RIB routes.

Syntax

show ip bgp neighbors *ip-addr* **rib-out-routes** *ip-addr mask* [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **rib-out-routes detail** *ip-addr mask* [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **rib-out-routes detail** [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **rib-out-routes** [**vrf** *vrf-name*]

Parameters

ip-addr

IP address of a neighbor in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

detail

Displays detailed RIB route information.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ip bgp neighbors rib-out-routes** command.

```
device# show ip bgp neighbors 123.123.123.3 rib-out-routes

       There are 5 RIB_out routes for neighbor 123.123.123.3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110.110.110.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
2      110.110.111.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
3      110.110.112.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
4      110.110.113.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
5      110.110.114.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4 neighbors.

Syntax

show ip bgp neighbors *ip-addr* **routes**

show ip bgp neighbors *ip-addr* **routes** { **best** | **not-installed-best** | **unreachable** } [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **routes detail** { **best** | **not-installed-best** | **unreachable** } [**vrf** *vrf-name*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

best
Displays routes received from the neighbor that are the best BGP4 routes to their destination.

not-installed-best
Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in the route table because the device received better routes from other sources.

unreachable
Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays

```
device# show ip bgp neighbors 10.11.12.13 routes best vrf red
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4 neighbors.

Syntax

show ip bgp neighbors *ip-addr* **routes-summary** [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays route summary information received in UPDATE messages.

```
device# show ip bgp neighbors routes-summary
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp peer-group

Displays peer-group information.

Syntax

show ip bgp peer-group *peer-group-name* [**vrf** *vrf-name*]

Parameters

peer-group-name
Specifies a peer group name.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Only the parameters that have values different from their defaults are listed.

Examples

This example shows sample output from the **show ip bgp peer-group** command.

```
device# show ip bgp peer-group
1   BGP peer-group is pg
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Members:
       IP Address: 1.1.1.1, AS: 100
       IP Address: 1::1, AS: 100

2   BGP peer-group is pg6
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Currently there are no members
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp routes

Displays BGP4 route information that is filtered by the table entry at which the display starts.

Syntax

show ip bgp routes [*num* | *ip-address/prefix* | **age** *num* | **as-path-access-list** *name* | **best** | **cidr-only** | **community-access-list** *name* | **community-reg-expression** *expression* | **detail** | **local** | **neighbor** *ip-addr* | **nexthop** *ip-addr* | **no-best** | **not-installed-best** | **prefix-list** *string* | **regular-expression** *name* | **route-map** *name* | **summary** | **unreachable**] [**vrf** *vrf-name*]

Parameters

num
Table entry at which the display starts.

ip-address/prefix
Table entry at which the display starts.

age
Displays BGP4 route information that is filtered by age.

as-path-access-list *name*
Displays BGP4 route information that is filtered by autonomous system (AS)-path access control list (ACL). The name must be between 1 and 32 ASCII characters in length.

best
Displays BGP4 route information that the device selected as best routes.

cidr-only
Displays BGP4 routes whose network masks do not match their class network length.

community-access-list *name*
Displays BGP4 route information for an AS-path community access list. The name must be between 1 and 32 ASCII characters in length.

community-reg-expression *expression*
Displays BGP4 route information for an ordered community-list regular expression.

detail
Displays BGP4 detailed route information.

local
Displays BGP4 route information about selected local routes.

neighbor *ip-addr*
Displays BGP4 route information about selected BGP neighbors.

nexthop *ip-addr*
Displays BGP4 route information about routes that are received from the specified next hop.

no-best
Displays BGP4 route information that the device selected as not best routes.

not-installed-best
Displays BGP4 route information about best routes that are not installed.

prefix-list *string*
Displays BGP4 route information that is filtered by prefix list. The string must be between 1 and 32 ASCII characters in length.

regular-expression *name*
Displays BGP4 route information about routes that are associated with the specified regular expression.

route-map *name*
Displays BGP4 route information about routes that use the specified route map.

summary
Displays BGP4 summary route information.

unreachable
Displays BGP4 route information about routes whose destinations are unreachable through any of the BGP4 paths in the BGP4 route table.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows output from the **show ip bgp routes** command.

```
device# show ip bgp routes

Total number of BGP Routes: 2000
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      150.150.150.0/24   103.103.1.1     2          100        0      BEx
         AS_PATH: 201
2      150.150.150.0/24   103.103.2.1     3          100        0      E
         AS_PATH: 202
3      150.150.150.0/24   103.103.3.1     4          100        0      E
         AS_PATH: 203
4      150.150.150.0/24   103.103.4.1     5          100        0      E
         AS_PATH: 204
5      150.150.150.0/24   103.103.5.1     6          100        0      E
--More--, next page: Space, next line: Return key, quit: Control-c^C
SLX#
```

This example shows sample output from the **show ip bgp routes** command when an IP address is specified.

```
device# show ip bgp routes  50.55.55.10

Number of BGP Routes matching display condition : 8
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      10.55.55.0/24      16.1.1.1         0         100        0      BME
         AS_PATH: 65200 65100
2      10.55.55.0/24      17.1.1.1         0         100        0      ME
         AS_PATH: 65200 65100
3      10.55.55.0/24      19.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
4      10.55.55.0/24      21.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
5      10.55.55.0/24      18.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
6      10.55.55.0/24      22.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
7      10.55.55.0/24      23.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
8      10.55.55.0/24      20.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
       Last update to IP routing table: 0h28m14s       Route is advertised to 7 peers:
        17.1.1.1(65200)                          18.1.1.1(65200)
19.1.1.1(65200)
        20.1.1.1(65200)                          21.1.1.1(65200)
22.1.1.1(65200)
        23.1.1.1(65200)
```

This example shows sample output from the **show ip bgp routes** command when the **summary** option is specified.

```
device# show ip bgp routes summary

  Total number of BGP routes (NLRIs) Installed     : 1
  Distinct BGP destination networks                : 1
  Filtered bgp routes for soft reconfig            : 0
  Routes originated by this router                 : 1
  Routes selected as BEST routes                   : 1
  Routes Installed as BEST routes                  : 1
  BEST routes not installed in IP forwarding table : 0
  Unreachable routes (no IGP route for NEXTHOP)    : 0
  IBGP routes selected as best routes              : 0
  EBGP routes selected as best routes              : 0
  BEST routes not valid for IP forwarding table    : 0
```

The following example shows output from the **show ip bgp routes** command when the **detail** option is specified.

```
device# show ip bgp routes detail

Total number of BGP Routes: 1600
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
1       Prefix: 150.150.150.0/24, Rx path-id:0x00000001, Tx path-id:0x00000001, rank:0x00000001,
Status: BEx,  Age: 0h54m0s
         NEXT_HOP: 104.1.1.4, Metric: 0, Learned from Peer: 104.1.1.4 (444)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: igp,  Weight: 0,  GROUP_BEST: 1
         AS_PATH: 444 201
2       Prefix: 150.150.150.0/24, Rx path-id:0x00010001, Tx path-id:0x00000003, rank:0x00000002,
Status: E,  Age: 0h53m50s
         NEXT_HOP: 104.1.1.4, Metric: 0, Learned from Peer: 104.1.1.4 (444)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: igp,  Weight: 0,  GROUP_BEST: 0
         AS_PATH: 444 202
--More--, next page: Space, next line: Return key, quit: Control-c^C
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp routes community

Displays BGP4 route information that is filtered by community and other options.

Syntax

show ip bgp routes community { *num* | **internet** | **local-as** | **no-advertise** | **no-export** } [**vrf** *vrf-name*]

Parameters

community
Displays routes filtered by a variety of communities.

num
Specific community member.

internet
Displays routes for the Internet community.

local-as
Displays routes for a local sub-AS within the confederation.

no-advertise
Displays routes with this community that cannot be advertised to any other BGP4 devices at all.

no-export
Displays routes for the community of sub-ASs within a confederation.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows output from the **show ip bgp routes community** command when the **internet** keyword is used.

```
device# show ip bgp routes community internet
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip bgp summary

Displays BGP information such as the local autonomous system number (ASN), maximum number of routes supported, and some BGP4 statistics.

Syntax

show ip bgp summary [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays summary BGP information.

```
device# show ip bgp summary

BGP4 Summary
  Router ID: 4.4.4.4   Local AS Number: 65300
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 2
  Number of Neighbors Configured: 8, UP: 8
  Number of Routes Installed: 80088, Uses 7688448 bytes
  Number of Routes Advertising to All Neighbors: 70077 (10011 entries), Uses 600660 bytes
  Number of Attribute Entries Installed: 16, Uses 1664 bytes
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  16.1.1.1          65200       ESTAB     2h26m 8s    10011    0        1        0
  17.1.1.1          65200       ESTAB     2h26m 8s    10011    0        10010    0
  18.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
  19.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
  20.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
  21.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
  22.1.1.1          65200       ESTAB     2h26m 2s    10011    0        10011    0
  23.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
…
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip dhcp relay address interface

Displays IP DHCP relay addresses configured on supported interfaces.

Syntax

show ip dhcp relay address interface [**ethernet** *slot/port*| **ve** *interface number*]

Parameters

ethernet *slot/port*
Interface name in slot/port format.

ve *interface number*
Interface name in slot/port format.

Modes

Privileged EXEC mode

Examples

The following example displays DHCP relay address(es) configured on interface 1/4:

```
device# show ip dhcp relay address interface ethernet 1/4
---------                      -------------                    --------
Interface                      Relay Address                    VRF Name
---------                      -------------                    --------
Eth 1/4                            10.3.4.5                          blue
Eth 1/4                              10.5.1.1                             default-vrf
```

The following example displays DHCP relay address(es) configured on Ve 300:

```
device# show ip dhcp rel add int ve 300

---------                  -------------                    --------
Interface                  Relay Address                    VRF Name
---------                  -------------                    --------
Ve 300                        10.0.1.2                       default-vrf
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip dhcp relay gateway

Displays IP DHCP Relay gateway addresses.

Syntax

show ip dhcp relay gateway {**interface** [**ethernet** *slot/port* | **Ve** *number*]}

Parameters

interface

The interface ethernet slot/port number or the Ve number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the gateway address configured on the switch or on the interface.

Examples

To display the gateway address configured on the switch:

```
device# show ip dhcp relay gateway
---------                    -------------
Interface                       Gateway Address
---------                    -------------
Eth 3/5                            10.1.1.1
Ve 100                          100.1.1.1
```

To display the gateway address configured on the interface:

```
device# show ip dhcp relay gateway interface ethernet 3/5
---------                    -------------
Interface                       Gateway Address
---------                    -------------
Eth 3/5                            10.1.1.1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip dhcp relay statistics

Displays the general information about the DHCP Relay function.

Syntax

show ip dhcp relay statistics

Modes

Privileged EXEC mode

Usage Guidelines

The **show ip dhcp relay statistics** command displays the following information about the IP DHCP Relay function for IP DHCP Relay addresses configured on the switch:

- DHCP Server IP Address configured in the switch.
- Number of DHCP DISCOVERY, OFFER, REQUEST, ACK, NAK, DECLINE, and RELEASE packets received.
- Number of DHCP client packets received (on port 67) and relayed by the Relay Agent.
- Number of DHCP server packets received (on port 67) and relayed by the Relay Agent.

DHCP unicast packets are forwarded directly per route. These packets are not trapped to the management module. As a result, the DHCP renewal Request/ACK and DHCP Release packets are not be counted toward statistics.

Examples

To display general information about the DHCP relay function:

```
device# show ip dhcp relay statistics
            DHCP Relay Statistics:
       ------------------------
Address         Disc.      Offer      Req.      Ack       Nak       Decline      Inform
-------         -----     -----       ----      ---       ---       -------       ------
10.1.0.1        400        100        2972      2968      0          0              0
20.2.0.1        400        100        2979      2975      0          0              0
30.3.0.1        400        100        3003      2998      0          0              0
40.4.0.1        400        100        3026      3018      0          0              0

Client Packets: 12780
Server Packets: 12359
Client Packets Dropped: 0
Server Packets Dropped: 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip igmp groups

Displays information related to learned groups in the IGMP protocol module.

Syntax

show ip igmp groups [**detail** | **interface** | **vlan** *vlan_id* | **bridge-domain** *bridge-domain_id*]

Parameters

detail
Displays detailed information.

interface
Specifies an interface type.

vlan *vlan_id*
Specifies a VLAN interface.

bridge-domain *bridge-domain_id*
Specifies a bridge-domain interface.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the IGMP database, including configured entries for either all groups on all interfaces, or all groups on specific interfaces, or specific groups on specific interfaces.

Examples

The following example displays the IP IGMP groups.

```
device# show ip igmp groups
Total Number of Groups: 2
IGMP Connected Group Membership
Group Address  Interface Uptime      Expires      Last Reporter   Version
225.1.1.1      vlan25    00:05:27     00:02:32     25.1.1.120       2
Member Ports: eth 2/24

225.1.1.2 bridge-domain20 00:05:27    00:02:32     25.1.1.120       2
Member Ports:  eth4/22.600 eth6/15.200  po2.200
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip igmp interface

Displays Layer 3 IGMP interface configuration information.

Syntax

show ip igmp interface [**ethernet** *slot/port* | **port-channel** | **Ve**]

Modes

Privileged EXEC mode

Examples

The following example displays IGMP protocol information for port-channel 1.

```
device# show ip igmp interface port-channel 1

Interface po1
 IGMP disabled
```

The following example displays the output for the **show ip igmp interface** command.

```
device# show ip igmp interface

Interface eth1/34
IGMP enabled
  IGMP query interval 125 seconds
  IGMP other-querier interval 255 seconds
  IGMP query response time 10 seconds
  IGMP last-member query interval 1
seconds
  IGMP immediate-leave enabled
  IGMP querier 0.0.0.0(this system)
  IGMP version 3

Interface Ve 10
IGMP enabled
 IGMP query interval 125 seconds
 IGMP other-querier interval 255 seconds
 IGMP query response time 10 seconds
 IGMP last-member query interval 1 seconds
 IGMP immediate-leave enabled
 IGMP querier 10.10.10.10(this system)
 IGMP version 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip igmp snooping

Displays IGMP snooping information.

Syntax

show ip igmp snooping [**mrouter vlan** *vlan_id* | **vlan** *vlan_id* | **bridge-domain** *bridge-domain_id*]

Parameters

mrouter vlan *vlan_id*
Specifies which VLAN interface to display the mrouter configuration related information.

vlan *vlan_id*
Specifies which VLAN interface to display the snooping configuration related information.

bridge-domain *bridge-domain_id*
Specifies which bridge-domain interface to display the snooping configuration related information.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **show ip igmp snooping** command to display IGMP snooping information, display multicast router port related information for the specified VLAN, or to display snooping statistics for the specified VLAN in the IGMP protocol module.

Examples

The following example displays IGMP snooping information.

```
device# show ip igmp snooping vlan 20
Vlan ID: 20
Multicast Router ports: eth4/2
Querier - Enabled,
IGMP Operation mode: IGMPv2
Is Fast-Leave Enabled : Disabled
Max Response time = 10
Last Member Query Interval = 1
Query interval = 125
Number of Multicast Groups: 1
Group: 225.0.0.1
Member Ports: eth4/2 eth6/15 po1
Mapped MAC address: 0100.5e00.0001


Bridge-domain ID: 20
Multicast Router ports: eth3/2.300
Querier - Enabled,
IGMP Operation mode: IGMPv2
Is Fast-Leave Enabled : Disabled
Max Response time = 10
Last Member Query Interval = 1
Query interval = 125
Number of Multicast Groups: 1
Group: 225.0.0.1
Member Ports: eth4/22.600 eth6/15.200 po2.200
Mapped MAC address: 0100.5e00.0001
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip igmp ssm-map

Displays the association between a configured prefix list and source address mapped to it.

Syntax

show ip igmp ssm-map

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show ip igmp ssm-map** command displays the following information:

Output field	Description
PrefixList Name	The name assigned to the prefix list.
Source Address	The source address IP.

Examples

The following example shows the association between a configured prefix list and source address mapped to it.

```
device# show ip igmp ssm-map

+-----------------------------------+-------------------+
|         PrefixList Name           |   Source Address  |
+-----------------------------------+-------------------+
   ssm-map-230-to-232                203.0.0.10
  ssm-map-233-to-234                204.0.0.11
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip igmp statistics bridge-domain

Displays IGMP statistics for the bridge-domain.

Syntax

show ip igmp statistics interface bridge-domain { **bridge-domain** | *bridge-domain_id* }

Parameters

bridge-domain *bridge-domain_id*
Specifies the bridge-domain ID.

Modes

Privileged EXEC mode

Examples

The following example displays the output for the **show ip igmp statistics interface bridge-domain** command.

```
device# show ip igmp statistics interface bridge-domain  20
IGMP packet statistics for all interfaces in bridge-domain 20:
IGMP Message type     Edge-Received Edge-Sent Edge-Rx-Errors
Membership Query       40             40              0
V1 Membership Report     40         40         0
V2 Membership Report     0          60         0
Group Leave          20          20          0
V3 Membership Report     0          0          0
PIM hello          0          0          0
IGMP Error Statistics:
Unknown types 0
Bad Length 0
Bad Checksum 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip igmp statistics interface

Displays IGMP statistics for an interface.

Syntax

show ip igmp statistics interface [**ethernet** *slot/port* | **port-channel** | **ve** *ve interface ID*]

Parameters

ethernet*slot/port*

Represents an Ethernet interface name in slot/port format.

port-channel *number*

Specifies a port-channel interface. The range is from 1 through 64.

ve *Ve interface number*

Specifies a virtual Ethernet (VE) interface number. The range is 1 - 4096.

Modes

Privileged EXEC mode

Examples

The following example displays the output of the **show ip igmp statistics interface** command.

```
device# show ip igmp statistics interface ve100

IGMP packet statistics for ve100:
IGMP Message type            Edge-Received  Edge-Sent  Edge-Rx-Errors
Membership Query                     0             229           0
V1 Membership Report                 0             0             0
V2 Membership Report                 0             0             0
Group Leave                          0             0             0
V3 Membership Report                 0             0             0
PIM hello                          456             0             0

IGMP Error Statistics:
Unknown types     0
Bad Length        0
Bad Checksum      0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip igmp statistics vlan

Displays information for a specific VLAN.

Syntax

show ip igmp statistics vlan *vlan-id*

Parameters

vlan-id

Specifies the VLAN-ID. The range is 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example displays the IP IGMP statistics on VLAN 1.

```
device# show ip igmp statistics interface vlan 1

IGMP packet statistics for all interfaces in vlan 1:
IGMP Message type     Edge-Received   Edge-Sent   Edge-Rx-Errors   ISL Received
Membership Query                  0           0                0              0
V1 Membership Report              0           0                0              0
V2 Membership Report              0           0                0              0
Group Leave                       0           0                0              0
V3 Membership Report              0           0                0              0
PIM hello                         0           0                0              0

IGMP Error Statistics:
Unknown types            0
Bad Length               0
Bad Checksum             0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip interface

Displays the IP address, status, and configuration for a specified interface.

Syntax

show ip interface { **brief** | **ethernet** *slot/port* }

Parameters

brief

Specifies a brief summary of IP interface status and configuration.

ethernet *slot/port*

Specifies an Ethernet slot and port.

Modes

Privileged EXEC mode

Usage Guidelines

You can also display a brief summary of such information for all interfaces.

Examples

The following example displays information about all of the interfaces in the summary format.

```
device# show ip interface brief
Interface              IP-Address          Vrf                        Status
Protocol
===========            ==========          ==========         ================
========
Port-channel 1         unassigned                               administratively down    down
Port-channel 2         unassigned                               administratively down    down
Ethernet 1/1           unassigned          default-vrf          up
down (UDLD blocked unidirectional link)
Ethernet 1/2           unassigned          default-vrf          up
down (Link-OAM blocked link)
Ethernet 1/3           unassigned          default-vrf          up                                  up
Ethernet 1/4           unassigned          default-vrf          administratively down    down
```

The following example displays the IP interface status of a specified Ethernet port.

```
device# show ip interface ethernet 1/1
 Ethernet 1/2 is up, line protocol is down (Link-OAM blocked link), Link-OAM is enabled
Hardware is Ethernet, address is 00e0.0c70.c005
    Current address is 00e0.0c70.c005
Pluggable media present
Interface index (ifindex) is 406880257
MTU 1548 bytes
10G Interface
LineSpeed Actual     : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Last clearing of show interface counters: 10:50:20
Queueing strategy: fifo
Receive Statistics:
    67181801 packets, 8867997496 bytes
    Unicasts: 67181799, Multicasts: 1, Broadcasts: 1
    64-byte pkts: 1, Over 64-byte pkts: 4, Over 127-byte pkts: 67181796
    Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
    Over 1518-byte pkts(Jumbo): 0
    Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
    Errors: 0, Discards: 0
Transmit Statistics:
    82627975 packets, 10906817712 bytes
    Unicasts: 82627873, Multicasts: 11, Broadcasts: 89
    Underruns: 0
    Errors: 0, Discards: 0
Rate info:
    Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 0.001014 Mbits/sec, 1 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:08:22
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip multicast snooping

Displays IP multicast snooping configuration information.

Syntax

show ip multicast snooping [**mcache***vlan interface* | **vlan** *vlan-id*]

Parameters

mcache

Specifies the multicast cache entries.

vlan interface

Specifies which VLAN's snooping mcache entries should be displayed.

vlan

Specifies the VLAN.

vlan-id

Specifies the VLAN-ID.

Modes

User EXEC mode

Examples

The following example displays the output for the **show ip multicast snooping mcache** command.

```
device# show ip multicast snooping mcache
Flags : V2|V3 : IGMP Receiver, P_G : PIM (*,G) Join, P_SG: PIM (S,G) Join
VlanID : 25
-------------
1(*, 225.1.1.1 )00:02:15NumOIF: 1
Outgoing Ports:
eth2/24       Flags: 0x14 ( V2)  00:02:15/126s
```

The following output displays v3 flag for entries learned through the IGMPv3 report.

```
device# show ip multicast snooping mca
Flags : V2|V3 : IGMP Receiver, P_G : PIM (*,G) Join, P_SG: PIM (S,G) Join
                 BR : PIM Blocked RPT
 Vlan ID : 10
 -------------
1     (20.20.20.20, 232.0.0.10 )  22:37:48    NumOIF: 1
       Outgoing Ports:
               eth1/34        Flags: 0x24 ( V3)  00:00:08/252s
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf

Displays OSPF information.

Syntax

show ip ospf [**vrf** *name*]

Parameters

vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ip ospf** command.

```
device# show ip ospf
OSPF Version                  Version 2
Router Id                     10.0.0.4
ASBR Status                   No
ABR Status                    No          (0)
Redistribute Ext Routes from
Initial SPF schedule delay    0           (msecs)
Minimum hold time for SPFs    0           (msecs)
Maximum hold time for SPFs    0           (msecs)
External LSA Counter          0
External LSA Checksum Sum     0
Originate New LSA Counter     0
Rx New LSA Counter            0
External LSA Limit            14913080
Administrative Distance
  -  External Routes:         110
  -  Intra Area Routes:       110
  -  Inter Area Routes:       110
Database Overflow Interval    0
Database Overflow State :     NOT OVERFLOWED
RFC 1583 Compatibility :      Disabled
NSSA Translator:              Enabled
Nonstop Routing:              Disabled
Graceful Restart              Enabled
Graceful Restart Helper       Enabled
Graceful Restart Time         120
LDP-SYNC: Not globally enabled
Interfaces with LDP-SYNC enabled:
    None
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf area

Displays the OSPF area table in a specified format.

Syntax

show ip ospf area { *A.B.C.D* | *decimal* } **database link-state** [**adv-router** *router-id* | **advertise** *index* | **asbr** { *asbr-id* | **adv-router** *router-id* } | **extensive** | **link-state-id** *id* | **network** { *net-id* | **adv-router** *router-id* } | **nssa** { *nssa-id* | **adv-router** *router-id* } | **router** { *router-id* | **adv-router** *router-id* } | **self-originate** | **sequence-number** *num* | **summary** { *id* | **adv-router** *router-id* }] [**vrf** *vrfname*]

show ip ospf area [**vrf** *vrfname*]

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format. Valid values range from 0 to 2147483647.

database link-state
Displays database link-state information.

adv-router *router-id*
Displays the link state for the advertising router that you specify.

advertise *index*
Displays the link state by Link State Advertisement (LSA) index.

asbr
Displays the link state for all autonomous system boundary router (ASBR) links.

asbr-id
Displays the state of a single ASBR link that you specify.

extensive
Displays detailed information for all entries in the OSPF database.

link-state-id *id*
Displays the link state by link-state ID.

network
Displays the link state by network link.

net-id
Displays the link state of a particular network link that you specify.

nssa
Displays the link state by not-so-stubby area (NSSA).

nssa-id
Displays the link state of a particular NSAA area that you specify.

router
Displays the link state by router link.

router-id

Displays the link state of a particular router link that you specify.

self-originate

Displays self-originated link states.

sequence-number *num*

Displays the link-state by sequence number that you specify.

summary

Displays the link state summary. Can specify link-state ID or advertising router ID.

id

Displays the link state for the advertising router that you specify.

vrf vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show ip ospf area** command.

```
device# show ip ospf area

Number of Areas is 1

Index   Area            Type    Cost       SPFR       ABR   ASBR  LSA     Chksum(Hex)
1       0               normal  0          4305       0     0     5       00024f5a
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf border-routers

Displays information about border routers and boundary routers.

Syntax

show ip ospf border-routers [*A.B.C.D*] [**vrf** *vrfname*]

Parameters

A.B.C.D

Specifies the router ID in dotted decimal format.

vrf *vrf name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about area border routers (ABRs) and autonomous system boundary routers (ASBRs). You can display information for all ABRs and ASBRs or for a specific router.

Examples

The following example displays information for all ABRs and ASBRs:

```
device# show ip ospf border-routers
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf config

Displays OSPF information.

Syntax

show ip ospf config [**vrf** *name*]

Parameters

vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the show ip ospf config command.

```
device# show ip ospf config

Router OSPF: Enabled
Nonstop Routing: Disabled
Graceful Restart: Enabled
Graceful Restart Helper: Enabled
Graceful Restart Time: 120

Redistribution: Disabled
Default OSPF Metric: 10
Maximum Paths: 8
OSPF Auto-cost Reference Bandwidth: Disabled
Default Passive Interface: Disabled
OSPF Redistribution Metric: Type2
OSPF External LSA Limit: 14913080
OSPF Database Overflow Interval: 0
RFC 1583 Compatibility: Disabled
VRF Lite capability: Disabled
Router id: 10.0.0.4
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf database

Shows OSPFv2 database information.

Syntax

show ip ospf database database-summary [**vrf** *vrfname*]

show ip ospf database external-link-state [**advertise** *index* | **extensive** | **link-state-id** *id* | **router-id** *router-id* | **sequence-number** *num*] [**vrf** *vrfname*]

show ip ospf database grace-link-state [**vrf** *vrfname*]

show ip ospf database link-state [**adv-router** *router-id* | **advertise** *index* | **asbr** { *asbr-id* | **adv-router** *router-id* } | **extensive** | **link-state-id** *id* | **network** { *net-id* | **adv-router** *router-id* } | **nssa** { *nssa-id* | **adv-router** *router-id* } | **router** { *router-id* | **adv-router** *router-id* } | **self-originate** | **sequence-number** *num* | **summary** { *id* | **adv-router** *router-id* }] [**vrf** *vrfname*]

show ip ospf database [**vrf** *vrfname*]

Parameters

database-summary
Displays how many link state advertisements (LSAs) of each type exist for each area, as well as total number of LSAs.

vrf *name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

external-link-state
Displays information by external link state, based on the following parameters:

advertise *index*
Displays the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's External LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.

extensive
Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.

link-state-id *id*
Displays external LSAs for the LSA source that you specify.

router-id *router-id*
Displays external LSAs for the advertising router that you specify.

sequence-number *num*
Displays the External LSA entries for the hexadecimal LSA sequence number that you specify.

link-state
Displays the link state, based on the following parameters:

adv-router *router-id*
Displays the link state for the advertising router that you specify.

advertise *index*
Displays the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's external-LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.

asbr
Displays autonomous system boundary router (ASBR) LSAs.

extensive
Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.

link-state-id *id*
Displays LSAs for the LSA source that you specify.

network
Displays either all network LSAs or the LSAs for a network that you specify.

nssa
Displays either all NSSA LSAs or the LSAs for a not-so-stubby area (NSSA) that you specify.

router
Displays LSAs by router link.

router-id *router-id*
Displays LSAs for the advertising router that you specify.

self-originate
Displays self-originated LSAs.

sequence-number
Displays the LSA entries for the hexadecimal LSA sequence number that you specify.

summary
Displays summary information. You can specify link-state ID or advertising router ID.

adv-router *router-id*
Displays the link state for the advertising router that you specify.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show ip ospf database** command.

```
device# show ip ospf database

Link States

Index Area ID         Type LS ID           Adv Rtr         Seq(Hex)        Age  Cksum
1     0               Rtr  200.1.2.3       200.1.2.3       0x80000bb8      235  0x6a51
2     0               Rtr  20.20.20.20     20.20.20.20     0x80000088      1680 0xcb6a
3     0               Rtr  54.1.1.1        54.1.1.1        0x8000009f      599  0x6c3d
4     0               Net  53.1.1.1        200.1.2.3       0x80000006      235  0xd22
5     0               Net  53.54.43.53     200.1.2.3       0x8000007e      626  0x53e6
```

The following example shows output for the **show ip ospf database** command when the **database-summary** keyword is used.

```
device# show ip ospf database database-summary

Area ID          Router  Network  Sum-Net  Sum-ASBR  NSSA-Ext  Opq-Area  Subtotal
0                3       2        0        0         0         0         5
AS External                                                              0
Total            3       2        0        0         0         0         5
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf filtered-lsa area

Displays information about type3 LSA filters attached to specified OSPFv2 areas and lists LSAs filtered in or out.

Syntax

show ip ospf filtered-lsa area { *ip-address* | *decimal* } { **in** | **out** } [**vrf** *vrf-name*]

Parameters

ip-address
Specifies the IP address of an area.

decimal
Specifies an area address in decimal format. Valid values range from 0 through 2147483647.

in
Specifies the incoming direction.

out
Specifies the outgoing direction.

vrf *vrf-name*
Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays information about type 3 LSA filtering in the out direction for OSPFv2 area 0.

```
device# show ip ospf filtered-lsa area 0 out
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf interface

Displays information about all or specific OSPF-enabled interfaces.

Syntax

show ip ospf interface [*A.B.C.D* | **brief**] [**vrf** *vrf-name*]

show ip ospf interface [**ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id*] [**brief**] [**vrf** *vrf-name*]

show ip ospf interface [**vrf** *vrf-name*]

Parameters

A.B.C.D
Specifies interface IP address in dotted decimal format.

brief
Displays summary information.

vrf *vrf-name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

ethernet *slot/port*
Specifies an Ethernet slot and port.

loopback *number*
Specifies a loopback port number. Valid values range from 1 through 255.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096

Modes

Privileged EXEC mode

Examples

The following example displays OSPF information about all enabled interfaces.

```
device# show ip ospf interface

Ethernet 1/2 admin up, oper up
     IP Address 53.1.1.36, Area 0
     BFD is disabled
     Database Filter: Not Configured
     State BDR, Pri 1, Cost 1, Options ------E-, Type broadcast Events 3
     Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
     DR:  Router ID 200.1.2.3         Interface Address 53.1.1.1
     BDR: Router ID 20.20.20.20       Interface Address 53.1.1.36
     Neighbor Count = 1, Adjacent Neighbor Count= 1
     Neighbor:         53.1.1.1 [id 200.1.2.3] (DR)
     Authentication-Key: None
     MD5 Authentication: Key None, Key-Id  None , Auth-change-wait-time 300
LDP-SYNC: Disabled, State: -

Loopback 1 admin up, oper up
     IP Address 20.20.20.20, Area 0
     BFD is disabled
     Database Filter: Not Configured
     State DR, Pri 1, Cost 1, Options ------E-, Type broadcast Events 2
     Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
     DR:  Router ID 20.20.20.20       Interface Address 20.20.20.20
     BDR: Router ID 0.0.0.0           Interface Address 0.0.0.0
     Neighbor Count = 0, Adjacent Neighbor Count= 0
     Authentication-Key: None
     MD5 Authentication: Key None, Key-Id  None , Auth-change-wait-time 300
LDP-SYNC: Disabled, State: -
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf neighbor

Displays OSPF neighbor information.

Syntax

show ip ospf neighbor [**extensive**] [**ethernet** *slot/port* | **router-id** *A.B.C.D* | **ve** *vlan_id*] [**vrf** *vrf-name*]

show ip ospf neighbor [**vrf** *vrf-name*]

Parameters

extensive
Displays detailed neighbor information.

ethernet *slot/port*
Specifies an Ethernet slot and port.

router-id *A.B.C.D*
Displays neighbor information for the specified router ID (in dotted decimal format).

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

vrf *vrf-name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF instance are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example displays information about OSPF neighbors.

```
device# show ip ospf neighbor

Number of Neighbors is 1, in FULL state 1

Port           Address         Pri State      Neigh Address   Neigh ID        Ev      Opt Cnt
Eth 1/2        53.1.1.36       1   FULL/DR    53.1.1.1        200.1.2.3       6       66  0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf redistribute route

Displays routes that have been redistributed into OSPF.

Syntax

show ip ospf redistribute route [*A.B.C.D:M*] [**vrf** *vrfname*]

Parameters

A.B.C.D:M
Specifies an IP address and mask for the output.

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows sample output for the **show ip ospf redistribute route** command.

```
device# show ip ospf redistribute route
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf routes

Displays OSPF calculated routes.

Syntax

show ip ospf routes [*A.B.C.D*] [**vrf** *vrfname*]

Parameters

A.B.C.D

Specifies a destination IP address in dotted decimal format.

vrf *vrfname*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display routes that OSPF calculated. You can display all routes or you can display information about a specific route.

Examples

The following example displays all OSPF-calculated routes.

```
device# show ip ospf routes

OSPF Regular Routes 7:

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.1             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 1          0.0.0.0         OSPF      0  0

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.2             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 2          0.0.0.0         OSPF      0  0

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.3             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 3          0.0.0.0         OSPF      0  0

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.4             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 4          0.0.0.0         OSPF      0  0

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.5             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 5          0.0.0.0         OSPF      0  0

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.6             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 6          0.0.0.0         OSPF      0  0

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.7             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 7          0.0.0.0         OSPF      0  0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf summary

Displays summary information for all OSPF instances.

Syntax

show ip ospf summary [**vrf** *vrfname* | **all-vrfs**| **all-vrfs total**]

Parameters

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

all-vrfs

Specifies all VRF instances. If this option is not used, details for the default VRF are shown in the output.

all-vrfs total

Displays the cumulative summary of OSPF information with the total numbers for all of the VRF intances. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows sample output with the details for the default VRF from the **show ip ospf summary** command.

```
device# show ip ospf summary

Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     5       2       1         12      2
```

The following example shows sample output from the **show ip ospf summary all-vrfs** command.

```
device# show ip ospf summary all-vrfs

Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     0       0       0         0       0
2   vrf_1           0       0       0         0       0
```

The following example shows sample output from the **show ip ospf summary all-vrfs total** command.

```
device# show ip ospf summary all-vrfs total
-------------------------------------------
        IPv4 OSPF VRFs Summary Total
-------------------------------------------
Number of VRFs: 1
Number of Interfaces: 200
Number of Neighbors: 200
Number of Neighbors in Full state: 200
Number of LSAs: 182600
Number of Routes: 102600
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf traffic

Displays OSPF traffic details.

Syntax

show ip ospf traffic

show ip ospf traffic [**ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id*] [**vrf** *vrf-name*]

Parameters

interface

Specifies an interface.

ethernet *slot* **/** *port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

vrf *vrf-name*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display details of OSPF traffic sent and received. You can display all traffic or specify a particular interface.

Examples

The following example shows all OSPF traffic.

```
device# show ip ospf traffic

                 Packets Received         Packets Sent
Hello                          10                   10
Database                       90                   89
LSA Req                        12                   11
LSA Upd                        12                   12
LSA Ack                        12                   12
No Packet Errors!
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf virtual link

Displays information about virtual links.

Syntax

show ip ospf virtual link [*index*] [**vrf** *vrfname*]

Parameters

index

Shows information about all virtual links or one virtual link that you specify.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows information about all virtual links.

```
device# show ip ospf virtual link
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip ospf virtual neighbor

Displays information about virtual neighbors.

Syntax

show ip ospf virtual neighbor [*index*] [**vrf** *vrfname*]

Parameters

index

Shows information about all virtual neighbors or one virtual neighbor that you specify.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows information about all virtual neighbors:

```
device# show ip ospf virtual neighbor
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim bsr

Displays bootstrap router (BSR) information.

Syntax

show ip pim [**all-vrf** | **vrf** *vrf-name*] **bsr**

Parameters

all-vrf

Displays information for all VRFs.

vrf *vrf-name*

Displays information for a specific VRF instance.

bsr

Displays BSR information.

Modes

User EXEC mode

Usage Guidelines

When entered without the **vrf** option, this command displays information for the default VRF instance.

Command Output

The **show ip pim bsr** command displays the following information:

Output Field.	Description
BSR address	The IP address of the interface configured as the PIM Sparse BSR.
BSR priority	The priority assigned to the interface for use during the BSR election process. During BSR election, the priorities of the candidate BSRs are compared and the interface with the highest BSR priority becomes the BSR.
Hash mask length	The number of significant bits in the IP multicast group comparison mask. This mask determines the IP multicast group numbers for which the device can be a BSR. The default is 32 bits, which allows the device to be a BSR for any valid IP multicast group number. NOTE This field appears only if this device is a candidate BSR.
Next bootstrap message in	Indicates how much time will pass before the BSR sends the next bootstrap message. The time is displayed in "hh:mm:ss" format.

Output Field.	Description
	NOTE This field appears only if this device is the BSR.
Next Candidate-RP-advertisement message in	Indicates how much time will pass before the BSR sends the next candidate PR advertisement message. The time is displayed in "hh:mm:ss" format. **NOTE** This field appears only if this device is a candidate BSR.
RP	Indicates the IP address of the Rendezvous Point (RP). **NOTE** This field appears only if this device is a candidate BSR.
group prefixes	Indicates the multicast groups for which the RP listed by the previous field is a candidate RP. **NOTE** This field appears only if this device is a candidate BSR.
Candidate-RP-advertisement period	Indicates how frequently the BSR sends candidate RP advertisement messages. **NOTE** This field appears only if this device is a candidate BSR.

Examples

The following example shows information for a device that has been elected as the BSR.

```
device> show ip pim bsr
PIMv2 Bootstrap information
------------------------------------------------------------------------------
  This system is the Elected BSR
  BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
  Next bootstrap message in 00:01:00
  Configuration:
    Candidate loopback 2 (Address 1.51.51.1). Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisment in 00:01:00
  RP: 1.51.51.1
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

The following example shows information for a device that is not the BSR.

```
device(config)# show ip pim bsr
PIMv2 Bootstrap information
------------------------------------------------------------------------------
  BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisment in 00:00:30
  RP: 1.51.51.3
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim bsr VRF

Displays bootstrap router (BSR) information.

Syntax

show ip pim [**all-vrf** | **vrf** *vrf-name*] **bsr**

Parameters

all-vrf

Displays information for all VRFs.

vrf *vrf-name*

Displays information for a specific VRF instance.

bsr

Displays BSR information.

Modes

User EXEC mode

Usage Guidelines

When entered without the **vrf** option, this command displays information for the default VRF instance.

Command Output

The **show ip pim bsr** command displays the following information:

Output Field.	Description
BSR address	The IP address of the interface configured as the PIM Sparse BSR.
BSR priority	The priority assigned to the interface for use during the BSR election process. During BSR election, the priorities of the candidate BSRs are compared and the interface with the highest BSR priority becomes the BSR.
Hash mask length	The number of significant bits in the IP multicast group comparison mask. This mask determines the IP multicast group numbers for which the device can be a BSR. The default is 32 bits, which allows the device to be a BSR for any valid IP multicast group number. NOTE This field appears only if this device is a candidate BSR.
Next bootstrap message in	Indicates how much time will pass before the BSR sends the next bootstrap message. The time is displayed in "hh:mm:ss" format.

Output Field.	Description
	NOTE This field appears only if this device is the BSR.
Next Candidate-RP-advertisement message in	Indicates how much time will pass before the BSR sends the next candidate PR advertisement message. The time is displayed in "hh:mm:ss" format. **NOTE** This field appears only if this device is a candidate BSR.
RP	Indicates the IP address of the Rendezvous Point (RP). **NOTE** This field appears only if this device is a candidate BSR.
group prefixes	Indicates the multicast groups for which the RP listed by the previous field is a candidate RP. **NOTE** This field appears only if this device is a candidate BSR.
Candidate-RP-advertisement period	Indicates how frequently the BSR sends candidate RP advertisement messages. **NOTE** This field appears only if this device is a candidate BSR.

Examples

The following example shows information for a device that has been elected as the BSR.

```
device> show ip pim bsr
PIMv2 Bootstrap information
------------------------------------------------------------------------------
  This system is the Elected BSR
  BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
  Next bootstrap message in 00:01:00
  Configuration:
    Candidate loopback 2 (Address 1.51.51.1). Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisment in 00:01:00
  RP: 1.51.51.1
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

The following example shows information for a device that is not the BSR.

```
device(config)# show ip pim bsr
PIMv2 Bootstrap information
------------------------------------------------------------------------------
  BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisment in 00:00:30
  RP: 1.51.51.3
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim interface

Displays information for PIM interfaces.

Syntax

show ip pim interface { **ethernet** *slot*/*port* | **loopback** *loopback-number* | **ve** *vlan ID* }

Parameters

ethernet *slot*/*port*

Specifies a physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *loopback-number*

Specifies a loopback interface.

ve *ve-number*

Specifies a virtual interface.

Modes

Privileged EXEC mode

Examples

The following example displays the output from the **show ip pim interface** command.

```
device# show ip pim interface
------------+--------------+----+-----+------------------------------+---+------
Interface |Local    |Ver|Mode | Designated Router |TTL| DR
          |Address |    |     |Address      Port   |Thr| Prio
------------+--------------+----+-----+------------------------------+---+------
Eth 2/30  55.1.1.1  v2   SM  Itself               1    1
Ve30      30.1.1.1  v2   SM  30.1.1.20    Ve30     1    1
Lo        1 4.4.4.4 v2   SM  Itself 1 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim interface VRF

Displays information for PIM interfaces.

Syntax

show ip pim interface VRF { **ethernet** *slot*/*port-id* | **loopback** *loopback-number* | **ve** *vlan ID* }

Parameters

loopback *loopback-number*
Specifies a loopback interface.

ve *ve-number*
Specifies a virtual interface.

Modes

Privileged EXEC mode

Examples

The following example displays the output from the **show ip pim interface** command.

```
device# show ip pim interface
-------------+---------------+----+-----+-------------------------------+---+------
Interface |Local    |Ver|Mode | Designated Router |TTL| DR
          |Address |   |     |Address      Port   |Thr| Prio
-------------+---------------+-----------------------------------------+---+------
Eth 2/30  55.1.1.1  v2   SM  Itself                1    1
Ve30      30.1.1.1  v2   SM  30.1.1.20    Ve30     1    1
Lo        1 4.4.4.4 v2   SM  Itself 1 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim mcache

Displays the multicast cache.

Syntax

show ip pim mcache [*A.B.C.D* | **ecmp** *ipv4 address*]

Parameters

A.B.C.D

Specifies the multicast group or source IP address.

ecmp*ipv4 address*

Specifies the PIM ECMP IPv4 information.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example displays the output for **show ip pim mcache** *ip-address-1 ip-address-2*.

```
device# show ip pim mcache 50.1.1.101 230.1.1.1
IP Multicast Mcache Table
Entry Flags    : sm  - Sparse Mode, ssm - Source Specific Multicast
                 RPT - RPT Bit, SPT - SPT Bit, LSrc - Local Source
                 LRcv - Local Receiver, RegProbe - Register In Progress
                 RegSupp - Register Suppression Timer, Reg - Register Complete
                 needRte - Route Required for Src/RP
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
                 MJ - Membership Join, BR - Blocked RPT, BA - Blocked Assert
                 BF - Blocked Filter
Total entries in mcache: 8
1    (50.1.1.101, 230.1.1.1) in Ve 40, Uptime 00:03:29
     Sparse Mode, RPT=0 SPT=1 Reg=0 RegSupp=0 RegProbe=0 LSrc=0 LRcv=1
     upstream neighbor=40.1.1.3
     num_oifs = 2
           Ve 2(00:03:29/181) Flags: IM
           Ve 10(00:03:29/0) Flags: MJ
     Flags (0x400784d1)
         sm=1 ssm=0 needRte=0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim neighbor

Displays information about PIM neighbors.

Syntax

show ip pim neighbor [**interface ethernet***slot*/*port* | **interface ve** *ve-num*]

Parameters

interface ethernet *slot*/*port*

Displays information for the specified Ethernet interface.

interface ve *ve-num*

Displays information for the specified VE interface.

Modes

User EXEC mode

Command Output

The **show ip pim neighbor** command displays the following information:

Output Field	Description
Port	The interface through which the device is connected to the neighbor.
Phyport	When there is a virtual interface, this is the physical port to which the neighbor is connected.
Neighbor	The IP interface of the PIM neighbor.
Holdtime sec	Indicates how many seconds the neighbor wants this device to hold the entry for this neighbor in memory. The neighbor sends the Hold Time in Hello packets: • If the device receives a new Hello packet before the Hold Time received in the previous packet expires, the device updates its table entry for the neighbor. • If the device does not receive a new Hello packet from the neighbor before the Hold time expires, the device assumes the neighbor is no longer available and removes the entry for the neighbor.
Age sec	The number of seconds since the device received the last hello message from the neighbor.
UpTime sec	The number of seconds the PIM neighbor has been up. This timer starts when the device receives the first Hello messages from the neighbor.
VRF	The VRF in which the interface is configured. This can be a VRF that the port was assigned to or the default VRF of the device.
Priority	The DR priority that is used in the DR election process. This can be a configured value or the default value of 1.

Examples

The following example shows information about PIM neighbors.

```
device(config)# show ip pim neighbor
--------+--------+---------------+--------+---+---------+---------+-----+-----------+-----------+----
Port    |PhyPort |Neighbor       |Holdtime|T  |PropDelay|Override |Age  |UpTime     |VRF        |Prio
        |        |               |sec     |Bit|msec     |msec     |sec  |           |           |
--------+--------+---------------+--------+---+---------+---------+-----+-----------+-----------+----
v2       e1/1     2.1.1.2         105      1   500       3000      0     00:44:10    default-vrf 1
v4       e1/2     4.1.1.2         105      1   500       3000      10    00:42:50    default-vrf 1
v5       e1/1     5.1.1.2         105      1   500       3000      0     00:44:00    default-vrf 1
v22      e1/1     22.1.1.1        105      1   500       3000      0     00:44:10    default-vrf 1
Total Number of Neighbors : 4
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim neighbor VRF

Displays information about PIM neighbors.

Syntax

show ip pim neighbor [**interface ethernet***slot*/*port* | **interface ve** *ve-num*]

Parameters

interface ethernet *slot*/*port*

Displays information for the specified Ethernet interface.

interface ve *ve-num*

Displays information for the specified VE interface.

Modes

User EXEC mode

Command Output

The **show ip pim neighbor** command displays the following information:

Output Field	Description
Port	The interface through which the device is connected to the neighbor.
Phyport	When there is a virtual interface, this is the physical port to which the neighbor is connected.
Neighbor	The IP interface of the PIM neighbor.
Holdtime sec	Indicates how many seconds the neighbor wants this device to hold the entry for this neighbor in memory. The neighbor sends the Hold Time in Hello packets: • If the device receives a new Hello packet before the Hold Time received in the previous packet expires, the device updates its table entry for the neighbor. • If the device does not receive a new Hello packet from the neighbor before the Hold time expires, the device assumes the neighbor is no longer available and removes the entry for the neighbor.
Age sec	The number of seconds since the device received the last hello message from the neighbor.
UpTime sec	The number of seconds the PIM neighbor has been up. This timer starts when the device receives the first Hello messages from the neighbor.
VRF	The VRF in which the interface is configured. This can be a VRF that the port was assigned to or the default VRF of the device.
Priority	The DR priority that is used in the DR election process. This can be a configured value or the default value of 1.

Examples

The following example shows information about PIM neighbors.

```
device(config)# show ip pim neighbor
--------+--------+---------------+--------+---+---------+---------+-----+-----------+-----------+----
Port    |PhyPort |Neighbor       |Holdtime|T  |PropDelay|Override |Age  |UpTime     |VRF        |Prio
        |        |               |sec     |Bit|msec     |msec     |sec  |           |           |
--------+--------+---------------+--------+---+---------+---------+-----+-----------+-----------+----
v2       e1/1     2.1.1.2         105      1   500       3000      0     00:44:10    default-vrf 1
v4       e1/2     4.1.1.2         105      1   500       3000      10    00:42:50    default-vrf 1
v5       e1/1     5.1.1.2         105      1   500       3000      0     00:44:00    default-vrf 1
v22      e1/1     22.1.1.1        105      1   500       3000      0     00:44:10    default-vrf 1
Total Number of Neighbors : 4
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rp-candidate

Displays candidate rendezvous point (RP) information.

Syntax

show ip pim rp-candidate

Parameters

rp-candidate

Specifies the candidate rendezvous point.

Modes

User EXEC mode

Usage Guidelines

When used without the **vrf** option, this command displays information for the default VRF.

Command Output

The **show ip pim rp-candidate** command displays the following information:

Output Field	Description
Candidate-RP-advertisement in	How time will pass before the BSR sends the next RP message. The time is displayed in "hh:mm:ss" format. **NOTE** This field appears only if this device is a candidate RP.
RP	The IP address of the RP. **NOTE** This field appears only if this device is a candidate RP.
group prefixes	The multicast groups for which the RP listed by the previous field is a candidate RP. **NOTE** This field appears only if this device is a candidate RP.
Candidate-RP-advertisement period	How frequently the BSR sends candidate RP advertisement messages. **NOTE** This field appears only if this device is a candidate RP.

Examples

The following example shows information for a candidate RP.

```
device# show ip pim rp-candidate
Next Candidate-RP-advertisement in 00:00:10
  RP: 207.95.7.1
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rp-candidate VRF

Displays candidate rendezvous point (RP) information.

Syntax

show ip pim rp-candidate

Parameters

rp-candidate

Specifies the candidate rendezvous point.

Modes

User EXEC mode

Usage Guidelines

When used without the **vrf** option, this command displays information for the default VRF.

Command Output

The **show ip pim rp-candidate** command displays the following information:

Output Field	Description
Candidate-RP-advertisement in	How time will pass before the BSR sends the next RP message. The time is displayed in "hh:mm:ss" format. **NOTE** This field appears only if this device is a candidate RP.
RP	The IP address of the RP. **NOTE** This field appears only if this device is a candidate RP.
group prefixes	The multicast groups for which the RP listed by the previous field is a candidate RP. **NOTE** This field appears only if this device is a candidate RP.
Candidate-RP-advertisement period	How frequently the BSR sends candidate RP advertisement messages. **NOTE** This field appears only if this device is a candidate RP.

Examples

The following example shows information for a candidate RP.

```
device# show ip pim rp-candidate
Next Candidate-RP-advertisement in 00:00:10
  RP: 207.95.7.1
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rp-hash

Displays rendezvous-point (RP) information for a PIM Sparse group.

Syntax

show ip pim rp-hash *group-addr*

Parameters

group-addr

Specifies the address of a PIM Sparse IP multicast group.

Modes

Privileged EXEC mode

Command Output

The **show ip pim rp-hash** command displays the following information:

Output Field	Description
RP	Indicates the IP address of the RP for the specified PIM Sparse group.
Info source	Indicates the source of the RP information. It can be a static-RP configuration or learned via the bootstrap router. If RP information is learned from the boot strap, the BSR IP address is also displayed.

Examples

The following example shows RP information for a PIM Sparse group.

```
device# show ip pim rp-hash 239.255.162.1
  RP: 207.95.7.1, v2
    Info source: 207.95.7.1, via bootstrap
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rp-hash VRF

Displays rendezvous-point (RP) information for a PIM Sparse group.

Syntax

show ip pim rp-hash *group-addr*

Parameters

group-addr

Specifies the address of a PIM Sparse IP multicast group.

Modes

Privileged EXEC mode

Command Output

The **show ip pim rp-hash** command displays the following information:

Output Field	Description
RP	Indicates the IP address of the RP for the specified PIM Sparse group.
Info source	Indicates the source of the RP information. It can be a static-RP configuration or learned via the bootstrap router. If RP information is learned from the boot strap, the BSR IP address is also displayed.

Examples

The following example shows RP information for a PIM Sparse group.

```
device# show ip pim rp-hash 239.255.162.1
  RP: 207.95.7.1, v2
    Info source: 207.95.7.1, via bootstrap
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rp-map

Displays rendezvous-point (RP)-to-group mapping information.

Syntax

show ip pim rp-map

Modes

User EXEC mode

Command Output

The **show ip pim rp-map** command displays the following information:

Output Field	Description
Group address	Indicates the PIM Sparse multicast group address using the listed RP.
RP address	Indicates the IP address of the RP for the listed PIM Sparse group.

Examples

The following example shows RP-to-group mapping.

```
device> show ip pim rp-map
Number of group-to-RP mappings: 6
Group address        RP address
------------------------------
1 239.255.163.1  99.99.99.5
2 239.255.163.2  99.99.99.5
3 239.255.163.3  99.99.99.5
4 239.255.162.1  99.99.99.5
5 239.255.162.2  43.43.43.1
6 239.255.162.3  99.99.99.5
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rp-map VRF

Displays rendezvous-point (RP)-to-group mapping information.

Syntax

show ip pim rp-map

Parameters

vrf *vrf-name*

Displays information for the specified VRF instance.

Modes

User EXEC mode

Command Output

The **show ip pim rp-map** command displays the following information:

Output Field	Description
Group address	Indicates the PIM Sparse multicast group address using the listed RP.
RP address	Indicates the IP address of the RP for the listed PIM Sparse group.

Examples

The following example shows RP-to-group mapping.

```
device# show ip pim rp-map
Number of group-to-RP mappings: 6
Group address        RP address
------------------------------
1 239.255.163.1  99.99.99.5
2 239.255.163.2  99.99.99.5
3 239.255.163.3  99.99.99.5
4 239.255.162.1  99.99.99.5
5 239.255.162.2  43.43.43.1
6 239.255.162.3  99.99.99.5
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rp-set

Displays rendezvous-point (RP)-set list for the device elected as the bootstrap router (BSR).

Syntax

show ip pim rp-set

Modes

User EXEC mode

Command Output

The **show ip pim rp-set** command displays the following information:

Output Field	Description
Number of group prefixes	The number of PIM Sparse group prefixes for which the RP is responsible.
Group prefix	Indicates the multicast groups for which the RP listed by the previous field is a candidate RP.
RPs expected or received	Indicates how many RPs were expected and received in the latest bootstrap message.
RP *num*	Indicates the RP number. If there are multiple RPs in the PIM Sparse domain, a line of information for each RP is listed, in ascending numerical order.
priority	The RP priority of the candidate RP. During the election process, the candidate RP with the highest priority is elected as the RP.
age	The age (in seconds) of this RP-set.
holdtime	Indicates the time in seconds for which this rp-set information is valid. If this rp-set information is not received from BSR within the holdtime period, the rp-set information is aged out and deleted.

Examples

The following example shows the RP set list for the device elected as BSR.

```
device# show ip pim rp-set
Static RP
---------
Static RP count: 2
1.51.51.4
1.51.51.5
Number of group prefixes Learnt from BSR: 1
Group prefix = 224.0.0.0/4      # RPs: 2
      RP 1: 1.51.51.1    priority=0    age=60    holdtime=150
      RP 2: 1.51.51.3    priority=0    age=30    holdtime=150
```

The following example shows the RP set list for devices that are not elected as BSR.

```
device# show ip pim rp-set
Static RP
---------
Static RP count: 2
1.51.51.4
1.51.51.5
Number of group prefixes Learnt from BSR: 1
Group prefix = 224.0.0.0/4      # RPs expected: 2
      # RPs received: 2
      RP 1: 1.51.51.1    priority=0    age=60    holdtime=150
      RP 2: 1.51.51.3    priority=0    age=30    holdtime=150
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rp-set VRF

Displays rendezvous-point (RP)-set list for the device elected as the bootstrap router (BSR).

Syntax

show ip pim rp-set

Parameters

all-vrf

Displays information for all VRF instances.

vrf *vrf-name*

Displays information for the specified VRF instance.

Modes

User EXEC mode

Command Output

The **show ip pim rp-set** command displays the following information:

Output Field	Description
Number of group prefixes	The number of PIM Sparse group prefixes for which the RP is responsible.
Group prefix	Indicates the multicast groups for which the RP listed by the previous field is a candidate RP.
RPs expected or received	Indicates how many RPs were expected and received in the latest bootstrap message.
RP *num*	Indicates the RP number. If there are multiple RPs in the PIM Sparse domain, a line of information for each RP is listed, in ascending numerical order.
priority	The RP priority of the candidate RP. During the election process, the candidate RP with the highest priority is elected as the RP.
age	The age (in seconds) of this RP-set.
holdtime	Indicates the time in seconds for which this rp-set information is valid. If this rp-set information is not received from BSR within the holdtime period, the rp-set information is aged out and deleted.

Examples

The following example shows the RP set list for the device elected as BSR.

```
device# show ip pim rp-set
Static RP
---------
Static RP count: 2
1.51.51.4
1.51.51.5
Number of group prefixes Learnt from BSR: 1
Group prefix = 224.0.0.0/4      # RPs: 2
      RP 1: 1.51.51.1    priority=0    age=60    holdtime=150
      RP 2: 1.51.51.3    priority=0    age=30    holdtime=150
```

The following example shows the RP set list for devices that are not elected as BSR.

```
device# show ip pim rp-set
Static RP
---------
Static RP count: 2
1.51.51.4
1.51.51.5
Number of group prefixes Learnt from BSR: 1
Group prefix = 224.0.0.0/4      # RPs expected: 2
      # RPs received: 2
      RP 1: 1.51.51.1    priority=0    age=60    holdtime=150
      RP 2: 1.51.51.3    priority=0    age=30    holdtime=150
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rpf

Displays what PIM sees as the best reverse path to the source. While there may be multiple routes back to the source, the one displayed by this command is the one that PIM thinks is best.

Syntax

show ip pim [**vrf** *vrf-name*] **rpf** *A.B.C.D*

Parameters

vrf *vrf-name*

Displays information for the specified VRF instance.

A.B.C.D

Specifies the source address for reverse-path forwarding (RPF) check.

Modes

User EXEC mode

Examples

This example shows best reverse path to the specified source:

```
device# show ip pim vrf eng rpf 130.50.11.10
Source 130.50.11.10 directly connected on e1/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim rpf VRF

Displays what PIM sees as the best reverse path to the source. While there may be multiple routes back to the source, the one displayed by this command is the one that PIM thinks is best.

Syntax

show ip pim [**vrf** *vrf-name*] **rpf** *A.B.C.D*

Parameters

vrf *vrf-name*

Displays information for the specified VRF instance.

A.B.C.D

Specifies the source address for reverse-path forwarding (RPF) check.

Modes

User EXEC mode

Examples

This example shows best reverse path to the specified source:

```
device# show ip pim vrf eng rpf 130.50.11.10
Source 130.50.11.10 directly connected on e1/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim traffic

Displays IPv4 PIM traffic statistics.

Syntax

show ip pim traffic

Modes

Privileged EXEC mode

Usage Guidelines

PIM control packet statistics for interfaces that are configured for standard PIM are listed first by the display.

Command Output

The **show ip pim traffic** command displays the following information:

Output Field	Description
Port	The port or virtual interface on which the PIM interface is configured.
HELLO	The number of PIM Hello messages sent or received on the interface.
JOIN-PRUNE	The number of Join or Prune messages sent or received on the interface. NOTE Unlike PIM Dense, PIM Sparse uses the same messages for Joins and Prunes.
ASSERT	The number of Assert messages sent or received on the interface.
REGISTER GRAFT (DM)	The number of Register messages sent or received on the interface.
REGISTER STOP (SM)	The number of Register Stop messages sent or received on the interface.
BOOTSTRAP MSGS (SM)	The number of bootstrap messages sent or received on the interface.
CAND. RP ADV. (SM)	The total number of Candidate-RP-Advertisement messages sent or received on the interface.
Err	The total number of messages discarded, including a separate counter for those that failed the checksum comparison.

Examples

This example shows PIM join and prune traffic statistics for received and sent packets:

```
device# show ip pim traffic
Port       |HELLO  |JOIN   |PRUNE  |ASSERT |GRAFT/REGISTER |REGISTER-STOP |BSR-MSGS  |RPC-MSGS
           |Rx     |Rx     |Rx     |Rx     |Rx             |Rx            |Rx        |Rx
-----------+-------+-------+-------+-------+---------------+--------------+----------+----------+
Ve10         54       0       0       0       0             0              0          0
Lo 1         0        0       0       0       0             0              0          0

device# show ip pim traffic
Port        |HELLO |JOIN   |PRUNE |ASSERT |GRAFT/REGISTER |REGISTER-STOP |BSR-MSGS |RPC-MSGS
            | Tx   |Tx     | Tx   |Tx     |Tx             |Tx            |         |         |---
------------+------+-------+------+-------+---------------+--------------+---------+---------+---
Ve10         29       0     0       0       0             0              0          0
Lo 1         28       0     0       0       0             0              0          0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip pim traffic VRF

Displays IPv4 PIM traffic statistics.

Syntax

show ip pim traffic [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies information for a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

PIM control packet statistics for interfaces that are configured for standard PIM are listed first by the display.

Command Output

The **show ip pim traffic** command displays the following information:

Output Field	Description
Port	The port or virtual interface on which the PIM interface is configured.
HELLO	The number of PIM Hello messages sent or received on the interface.
JOIN-PRUNE	The number of Join or Prune messages sent or received on the interface. NOTE Unlike PIM Dense, PIM Sparse uses the same messages for Joins and Prunes.
ASSERT	The number of Assert messages sent or received on the interface.
REGISTER GRAFT (DM)	The number of Register messages sent or received on the interface.
REGISTER STOP (SM)	The number of Register Stop messages sent or received on the interface.
BOOTSTRAP MSGS (SM)	The number of bootstrap messages sent or received on the interface.
CAND. RP ADV. (SM)	The total number of Candidate-RP-Advertisement messages sent or received on the interface.
Err	The total number of messages discarded, including a separate counter for those that failed the checksum comparison.

Examples

This example shows PIM join and prune traffic statistics for received and sent packets:

```
device# show ip pim traffic
Port       |HELLO  |JOIN   |PRUNE  |ASSERT |GRAFT/REGISTER |REGISTER-STOP |BSR-MSGS  |RPC-MSGS
           |Rx     |Rx     |Rx     |Rx     |Rx             |Rx            |Rx        |Rx
-----------+-------+-------+-------+-------+---------------+--------------+----------+----------+
Ve10         54       0       0       0       0             0              0          0
Lo 1         0        0       0       0       0             0              0          0

device# show ip pim traffic
Port        |HELLO |JOIN   |PRUNE |ASSERT |GRAFT/REGISTER |REGISTER-STOP |BSR-MSGS |RPC-MSGS
            | Tx   |Tx     | Tx   |Tx     |Tx             |Tx            |         |         |---
------------+------+-------+------+-------+---------------+--------------+---------+---------+---
Ve10         29       0     0       0       0             0              0          0
Lo 1         28       0     0       0       0             0              0          0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ip route

Displays IP route information for IPv4 interfaces.

Syntax

show ip route [**vrf** *vrf-name*]

show ip route *A.B.C.D* [**vrf** *vrf-name*]

show ip route *A.B.C.D/M* [**longer**] [**vrf** *vrf-name*]

show ip route all [**vrf** *vrf-name*]

show ip route bgp [**vrf** *vrf-name*]

show ip route connected [**vrf** *vrf-name*]

show ip route import [*src-vrf-name*] [**vrf** *vrf-name*]

show ip route nexthop [*nexthopID* [**ref-routes**]] [**vrf** *vrf-name*]

show ip route ospf [**vrf** *vrf-name*]

show ip route slot *line-card-number* [*A.B.C.D* | *A.B.C.D/M*] [**vrf** *vrf-name*]

show ip route static [**vrf** *vrf-name*]

show ip route summary [**vrf** *vrf-name*]

show ip route system-summary

Parameters

vrf*vrf-name*
: Specifies routes for a selected VRF instance.

A.B.C.D/M
: Specifies the IPv4 address and optional mask.

  longer
  : Specifies routes that match the specified prefix.

all
: Specifies information for all configured IPv4 routes.

bgp
: Specifies BGP route information.

connected
: Specifies directly connected routes, such as local Layer 3 interfaces.

import
: Specifies imported IPv4 routes.

  src-vrf-name
  : Specifies a VRF instance from which routes are leaked.

nexthop
: Specifies the configured next hop.

nexthopID
Valid values range from 0 through 4294967294.

ref-routes
Specifies all routes that point to the specified *next-hop ID* .

ospf
Specifies routes learned from the Open Shortest Path First (OSPF) protocol.

slot *line-card-number*
Specifies routes with the provided line card number.

static
Specifies configured static routes.

summary
Specifies summary information for all routes.

system-summary
Specifies a system-level routing summary.

Modes

Privileged EXEC mode

Usage Guidelines

If leaked subnet routes are present, that information displays in the output.

To view the status of management routes, use the **show ip route vrf** command and enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually. Example output is shown below.

```
device# show ip route vrf mgmt-vrf
IP Routing Table for VRF "mgmt-vrf"
Total number of IP routes: 3
'*' denotes best ucast next-hop
'[x/y]' denotes [preference/metric]

0.0.0.0/0
    *via 10.25.96.1, mgmt 1, [1/1], 8d15h, static, tag 0
10.25.96.0/22, attached
    *via DIRECT, mgmt 1, [0/0], 8d15h, direct, tag 0
10.25.96.38/32, attached
    *via DIRECT, mgmt 1, [0/0], 8d15h, local, tag 0
```

Examples

The following example displays output for the **system-summary** option.

```
device# show ip route system-summary
System Route Count: 3 Max routes: 4096 (Route limit not exceeded)
System Nexthop Count: 2 Max nexthops: 1024 (Nexthop limit not exceeded)

VRF-Name: default-vrf
  Route count: 0 Max routes: Not Set (Route limit not exceeded)
  0 connected, 0 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS, 0 unnumbered

VRF-Name: mgmt-vrf
  Route count: 3 Max routes: Not Set (Route limit not exceeded)
  1 connected, 1 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS, 0 unnumbered
```

The following example displays output for the **connected** option.

```
device# show ip route connected
 Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       1.1.1.0/24         DIRECT          Te 2/1      0/0           D    4m33s
2       1.1.2.0/24         DIRECT          Te 2/2      0/0           D    2m42s
```

The following example displays output for the **summary** option.

```
device# show ip route summary
IP Routing Table - 7 entries:
  8 direct, 0 static, 0 RIP, 0 OSPF, 8 BGP, 0 ISIS, 80 EVPN Host
  Number of prefixes:
  /24: 7
Nexthop Table Entry - 4 entries
```

The following example displays output for the **nexthop** option.

```
device# show ip route nexthop
 Total number of IP nexthop entries: 4; Forwarding Use: 4
       NextHopIp        Port             RefCount      ID          Age
1      1.1.1.2          Te 2/1           3/3           2147549184 277
2      0.0.0.0          Te 2/2           1/1           2147484008 191
3      0.0.0.0          Te 2/1           2/2           2147484009 302
4      1.1.1.2          Te 2/1           1/1           2147549185 190
       1.1.2.2          Te 2/2
```

The following example displays output for a specific next-hop ID option.

```
device# show ip route nexthop 2147549184
       NextHopIp        Port             RefCount      ID          Age
1      1.1.1.2          Te 2/1           3/3           2147549184 288
```

The following example displays output for the **ref-routes** option.

```
device# show ip route nexthop 2147549184 ref-routes
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m10s
2       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    4m54s
3       100.1.3.0/24       1.1.1.2         Te 2/1      1
```

The following example displays output for a specific IP address.

```
device# show ip route 100.1.1.1
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
4       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m37s
```

The following example displays output for the **longer** option.

```
device# show ip route 100.0.0.0/8 longer
1       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    14m37s
2       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    14m21s
3       100.1.3.0/24       1.1.1.2         Te 2/1      1/1           S    14m18s
4       100.2.1.0/24       DIRECT          Te 2/1      1/1           S    14m2s
5       100.3.1.0/24       1.1.1.2         Te 2/1      1/1           S    13m10s
        100.3.1.0/24       1.1.2.2         Te 2/2      1/1           S    13m10s
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp

Displays BGP4+ route information.

Syntax

show ipv6 bgp

show ipv6 bgp *ipv6-addr* [*/prefix*]

show ipv6 bgp *ipv6-addr* [*/prefix*] [**longer-prefixes**] [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation, with optional mask.

/prefix
IPv6 mask length in CIDR notation.

longer-prefixes
Filters on prefixes equal to or greater than that specified by *prefix.*

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays sample output from the **show ipv6 bgp** command.

```
device# show ipv6 bgp
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp attribute-entries

Displays BGP4+ route-attribute entries that are stored in device memory.

Syntax

show ipv6 bgp attribute-entries [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4+ attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4+ route-attribute entries that are stored in device memory.

Examples

This example show sample output for the **show ipv6 bgp attribute-entries** command.

```
device# show ipv6 bgp attribute-entries

        Total number of BGP Attribute Entries: 1
1       Next Hop   : ::                                        MED      :0              Origin:INCOMP
        Originator:0.0.0.0           Cluster List:None
        Aggregator:AS Number :0           Router-ID:0.0.0.0          Atomic:None
        Local Pref:100              Communities:Internet
        AS Path    : (length 0)
           AsPathLen: 0  AsNum: 0, SegmentNum: 0, Neighboring As: 0, Source As 0
        Address: 0x0b456c4c  Hash:876 (0x03000000)
        Links: 0x00000000, 0x00000000
        Reference Counts: 1:0:1, Magic: 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp dampened-paths

Displays all BGP4+ dampened routes.

Syntax

show ipv6 bgp dampened-paths [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 bgp dampened-paths** command.

```
device# show ipv6 bgp dampened-paths

    Status Code  >:best d:damped h:history *:valid
    Network                                   From                                    Flaps
Since       Reuse       Path
*d  110:110:110:4::/64                        160:160:160::10                         36    0 :2 :
54    0 :10:10    111
*d  110:110:110:3::/64                        160:160:160::10                         36    0 :2 :
54    0 :10:10    111
*d  110:110:110:2::/64                        160:160:160::10                         36    0 :2 :
54    0 :10:10    111
*d  110:110:110:1::/64                        160:160:160::10                         36    0 :2 :
54    0 :10:10    111
*d  110:110:110::/64                          160:160:160::10                         36    0 :2 :
54    0 :10:10    111
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp filtered-routes

Displays BGP4+ filtered routes that are received from a neighbor or peer group.

Syntax

show ipv6 bgp filtered-routes [**detail**] [*ipv6-addr* { **/** *mask* } [**longer-prefixes**]] | **as-path-access-list** *name* | **prefix-list** *name*] [**vrf** *vrf-name*]

Parameters

detail
Optionally displays detailed route information.

ipv6-addr
IPv6 address of the destination network in dotted-decimal notation.

mask
IPv6 mask of the destination network in CIDR notation.

longer-prefixes
Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

as-path-access-list *name*
Specifies an AS-path ACL. The name must be between 1 and 32 ASCII characters in length.

prefix-list *name*
Specifies an IP prefix list. The name must be between 1 and 32 ASCII characters in length.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays BGP4+ filtered routes.

```
device# show ipv6 bgp filtered-routes
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp flap-statistics

Displays BGP4+ route-dampening statistics for all dampened routes with a variety of options.

Syntax

show ipv6 bgp flap-statistics

show ipv6 bgp flap-statistics *ipv6-addr* { **/** *mask* } [**longer-prefixes** [**vrf** *vrf-name*] | **vrf** *vrf-name*]

show ipv6 bgp flap-statistics neighbor *ipv6-addr* [**vrf** *vrf-name*]

show ipv6 bgp flap-statistics regular-expression *name* [**vrf** *vrf-name*]

show ipv6 bgp flap-statistics vrf *vrf-name*

Parameters

ipv6-addr
IPv6 address of a specified route in dotted-decimal notation.

mask
IPv6 mask of a specified route in CIDR notation.

longer-prefixes
Displays statistics for routes that match the specified route or have a longer prefix than the specified route.

vrf *vrf-name*
Specifies a VRF instance.

neighbor
Displays flap statistics only for routes learned from the specified neighbor.

ip-addr
IPv6 address of the neighbor.

regular-expression
Specifies a regular expression in the display output on which to filter.

name
Name of an AS-path filter or regular expression.

Modes

Privileged EXEC mode

Examples

This example displays flap statistics for a neighbor.

```
device# show ipv6 bgp flap-statistics neighbor 2001:
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors

Displays configuration information and statistics for BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors [*ipv6-addr*]

show ipv6 bgp neighbors last-packet-with-error [**vrf** *vrf-name*]

show ipv6 bgp neighbors routes-summary [**vrf** *vrf-name*]

show ipv6 bgp neighbors vrf *vrf-name*

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

last-packet-with-error
Displays the last packet with an error.

route-summary
Displays routes received, routes accepted, number of routes advertised by peer, and so on.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP4+ neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

Examples

This example shows sample output from the show ipv6 bgp neighbors command.

```
device# show ipv6 bgp neighbors

    Total number of BGP Neighbors: 1
1   IP Address: 1:2::3, AS: 100 (IBGP), RouterID: 0.0.0.0, VRF: default-vrf
    State: CONNECT, Time: 0h3m3s, KeepAliveTime: 60, HoldTime: 180
    Minimal Route Advertisement Interval: 0 seconds
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 0       0       0         0            0
       Received: 0       0       0         0            0
    Last Connection Reset Reason:Unknown
    Notification Sent:     Unspecified
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer configured for IPV6 unicast  Routes
    Neighbor ipv6 MPLS Label Capability Negotiation:
    Neighbor AS4 Capability Negotiation:
    Outbound Policy Group:
       ID: 2, Use Count: 3
       Last update time was 172 sec ago
Error: TCP status not available
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors advertised-routes

Displays the routes that the device has advertised to the neighbor during the current BGP4+ session.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **advertised-routes** [**detail** | **/** *mask-bits*] [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

detail
Displays details of advertised routes.

mask-bits
Number of mask bits in CIDR notation.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays the details of advertised routes.

```
device# show ipv6 bgp neighbors 123::3 advertised-routes

       There are 5 routes advertised to neighbor 123::3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110:110:110::/64   123::2           0                     0      BE
         AS_PATH: 222 111
2      110:110:110:1::/64 123::2           0                     0      BE
         AS_PATH: 222 111
3      110:110:110:2::/64 123::2           0                     0      BE
         AS_PATH: 222 111
4      110:110:110:3::/64 123::2           0                     0      BE
         AS_PATH: 222 111
5      110:110:110:4::/64 123::2           0                     0      BE
         AS_PATH: 222 111
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors flap-statistics

Displays the route flap statistics for routes received from or sent to a BGP4+ neighbor.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **flap-statistics** [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows flap statistics.

```
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors last-packet-with-error

Displays information about the last packet that contained an error from any of a device's neighbors.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **last-packet-with-error** [**decode**] [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

decode
Decodes last packet that contained an error from any of a device's neighbors.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ipv6 bgp neighbors last-packet-with-error** command when no packet from a specified neighbor contained an error.

```
device# show ipv6 bgp neighbors 123::3 last-packet-with-error

 Received Message Length: 45
 BGP Message:
  0xffffffff  0xffffffff  0xffffffff  0xffffffff  0x002d0104
  0x014b00b4  0x09090909  0x10020601  0x04020000  0x01020202
  0x00020280  0x00

 BGP Header
  Marker:   0xffffffff  0xffffffff  0xffffffff  0xffffffff
  Message Length: (0x002d) 45
  Message Type: (0x01) OPEN

 OPEN Message
 Version: (0x04) 4
 AS Number: (0x014b) 331
 Hold Time: (0x00b4) 180
 BGP Identifier: (0x09090909) 9.9.9.9
 Optional Parameter length: (0x10) 16

 OPEN message optional parameters
  Parameter Type: (0x02) Capability
  Parameter Length: (0x06) 6
   Capability Type: (0x01) MULTIPROTOCOL EXTENSIONS
   Capability Length: (0x04) 4
   AFI: (0x0200) Unknown(512)
   Reserved: (0x00) 0
   SAFI: (0x01) Unicast

  Parameter Type: (0x02) Capability
  Parameter Length: (0x02) 2
   Capability Type: (0x02) ROUTE REFRESH(new)
   Capability Length: (0x00) 0

  Parameter Type: (0x02) Capability
  Parameter Length: (0x02) 2
   Capability Type: (0x80) ROUTE REFRESH(old)
   Capability Length: (0x00) 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **received**

show ipv6 bgp neighbors *ipv6-addr* **received detail** [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **received prefix-filter** [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

detail

Displays detailed information for ORFs received from BGP4+ neighbors of the device.

vrf *vrf-name*

Specifies a VRF instance.

prefix-filter

Displays the results for ORFs that are prefix-based.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 bgp neighbors received** command when the **prefix-filter** keyword is used.

```
device# show ipv6 bgp neighbors 2001:db8:93e8:cc00::1 received prefix-filter
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors received-routes

Lists all route information received in route updates from BGP4+ neighbors of the device since the soft-reconfiguration feature was enabled.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **received-routes** [**detail**] [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Displays detailed route information.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays the .

```
device# show ipv6 bgp neighbors 160:160:160::10 received-routes

       There are 5 received routes from neighbor 160:160:160::10
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      110:110:110::/64    160:160:160::10  0         100        0      BE
         AS_PATH: 111
2      110:110:110:1::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
3      110:110:110:2::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
4      110:110:110:3::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
5      110:110:110:4::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors rib-out-routes

Displays information about BGP4+ outbound RIB routes.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes** *ipv6-addr mask* [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes detail** *ipv6-addr mask* [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes detail** [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes** [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

detail

Displays detailed RIB route information.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ipv6 bgp neighbors rib-out-routes** command.

```
device# show ipv6 bgp neighbors 123::3 rib-out-routes

       There are 5 RIB_out routes for neighbor 123::3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110:110:110::/64   160:160:160::10  0         100        0      BE
         AS_PATH: 111
2      110:110:110:1::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
3      110:110:110:2::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
4      110:110:110:3::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
5      110:110:110:4::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4+ neighbors.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **routes** [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **routes** [**best** | **not-installed-best** | **unreachable** [**vrf** *vrf-name*]]

show ipv6 bgp neighbors *ipv6-addr* **routes detail** [**best** | **not-installed-best** | **unreachable** [**vrf** *vrf-name*]]

show ipv6 bgp neighbors *ipv6-addr* **routes detail** [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

best
Displays routes received from the neighbor that are the best BGP4+ routes to their destination.

not-installed-best
Displays routes received from the neighbor that are the best BGP4+ routes to their destination but were not installed in the route table because the device received better routes from other sources.

unreachable
Displays routes that are unreachable because the device does not have a valid OSPF or static route to the next hop.

vrf *vrf-name*
Specifies a VRF instance.

detail
Displays detailed information for the specified route types.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ipv6 bgp neighbors routes** command when the **best** keyword is used.

```
device# show ipv6 bgp neighbor 2001:db8::106 routes best
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4+ neighbors.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **routes-summary** [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp neighbors routes-summary** command displays the following information.

Output field	Description
IP Address	The IPv6 address of the neighbor
Routes Received	How many routes the device has received from the neighbor during the current BGP4+ session: • Accepted or Installed - Indicates how many of the received routes the device accepted and installed in the BGP4+ route table. • Filtered or Kept - Indicates how many routes were filtered out, but were nonetheless retained in memory for use by the soft reconfiguration feature. • Filtered - Indicates how many of the received routes were filtered out.
Routes Selected as BEST Routes	The number of routes that the device selected as the best routes to their destinations.
BEST Routes not Installed in IPv6 Forwarding Table	The number of routes received from the neighbor that are the best BGP4+ routes to their destinations, but were nonetheless not installed in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, or static IPv6 routes).
Unreachable Routes	The number of routes received from the neighbor that are unreachable because the device does not have a valid OSPFv3, or static IPv6 route to the next hop.
History Routes	The number of routes that are down but are being retained for route flap dampening purposes.

Output field	Description
NLRIs Received in Update Message	The number of routes received in Network Layer Reachability (NLRI) format in UPDATE messages: • Withdraws - The number of withdrawn routes the device has received. • Replacements - The number of replacement routes the device has received.
NLRIs Discarded due to	Indicates the number of times the device discarded an NLRI for the neighbor due to the following reasons: • Maximum Prefix Limit - The device's configured maximum prefix amount had been reached. • AS Loop - An AS loop occurred. An AS loop occurs when the BGP4+ AS-path attribute contains the local AS number. • Invalid Nexthop Address - The next hop value was not acceptable. • Duplicated Originator_ID - The originator ID was the same as the local router ID. • Cluster_ID - The cluster list contained the local cluster ID, or contained the local router ID (see above) if the cluster ID is not configured.
Routes Advertised	The number of routes the device has advertised to this neighbor: • To be Sent - The number of routes the device has queued to send to this neighbor. • To be Withdrawn - The number of NLRIs for withdrawing routes the device has queued up to send to this neighbor in UPDATE messages.
NLRIs Sent in Update Message	The number of NLRIs for new routes the device has sent to this neighbor in UPDATE messages: • Withdraws - The number of routes the device has sent to the neighbor to withdraw. • Replacements - The number of routes the device has sent to the neighbor to replace routes the neighbor already has.
Peer Out of Memory Count for	Statistics for the times the device has run out of BGP4+ memory for the neighbor during the current BGP4+ session: • Receiving Update Messages - The number of times UPDATE messages were discarded because there was no memory for attribute entries. • Accepting Routes(NLRI) - The number of NLRIs discarded because there was no memory for NLRI entries. This count is not included in the Receiving Update Messages count. • Attributes - The number of times there was no memory for BGP4+ attribute entries. • Outbound Routes (RIB-out) - The number of times there was no memory to place a "best" route into the neighbor's route information base (Adj-RIB-Out) for routes to be advertised. • Outbound Routes Holder - For debugging purposes only.

Examples

This example shows sample output from the **show ipv6 bgp neighbors routes-summary** command.

```
device# show ipv6 bgp neighbors routes-summary
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp peer-group

Displays peer-group information.

Syntax

show ipv6 bgp peer-group *peer-group-name* [**vrf** *vrf-name*]

Parameters

peer-group-name
Specifies a peer group name.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Only the parameters that have values different from their defaults are listed.

Examples

This example shows sample output from the **show ipv6 bgp peer-group** command.

```
device# show ipv6 bgp peer-group

1   BGP peer-group is pg
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Members:
       IP Address: 1.1.1.1, AS: 100
       IP Address: 1::1, AS: 100

2   BGP peer-group is pg6
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Currently there are no members.
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp routes

Displays BGP4+ route information that is filtered by the table entry at which the display starts.

Syntax

show ipv6 bgp routes [*num* | *ipv6-address/prefix* | **age** *num* | **as-path-access-list** *name* | **best** | **cidr-only** | **community-access-list** *name* | **community-reg-expression** *expression* | **detail** | **local** | **neighbor** *ipv6-addr* | **nexthop** *ipv6-addr* | **no-best** | **not-installed-best** | **prefix-list** *string* | **regular-expression** *name* | **route-map** *name* | **summary** | **unreachable**] [**vrf** *vrf-name*]

Parameters

num
Table entry at which the display starts.

ipv6-address/prefix
Table entry at which the display starts.

age
Displays BGP4+ route information that is filtered by age.

as-path-access-list *name*
Displays BGP4+ route information that is filtered by autonomous system (AS)-path access control list (ACL). The name must be between 1 and 32 ASCII characters in length.

best
Displays BGP4+ route information that the device selected as best routes.

cidr-only
Displays BGP4+ routes whose network masks do not match their class network length.

community-access-list *name*
Displays BGP4+ route information for an AS-path community access list. The name must be between 1 and 32 ASCII characters in length.

community-reg-expression *expression*
Displays BGP4+ route information for an ordered community-list regular expression.

detail
Displays BGP4+ detailed route information.

local
Displays BGP4+ route information about selected local routes.

neighbor *ip-addr*
Displays BGP4+ route information about selected BGP neighbors.

nexthop *ip-addr*
Displays BGP4+ route information about routes that are received from the specified next hop.

no-best
Displays BGP4+ route information that the device selected as not best routes.

not-installed-best
Displays BGP4+ route information about best routes that are not installed.

prefix-list *string*
Displays BGP4+ route information that is filtered by prefix list. The string must be between 1 and 32 ASCII characters in length.

regular-expression *name*
Displays BGP4+ route information about routes that are associated with the specified regular expression.

route-map *name*
Displays BGP4+ route information about routes that use the specified route map.

summary
Displays BGP4+ summary route information.

unreachable
Displays BGP4+ route information about routes whose destinations are unreachable through any of the BGP4+ paths in the BGP4+ route table.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows sample input from the **show ipv6 bgp routes** command.

```
device# show ipv6 bgp routes

Total number of BGP Routes: 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      107:1:1::/64       ::              0          100        32768  BL
         AS_PATH:
```

This example shows sample input from the **show ip bgp routes** command when the **summary** keyword is used.

```
device# show ipv6 bgp routes summary

  Total number of BGP routes (NLRIs) Installed     : 1
  Distinct BGP destination networks                : 1
  Filtered bgp routes for soft reconfig            : 0
  Routes originated by this router                 : 1
  Routes selected as BEST routes                   : 1
  Routes Installed as BEST routes                  : 1
  BEST routes not installed in IP forwarding table : 0
  Unreachable routes (no IGP route for NEXTHOP)    : 0
  IBGP routes selected as best routes              : 0
  EBGP routes selected as best routes              : 0
  BEST routes not valid for IP forwarding table    : 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp routes community

Displays BGP4+ route information that is filtered by community and other options.

Syntax

show ipv6 bgp routes community { *num* | **internet** | **local-as** | **no-advertise** | **no-export** } [**vrf** *vrf-name*]

Parameters

community
Displays routes filtered by a variety of communities.

num
Specific community member.

internet
Displays routes for the Internet community.

local-as
Displays routes for a local sub-AS within the confederation.

no-advertise
Displays routes with this community that cannot be advertised to any other BGP4+ devices at all.

no-export
Displays routes for the community of sub-ASs within a confederation.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows output from the **show ipv6 bgp routes community** command when the **internet** keyword is used.

```
device# show ipv6 bgp routes community internet
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 bgp summary

Displays BGP information such as the local autonomous system number (ASN), maximum number of routes supported, and some BGP4+ statistics.

Syntax

show ipv6 bgp summary [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays summary BGP4+ information.

```
device# show ipv6 bgp summary

  BGP4 Summary
  Router ID: 107.1.1.8   Local AS Number: 100
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 1, UP: 0
  Number of Routes Installed: 1, Uses 96 bytes
  Number of Routes Advertising to All Neighbors: 1 (1 entries), Uses 60 bytes
  Number of Attribute Entries Installed: 1, Uses 104 bytes
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  1:2::3            100         CONN      0h 0m18s    0        0        0        1
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 counters interface

Displays ipv6 statistics for an interface.

Syntax

show ipv6 counters interface [**ethernet** *slot/plot* | **loopback** *loopback-number* | **ve** *ve-number*]

Parameters

interface
Specifies an interface.

ethernet *slot/plot*
Specifies physical Ethernet interface and a valid slot and port on it.

loopback *loopback-number*
Specifies the loopback interface.

ve *ve-number*
Specifies the virtual Ethernet (ve) number.

Modes

Privileged EXEC mode

Examples

The following is an example of the **show ipv6 counters interface** command output.

```
device# show ipv6 counters interface ethernet 1/1

 Interface Ethernet 1/1 IPv6 statistics (ifindex 406896641)
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 dhcp relay address interface

Displays IPv6 DHCP Relay addresses configured on supported interfaces.

Syntax

show ipv6 dhcp relay address interface [**ethernet** *slot/port* | **ve** *interface number*]

Parameters

ethernet
Specifies the ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

ve
Specifies the Ve interface.

interface number
Specifies the Ve interface number.

Modes

Privileged EXEC mode

Examples

The following example displays IPv6 DHCP relay address(es) configured per interface.

```
device# show ipv6 dhcp relay address interface ethernet 3/21

Interface              Relay Address                        VRF Name             Outgoing Interface
---------              -------------                        -------------
------------------------
Eth 3/21               4001::101                            default-vrf
Eth 3/21               fe80::8                                blue                        Ve 100
```

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 dhcp relay statistics

Displays general information about the DHCPv6 Relay function.

Syntax

show ipv6 dhcp relay statistics

Modes

Privileged EXEC mode

Usage Guidelines

The **show ipv6 dhcp relay statistics** command displays the following information about the IP DHCP Relay function for IP DHCP Relay addresses configured on the device:

- Number of DHCP Error packets dropped.
- Number of DHCP SOLICIT, REQUEST, CONFIRM, RENEW, REBIND, RELEASE, DECLINE, INFORMATION-REQUEST, RELAY-FORWARD, RELAY-REPLY packets received.
- Number of DHCP RELAY-FORWARD, REPLY packets sent.

Examples

The following example displays statistics for the device.

```
device# show ipv6 dhcp relay statistics

Packets dropped           :  0
    Error                 :  0
Packets received          :  0
    SOLICIT               :  0
    REQUEST               :  0
    CONFIRM               :  0
    RENEW                 :  0
    REBIND                :  0
    RELEASE               :  0
    DECLINE               :  0
    INFORMATION-REQUEST   :  0
    RELAY-FORWARD         :  0
    RELAY-REPLY           :  0
Packets sent              :  0
    RELAY-FORWARD         :  0
    REPLY                 :  0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 interface

Displays details of IPv6 interfaces.

Syntax

show ipv6 interface [**brief** | **ethernet** *slot/port* | **loopback** loopback-port-number | **ve** *ve_id*]

Parameters

brief

Displays brief interface information.

ethernet

Specifies Ethernet interface.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback *loopback-port-number*

Specifies the loopback interface. The range is from 1 to 255.

ve *ve-id*

Specifies the VE ID of a virtual Ethernet (VE) interface. The range is from 1 to 4096.

Modes

Privileged EXEC mode

Interface configuration mode

Examples

The following example displays the output of the **show ipv6 interface** command with an Ethernet interface specified:

```
device# show ipv6 interface ethernet 2/25
 Ethernet 2/25 is up protocol is up
 IPv6 Address: 2025:2525:aaaa::1/64  Primary  Confirmed
 IPv6 Address: 2500:ffee:1234::12/64  Secondary  Confirmed
 IPv6 Address: 2500:ffee:1234::14/64  Secondary  Confirmed
 IPv6 Address: 2500:ffee:1234::16/64  Secondary  Confirmed
 IPv6 Address: fe80::748e:f8ff:fe09:e10d/128  Link-local  Confirmed
 IPv6 multicast groups locally joined:
    ff02::1
    ff02::2    ff02::1:ff00:1    ff02::1:ff00:12
    ff02::1:ff00:14    ff02::1:ff00:16    ff02::1:ff09:e10d

 IPv6 MTU: 1500
 Vrf : default-vrf
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 nd

Displays the router advertisement information.

Syntax

show ipv6 nd interface [**ethernet** *slot/plot* | **prefix** | **ve** *ve-number* | **vrf** *vrf-name*]

Parameters

interface
Specifies an interface.

ethernet *slot/plot*
Specifies physical Ethernet interface and a valid slot and port on it.

prefix
Displays prefix information.

ve *ve-number*
Specifies the virtual Ethernet (ve) number.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following is an example of the **show ipv6 nd** command output.

```
device# show ipv6 nd interface ethenet 3/5
ICMPv6 ND Interfaces for VRF  default-vrf
  IPv6 address:  2ffe::1
  Router-Advertisement active timers:
    Last Router-Advertisement sent: 00:01:25
    Next Router-Advertisement sent in: 00:07:06
  Router-Advertisement parameters:
    Periodic interval:  200 to 600 seconds
    Send 'Managed Address Configuration' flag: false
    Send 'Other Stateful Configuration' flag: false
    Send 'Current Hop Limit' field: 64
    Send 'MTU' option value: 1500
    Send 'Router Lifetime' field: 1800 secs
    Send 'Reachable Time' field: 0 ms
    Send 'Retrans Timer' field: 0 ms
    Suppress RA: false
    Suppress MTU in RA: false
    Suppress All RA: false
  Neighbor-Solicitation parameters:
    NS retransmit interval: 1 secs
    DAD Attempts: 2
    DAD expiry: 1 secs
  Neighbor Cache Expiry: 14400 secs
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 nd suppression-cache

Displays IPv6 neighbor discovery (ND)-suppression information.

Syntax

show ipv6 nd suppression-cache [**summary**]

show ipv6 nd suppression-cache bridge-domain *bridge-domain-id*

show ipv6 nd suppression-cache vlan *vlan-id*

Parameters

summary

Specifies summary format.

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 nd suppression-cache** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
IP	Displays the IPv6 address.
Mac	Displays the MAC address.
Interface	Displays the interface type and ID. "Tu" represents a tunnel interface, followed by the end-point IP.
Age	In hh:mm:ss format, displays the time since the most recent renewal of a dynamic entry. For a static entry, displays "Never".
Flags	Displays "L" (locally learned adjacency), "R" (remote learned adjacency), or RS (remote static adjacency).

Examples

The following example displays the results of the basic form of this command.

```
device# show ipv6 nd suppression-cache
Flags: L  - Locally Learnt Adjacency
       R  - Remote Learnt Adjacency
       RS - Remote Static Adjacency
Vlan/Bd IP                        Mac            Interface                   Age      Flags
-------------------------------------------------------------------------------------------
4006(V) fd80:113:114:1:4006::114  609c.9fb1.1401 Tu 61441 (114.114.114.114) Never    RS
4006(V) fd80:113:114:1:4006::1001 00ef.4006.3601 Eth 0/41                   00:00:17 L
4006(V) fd80:113:114:1:4006::1002 00ef.4006.3602 Eth 0/41                   00:00:17 L
4006(V) fe80::1                   00ef.4006.3601 Eth 0/41                   00:16:16 L
4006(V) fe80::2                   00ef.4006.3602 Eth 0/41                   00:16:16 L
4006(V) fe80::629c:9fff:feb1:1401 609c.9fb1.1401 Tu 61441 (114.114.114.114) Never    RS
4007(V) fd80:113:114:1:4007::1001 00ef.4007.4601 Tu 61441 (114.114.114.114) Never    R
4007(V) fd80:113:114:1:4007::1002 00ef.4007.4602 Tu 61441 (114.114.114.114) Never    R
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 nd suppression-statistics

Displays IPv6 neighbor discovery (ND)-suppression statistics.

Syntax

show ipv6 nd suppression-statistics

show ipv6 nd suppression-statistics bridge-domain *bridge-domain-id*

show ipv6 nd suppression-statistics vlan *vlan-id*

Parameters

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 nd suppression-statistics** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
Forwarded	Displays the number of packets forwarded.
Suppressed	Displays the number of packets suppressed.
Proxy Nd	Displays the number of packets for which the device has sent proxy-Nd replies.

Examples

The following example displays the results of the basic form of this command.

```
device# show ipv6 nd suppression-statistics
Vlan/Bd         Forwarded     Suppressed    Proxy Nd
-----------------------------------------------------------
110 (V)         0             117           0
254 (V)         3             10            0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 nd suppression-status

Displays the IPv6 neighbor discovery (ND)-suppression status.

Syntax

show ipv6 nd suppression-status

show ipv6 nd suppression-status bridge-domain *bridge-domain-id*

show ipv6 nd suppression-status vlan *vlan-id*

Parameters

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 nd suppression-status** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
Configuration	Displays "Enabled" or "Disabled".
Evpn-Register	Displays "Yes" if the VLAN is extended through EVPN or "No" if it is not extended.
Operation	Displays "Active" or "Inactive".

Examples

The following example displays the results of the basic form of this command.

```
device# show ipv6 nd suppression-status
Vlan/Bd          Configuration   Evpn-Register   Operation
-------------------------------------------------------
4003 (V)         Enabled         Yes             Active
4005 (V)         Disabled        No              Inactive
4006 (V)         Enabled         Yes             Active
4007 (V)         Enabled         Yes             Active
4090 (V)         Disabled        No              Inactive
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 neighbor

Displays the IPv6 neighbors.

Syntax

show ipv6 neighbor [*ipv6-address*] [**vrf** *vrf-name*]

show ipv6 neighbor [**dynamic** | **static**] [**summary**] [**vrf** *vrf-name*]

show ipv6 neighbor [**ethernet** *slot* **/** *port* | **ve** *ve-num*] [**vrf** *vrf-name*]

Parameters

ipv6-address
Restricts the display to the entries for the specified IPv6 address. Specify this parameter in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

static
Displays the static IPv6 neighbors.

dynamic
Displays the dynamic IPv6 neighbors .

summary
Displays the summary of IPv6 neighbors.

ve *ve-num*
Restricts the display to the entries for the specified VE interface. The range is from 1 to 4096.

vrf *vrf-name*
Displays the IPv6 neighbor information for the specified Virtual Routing/Forwarding (VRF) instance.

Modes

Privileged EXEC mode

Examples

The following example is output of the **show ipv6 neighbor summary** command.

```
device# show ipv6 neighbor summary
Static Entries          : 0
Dynamic Entries         : 0
Leaked Entries          : 0
Pre-arp Entries         : 0
Evpn Entries            : 0
Evpn Sticky Entries     : 0
Total Entries           : 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf

Displays OSPFv3 information.

Syntax

show ipv6 ospf [**vrf** *name*]

Parameters

vrf *name*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the show ipv6 ospf command.

```
device# show ipv6 ospf
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf area

Displays the OSPFv3 area table in a specified format.

Syntax

show ipv6 ospf area [*A.B.C.D*] [*decimal*] [**vrf** *vrfname*]

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format. Valid values range from 0 to 2147483647.

vrf vrf *name*

Specifies a non-default VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 ospf area** command when no arguments or keywords are used.

```
device# show ipv6 ospf area
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf database

Displays lists of information about different OSPFv3 link-state advertisements (LSAs).

Syntax

show ipv6 ospf database [**advrtr** *A.B.C.D* | **extensive** | **grace** | **link-id** *decimal* | **prefix** *ipv6-addr*] [**vrf** *vrfname*]

show ipv6 ospf database [**as-external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** [*decimal*] | **network** | **router** | **type-7**] [**advrtr** *A.B.C.D* | **link-id** *decimal*] [**vrf** *vrfname*]

show ipv6 ospf database scope { **area** { *A.B.C.D* | *decimal* } | **as** | **link** } [**vrf** *vrfname*]

show ipv6 ospf database summary [**all-vrfs** | **vrf** *vrfname*]

Parameters

advrtr *A.B.C.D*
Displays LSAs by Advertising Router Id in dotted decimal format.

extensive
Displays detailed lists of LSA information.

grace
Displays grace LSA information.

link-id *decimal*
Link-state ID that differentiates LSAs. Valid values range from 1 through 4294967295.

prefix
Display LSAs that contain a prefix.

ipv6-addr
Specifies an IPv6 address.

vrf vrf *name*
Specifies a non-default VRF instance.

as-external
Displays information about external LSAs.

inter-prefix
Displays information about inter area prefix LSAs.

inter-router
Displays information about inter area router LSAs.

intra-prefix
Displays information about intra area prefix LSAs.

link *decimal*
Displays information about the link LSAs.

network
Displays information about network LSAs.

router
Displays information about router LSAs.

type-7
Displays information about the not so stubby area (NSSA) external LSAs.

scope
Displays LSA information by LSA scope.

area
Displays LSAs by scope within a specified area.

as
Displays autonomous system (AS) LSAs by scope.

link
Displays link LSAs by scope.

summary
Displays LSA summary information.

all-vrfs
Specifies all VRFs.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf database as-external** command using the **link-id** keyword:

```
device# show ipv6 ospf database as-external link-id 5
```

The following is sample output from the **show ipv6 ospf database inter-prefix** command using the **link-id** keyword:

```
device# show ipv6 ospf database inter-prefix link-id 5
```

The following is sample output from the **show ipv6 ospf database network** command:

```
device# show ipv6 ospf database network
```

The following is sample output from the **show ipv6 ospf database router** command:

```
device# show ipv6 ospf database router
```

The following is sample output from the **show ipv6 ospf database type-7** command:

```
device# show ipv6 ospf database type-7
```

The following is sample output from the **show ipv6 ospf database scope** command using the **area** keyword:

```
device# show ipv6 ospf database scope area 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf interface

Displays interface information for all or specific OSPFv3-enabled interfaces.

Syntax

show ipv6 ospf interface brief [**all-vrfs** | **vrf** *vrf-name*]

show ipv6 ospf interface [**ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id*]

show ipv6 ospf interface [**vrf** *vrf-name*]

Parameters

brief
Displays summary information.

all-vrfs
Displays the information for all VRF instances.

vrf *vrf-name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

ethernet *slot/port*
Specifies an Ethernet slot and port.

loopback *number*
Specifies a loopback port number. Valid values range from 1 through 255.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf interface** command when no arguments or keywords are used.

The following is sample output from the **show ipv6 ospf interface** command the **brief** keyword is used.

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf memory

Displays information about OSPFv3 memory usage.

Syntax

show ipv6 ospf memory [**vrf** *vrfname*]

Parameters

vrf *vrfname*

Displays the information for the specified VRF instance.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf memory vrf** *vrf-name* command:

```
device# show ipv6 ospf memory vrf vrf-1
   Total Dynamic Memory Allocated for this instance : 87046288 bytes
global shared memory pool for all instances
   Memory Type               Size       Allocated  Max-alloc  Alloc-Fails
   MTYPE_OSPF6_AREA          1100       1024       1065       0
   MTYPE_OSPF6_AREA_RANGE    52         0          16         0
   MTYPE_OSPF6_SUMMARY_ADDRE 36         0          16         0
   MTYPE_OSPF6_IF            396        2048       2625       0
   MTYPE_OSPF6_NEIGHBOR      24916      2048       2098       0
   MTYPE_OSPF6_ROUTE_NODE    36         71666      72415      0
   MTYPE_OSPF6_ROUTE_INFO    52         71666      80537      0
   MTYPE_OSPF6_PREFIX        24         0          16         0
   MTYPE_OSPF6_LSA           252        76787      133135     0
   MTYPE_OSPF6_VERTEX        196        5120       5327       0
   MTYPE_OSPF6_SPFTREE       60         1024       1056       0
   MTYPE_OSPF6_NEXTHOP       32         5134       8192       0
   MTYPE_OSPF6_EXTERNAL_INFO 52         0          1024       0
   MTYPE_THREAD              68         14703      15192      0
   MTYPE_OSPF6_LINK_LIST     44         6849444    7050698    0
   MTYPE_OSPF6_LINK_NODE     28         170996     265654     0
   MTYPE_OSPF6_LSA_RETRANSMI 20         0          25598      0
Global Memory Pool Usage for all instances : 415468328 bytes
global Heap memory for all instances
   Memory Type               Size       Allocated  Max-alloc  Alloc-Fails
   MTYPE_OSPF6_TOP           41104      1024       1024       0
   MTYPE_OSPF6_LSA_HDR       416        76787      107723     0
   MTYPE_OSPF6_RMAP_COMPILED 0          0          0          0
   MTYPE_OSPF6_OTHER         96         132591     137421     0
   MTYPE_THREAD_MASTER       200        1024       1024       0
---------------------
Packet Tx thread Info
---------------------
Queue Id[0]: Enqueued[291763] Dequeued [291763]
Queue Id[1]: Enqueued[13108] Dequeued [13108]
Send Failed Packets - 0
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf neighbor

Displays detailed or summary OSPFv3 neighbor information.

Syntax

show ipv6 ospf neighbor [**all-vrfs** | **vrf** *vrf-name*]

show ipv6 ospf neighbor detail [**vrf** *vrf-name*]

show ipv6 ospf neighbor interface [**ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id*]

show ipv6 ospf neighbor router-id *A.B.C.D* [**vrf** *vrf-name*]

Parameters

all-vrfs
Specifies all VRF instances.

vrf *vrf-name*
Specifies a non-default VRF instance.

detail
Displays detailed neighbor information.

interface
Displays OSPFv3 interface information.

ethernet *slot/port*
Specifies an Ethernet slot and port.

loopback *number*
Specifies a loopback port number. Valid values range from 1 through 255.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

router-id *A.B.C.D*
Specifies neighbor information for the specified router ID (in dotted decimal format).

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 ospf neighbor** command when no arguments or keywords are used.

```
device# show ipv6 ospf neighbor
Total number of neighbors in all states: 1
Number of neighbors in state Full      : 1

RouterID        Pri State  DR              BDR             Interface     State   QCount
1.4.4.4         1 Full     100.5.5.5       1.4.4.4         Eth 1/13      DR      0
device#
```

The following example shows sample output from the **show ipv6 ospf neighbor detail** command when no arguments or keywords are used.

```
device# show ipv6 ospf neighbor detail
Total number of neighbors in all states: 1
Number of neighbors in state Full      : 1

RouterID        Pri State  DR              BDR             Interface     State   QCount
1.4.4.4         1 Full     100.5.5.5       1.4.4.4         Eth 1/13      DR      0
                Option: 00-00-00    Timer: 692
BFD State: NONE, BFD HoldoverInterval(sec):Configured: 0 Current: 0
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf redistribute route

Displays all IPv6 routes or a specified IPv6 route that the device has redistributed into OSPFv3.

Syntax

show ipv6 ospf redistribute route *A.B.C.D:M* [**vrf** *vrf-name*]

show ipv6 ospf redistribute route [**vrf** *vrf-name*]

Parameters

A.B.C.D:M
Specifies an IPv6 address.

vrf *vrfname*
Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf redistribute route** command when no arguments or keywords are used:

```
device# show ipv6 ospf redistribute route
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf routes

Displays OSPFv3 routes.

Syntax

show ipv6 ospf routes *A.B.C.D:M* [**vrf** *vrfname*]

show ipv6 ospf routes [**vrf** *vrfname*]

Parameters

A.B.C.D:M
Specifies a destination IPv6 address.

vrf *vrfname*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays OSPFv3-calculated routes.

```
device# show ipv6 ospf routes
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf spf

Displays OSPFv3 SPF node, table, and tree information.

Syntax

show ipv6 ospf spf { **node** | **table** | **tree** } [**area** { *A.B.C.D* | *decimal* }] [**vrf** *vrfname*]

Parameters

node
: Displays OSPFv3 node information.

table
: Specifies a SPF table.

tree
: Specifies a SPF tree.

area
: Specifies an area.

A.B.C.D
: Area address in dotted decimal format.

decimal
: Area address in decimal format.

vrf *vrfname*
: Specifies an non-default VRF instance.

Examples

The following example shows sample output from the **show ipv6 ospf spf** command when the **node** keyword is used.

```
device# show ipv6 ospf spf node
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf summary

Displays summary information for all OSPFv3 instances.

Syntax

show ipv6 ospf summary [**all-vrfs** | **all-vrfs total** | **vrf** *vrfname*]

Parameters

all-vrfs

Specifies all VRF instances. If this option is not used, details for the default VRF are shown in the output.

vrf *vrfname*

Specifies a non-default VRF instance. If this option is not used, details for the default VRF are shown in the output.

all-vrfs total

Displays the cumulative summary of OSPF information with the total numbers for all of the VRF intances. If this option is not used, details for the default VRF are shown in the output. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows sample default VRF output from the **show ipv6 ospf summary** command when no arguments or keywords are used.

```
device# show ipv6 ospf summary
Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     0       0       0         0       0
```

The following example shows sample output from the **show ipv6 ospf summary all-vrfs total** command.

```
device# show ipv6 ospf summary all-vrfs total

----------------------------------------
         IPv6 OSPF Summary Total
----------------------------------------
Number of instances: 1024
Number of interfaces: 2048
Number of neighbors: 2048
Number of neighbors in FULL state: 2048
Number of LSAs: 76786
Number of Routes: 67570
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf virtual-links

Displays information about all OSPFv3 virtual links or specified links.

Syntax

show ipv6 ospf virtual-links brief [**vrf** *vrfname*]

show ipv6 ospf virtual-links [**vrf** *vrfname*]

Parameters

brief
Displays summary information.

vrf *vrfname*
Specifies a non-default VRF instance.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf virtual-links** command when no arguments or keywords are used:

```
device# show ipv6 ospf virtual-links
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 ospf virtual-neighbor

Displays information about OSPFv3 virtual neighbors.

Syntax

show ipv6 ospf virtual-neighbor brief [**vrf** *vrfname*]

show ipv6 ospf virtual-neighbor [**vrf** *vrfname*]

Parameters

brief

Displays summary information.

vrf *vrfname*

Specifies a nondefault VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 ospf virtual-neighbor** command when no arguments or keywords are used.

```
device# show ipv6 ospf virtual-neighbor
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 prefix-list

Displays IPv6 prefix-lists.

Syntax

show ipv6 prefix-list *prefix-list-name*

Parameters

prefix-list-name
Specifies an IPv6 prefix list name.

Modes

User EXEC mode

Usage Guidelines

The *prefix-list-name* parameter restricts the display to the specified prefix list. Specify the name of the prefix list that you want to display.

Command Output

The **show ipv6 prefix-list** command displays the following information:

Examples

The following example shows how to display IPv6 prefix lists.

```
device# show ipv6 prefix-lists
ipv6 prefix-list routesfor2001: 2 entries
     seq 5 permit 2001::/16
     seq 10 permit 2001:db8::/32
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 route

Displays the router advertisement information.

Syntax

show ipv6 route [**all** | **bgp** | **connected** | **import** *source-name* | **nexthop** *nexthop-id* | **ospf** | **static** | **summary** | **system-summary**] *vrf-name*

show ipv6 route [**slot** *linecard-number* | **static** | **system-summary** | **vrf** *number*]

Parameters

all
Specifies all routes.

bgp
Specifies BGP routes.

connected
Displays the directly connected routes.

import *source-name*
Specifies import routes and the source VRF name

nexthop *nexthop-id*
Displays the route nexthop table.

ospf
Specifies OSPF routes.

slot *linecard-number*
Specifies the IPv6 route information on a slot and the linecard number.

static
Specifies static IPv6 routes.

summary
Displays the route summary.

system-summary
Displays the system-level summary for IPv6 routes.

vrf-name
The name of the VRF context.

vrf *number*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following is an example of the **show ipv6 route** command output.

```
SLX# show ipv6 route
IPv6 Routing Table for VRF "default-vrf"
Total number of IPv6 routes: 11
'*' denotes best ucast next-hop
'[x/y]' denotes [preference/metric]

1200:1201::/64, attached
    *via ::, Eth 2/45, [0/0], 45m29s, direct, tag 0
1200:1201::1:1/128, attached
    *via ::, Eth 2/45, [0/0], 45m29s, local, tag 0
1200:1202::/64, attached
    *via ::, Ve 2, [0/0], 45m26s, direct, tag 0
1200:1202::1:1/128, attached
    *via ::, Ve 2, [0/0], 45m26s, local, tag 0
2221::/32
    *via 1200:1201::1:2, Eth 2/45, [100/10], 11m41s, static, tag 300
2222::/48
    *via fe80::205:33ff:fee6:a531, Eth 2/45, [1/1], 43m44s, static, tag 0
2222::1/128
    *via fe80::205:33ff:fee6:a531, Eth 2/45, [110/1], 0m7s, ospfv3, intra, tag 0
2223::/64
    *via 1200:1202::1:2, Ve 2, [1/1], 3m45s, static, tag 0
2224::1/128
    *via fe80::205:33ff:fee6:a501, Ve 2, [1/1], 43m41s, static, tag 0
fe80::/10, attached
    *via ::, , [0/0], 6h30m, local, tag 0
ff00::/8, attached
    *via ::, Null0, [0/0], 6h30m, local, tag 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 static route

Displays information about IPv6 static routes.

Syntax

show ipv6 static route [*ipv6prefix* | **vrf** *vrf-name*]

Parameters

ipv6prefix

The IPv6 prefix in the *A:B::/length* format.

vrf vrf-name

The name of the VRF context.

Modes

Privileged EXEC mode

Examples

The following example displays the IPv6 static route information for the default VRF.

```
device# show ipv6 static route
IPv6 Configured Static Routes for VRF "default-vrf"

3002:7::/64-> 1200:3::1:2 preference: 1
   nh_vrf (default-vrf)

3002:9::/64-> 1200:4::1:2 preference: 1
   nh_vrf (default-vrf)
device#
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ipv6 vrrp

Displays information about IPv6 VRRP and VRRP-E sessions.

Syntax

show ipv6 vrrp

show ipv6 vrrp *VRID* [**detail** | **summary**]

show ipv6 vrrp detail

show ipv6 vrrp summary [**vrf** { *vrf-name* | **all** | **default-vrf** }]

show ipv6 vrrp interface { **ethernet** *slot*/*port* } [**detail** | **summary**]

show ipv6 vrrp interface ve *vlan_id* [**detail** | **summary**]

Parameters

VRID
The virtual group ID about which to display information. The range is from 1 through 16.

detail
Displays all session information in detail, including session statistics.

summary
Displays session-information summaries.

vrf
Specifies a VRF instance or all VRFs.

vrf-name
Specifies a VRF instance. For the default vrf, enter **default-vrf**.

all
Specifies all VRFs.

interface
Displays information for an interface that you specify.

ethernet *slot port*
Specifies a valid, physical Ethernet interface with a slot and port number.

ve *vlan_id*
Specifies the VE VLAN number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about IPv6 VRRP and VRRP-E sessions, either in summary or full-detail format. You can also specify a particular virtual group ID, or an interface for which to display VRRP output.

NOTE
IPv6 VRRP-E supports only the VE interface type.

To display information for IPv6 VRRP sessions using the default VRF, you can use the **show ipv6 vrrp summary** syntax (with no additional parameters).

To display information for the default or a named VRF, you can use the **show ipv6 vrrp summary vrf** syntax with the *vrf-name* option.

To display information about all VRFs, use the **show ipv6 vrrp summary vrf all** syntax.

Examples

The following example displays information about all IPv6 VRRP sessions on the device.

```
device# show ipv6 vrrp

Total number of VRRP session(s)    : 2

VRID 14
  Interface: Ve 2018;  Ifindex: 1207961570
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): fe80::1
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1000 milli sec  (default: 1000 milli sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========
  Statistics:
    Advertisements: Rx: 0, Tx: 35
    Neighbor Advertisements: Tx: 1

VRID 15
  Interface: Ve 2019;  Ifindex: 1207961571
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): fe80::1
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1000 milli sec  (default: 1000 milli sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========
  Statistics:
    Advertisements: Rx: 0, Tx: 448
    Neighbor Advertisements: Tx: 1
```

The following example displays IPv6 VRRP information in detail for a specific virtual group ID of 19, including session statistics.

```
device# show ipv6 vrrp 19 detail

Total number of VRRP session(s)   : 1
VRID 15
  Interface: Ve 2019;  Ifindex: 1207961571
  Mode: VRRPE
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Backup
  Session Master IP Address: fe80::205:33ff:fe79:fb1e
  Virtual IP(s): 2001:2019:8192::1
  Virtual MAC Address: 02e0.5200.2513
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: DISABLE  (default: DISABLED)
  Advertise-backup: ENABLE  (default: DISABLED)
  Backup Advertisement interval: 60 sec  (default: 60 sec)
  Short-path-forwarding: Enabled
  Revert-Priority: unset; SPF Reverted: No
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========
  Global Statistics:
  ==================
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0
  Session Statistics:
  ===================
    Advertisements             : Rx: 103259, Tx: 1721
    Neighbor Advertisements             : Tx: 0
    Session becoming master    : 0
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0
    VRRPE backup advt sent     : 1721
    VRRPE backup advt recvd    : 0
```

The following example displays summary information for IPv6 VRRP statistics on the default VRF. (This command is equivalent to **show ipv6 vrrp summary vrf default-vrf**.)

```
device# show ipv6 vrrp summary

Total number of VRRP session(s)   : 1
Master session count  : 1
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
15    VRRPE    Ve 2019    Enabled 100       Master   Enabled     unset     No
```

The following example displays summary information for IPv6 VRRP statistics on the VRF named red.

```
device# show ipv6 vrrp summary vrf red

Total number of VRRP session(s)   : 1
Master session count  : 1
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
14    VRRPE    Ve 2018    Enabled 100       Master   Enabled     unset     No
```

The following example displays summary information for IPv6 VRRP statistics on all VRFs.

```
device# show ipv6 vrrp summary vrf all

Total number of VRRP session(s)   : 2
Master session count  : 2
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
14    VRRPE    Ve 2018    Enabled 100       Master   Enabled     unset     No
15    VRRPE    Ve 2019    Enabled 100       Master   Enabled     unset     No
```

The following example displays information for IPv6 VRRP-E tracked networks.

```
device# show ipv6 vrrp detail

Total number of VRRP session(s)   : 1

VRID 2
  Interface: Ve 100;  Ifindex: 1207959652
  Mode: VRRPE
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 2001:2019:8192::1
  Virtual MAC Address: 02e0.5225.1002
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: DISABLE  (default: DISABLED)
  Advertise-backup: DISABLE  (default: DISABLED)
  Backup Advertisement interval: 60 sec  (default: 60 sec)
  Short-path-forwarding: Disabled
  Revert-Priority: unset; SPF Reverted: No
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========

  Tracknetwork:
    Network(s)                Priority  Status
    =========                 ========  ==========
    2001::/64                 20        Up

  Global Statistics:
  ==================
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0

  Session Statistics:
  ===================
    Advertisements             : Rx: 0, Tx: 132
    Neighbor Advertisements           : Tx: 66
    Session becoming master    : 1
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0
    VRRPE backup advt sent     : 0
    VRRPE backup advt recvd    : 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

Show J through Show Z

show lacp

Displays the Link Aggregation Control Protocol (LACP) traffic statistics for a specific port-channel or for all port-channels; or displays the system ID.

Syntax

show lacp { **counter** [*port-channel*] | **sys-id** }

Parameters

counters

Displays LACP statistics for all port-channel interfaces.

port-channel

Displays counters for a specific port channel interface. Valid values range from 1 through 64.

sys-id

Displays the system ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the LACP statistics for each port-channel interface for all port-channel interfaces or a single port-channel interface, or by system ID.

Examples

The following example displays the LACP statistics for all port-channels.

```
device# show lacp counter
 Traffic statistics
Port            LACPDUs            Marker           Pckt err
              Sent     Recv     Sent     Recv     Sent     Recv
 Aggregator Po 11
Eth 0/49      5271     5172     0        0        0        0

 Aggregator Po 12
Eth 0/50      5294     5198     0        0        0        0

 Aggregator Po 13
Eth 0/51      5260     5187     0        0        0        0
Eth 0/52      0        0        0        0        0        0
```

The following example displays the local system ID.

```
device# show lacp sys-id
System ID: 0x8000,00-04-96-9f-5d-5c
```

History

Release version	Command history
18x.1.00	This command was introduced.

show link-oam info

Displays the link OAM information.

Syntax

show link-oam info

Modes

Privileged EXEC mode

Command Output

The **show link-oam info** command displays the following information:

Output field	Description
Ethernet Port	Indicates the ethernet port where the EFM-OAM is enabled.
Link Status	Indicates whether the physical link is operational (up) or has any fault (down).
OAM Status	Indicates the status of OAM on the link between the local and remote DTEs. The status is enabled if the OAM client is satisfied with the local and remote settings.
Mode	Indicates whether the DTE is in active or passive modes. Active DTEs can start the discovery process and passive DTEs can only respond.
Local Stable	Indicates the reception of the remote DTE state information and is satisfied with the remote OAM settings.
Remote Stable	Indicates the reception of the local DTE state information at the remote DTE and is satisfied with the local OAM settings.

Examples

The following example displays sample output from the **show link-oam info** command.

```
device#show link-oam info
Ethernet Link Status     OAM Status      Mode       Local Stable    Remote Stable
1/1      up              up              active     satisfied       satisfied
1/2      up              up              passive    satisfied       satisfied
1/3      up              up              active     satisfied       satisfied
1/4      up              init            passive    unsatisfied     unsatisfied
1/5      down            down            passive    unsatisfied     unsatisfied
1/6      down            down            passive    unsatisfied     unsatisfied
1/7      down            down            passive    unsatisfied     unsatisfied
```

History

Release version	Command history
18x.1.00	This command was introduced.

show link-oam info detail

Displays the detailed dump of the link OAM internal state for all ports.

Syntax

show link-oam info detail

Modes

Privileged EXEC mode

Command Output

The **show link-oam info detail** command displays the following information:

Output field	Description
Local information	Displays the local information.
Remote information	Displays the remote information.

Examples

This example displays the detailed dump of Link OAM statistics for all ports:

```
device# show link-oam info detail
OAM information for Ethernet port: 2/1
        +link-oam mode:        active
        +link status:          up
        +oam status:           init
        Local information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                state:               activeSend
                dying-gasp:          false
                critical-event:      false
                link-fault:          false
        Remote information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                dying-gasp:          false
                critical-event:      false
                link-fault:          false

OAM information for Ethernet port: 2/2
        +link-oam mode:        passive
        +link status:          down
        +oam status:           init
        Local information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                state:               down
                dying-gasp:          false
                critical-event:      false
                link-fault:          false
        Remote information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                dying-gasp:          false
                critical-event:      false
                link-fault:          false
```

History

Release version	Command history
18x.1.00	This command was introduced.

show link-oam statistics

Display the link OAM statistics.

Syntax

show link-oam statistics

Modes

Privileged EXEC mode

Command Output

The **show link-oam statistics** command displays the following information:

Output field	Description
Ethernet Port	Indicates the ethernet port where the EFM-OAM is enabled.
Tx PDUs	Indicates the number of PDUs transmitted.
Rx PDUs	Indicates the number of PDUs received.

Examples

The following example displays sample output from the **show link-oam statistics** command.

```
device# show link-oam statistics
Ethernet Tx PDUs    Rx PDUs
2/1         93         92
2/2            45         46
```

History

Release version	Command history
18x.1.00	This command was introduced.

show link-oam statistics detail

Displays the detailed dump of Link OAM statistics for all ports.

Syntax

show link-oam statistics detail

Modes

Privileged EXEC mode

Command Output

The **show link-oam statistics detail** command displays the following information:

Output field	Description
Tx statistics	Details the data transmitted.
Rx statistics	Details the date received.

Examples

This example displays the detailed dump of Link OAM statistics for all ports:

```
device# show link-oam statistics detail
OAM statistics for Ethernet port: 1/1
        Tx statistics
                information OAMPDUs:                    587
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
        Rx statistics
                information OAMPDUs:                    442
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                unsupported OAMPDUs:                    0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
                discarded TLVs:                         0
                unrecognized TLVs:                      0
OAM statistics for Ethernet port: 1/2
        Tx statistics
                information OAMPDUs:                    440
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
        Rx statistics
                information OAMPDUs:                    441
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                unsupported OAMPDUs:                    0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
                discarded TLVs:                         0
                unrecognized TLVs:                      0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show lldp interface

Displays the LLDP status on the specified interface.

Syntax

show lldp interface [**ethernet** *slot/port*]

Parameters

ethernet

Use this parameter to specify an Ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **ethernet** *slot/port* parameter is not specified, this command displays the LLDP status information received on all the interfaces.

Examples

To display all the LLDP ethernet interface information, enter the following:

```
device# show lldp interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
  1/1
  1/2
  1/3
  1/4
  1/5
  1/6
  1/8
  1/9
  1/10
  1/11
  1/12
  1/13
  1/14
  1/15
  1/16
  1/17
  1/18
  1/19
  1/20
  1/21
  1/22
  1/23
```

To display the LLDP interface information for a specified ethernet interface, enter the following:

```
device# show lldp interface ethernet 1/18
LLDP information for Eth 1/18
  State:                   Enabled
  Mode:                    Receive/Transmit
  Advertise Transmitted:   30 seconds
  Hold time for advertise: 120 seconds
  Tx Delay Timer:          1 seconds
  Transmit TLVs:           Chassis ID              Port ID
                           TTL                     Port Description
                           System Name
```

History

Release version	Command history
18x.1.00	This command was introduced.

show lldp neighbors

Displays LLDP information for all neighboring devices on the specified interface.

Syntax

show lldp neighbors [**interface** [**ethernet** *slot/port*]] [**detail**]

Parameters

ethernet

Use this parameter to specify an Ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

detail

Specifies the details of the LLDP neighbor information.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display LLDP information for all neighboring devices on the specified interface.

Examples

To display LLDP neighbor information on a specific interface, enter the following:

```
device# show lldp neighbors interface ethernet 1/18
Local Port  Dead Interval  Remaining Life  Remote Port ID   Remote Port Descr Chassis ID       Tx  Rx
System Name
Eth 1/18      120            115            Ethernet 2/25    Eth 2/25        768e.f807.6000   655 654
R6
```

To display detailed LLDP neighbor information on a specific interface, enter the following:

```
device# show lldp neighbors interface ethernet 1/18 detail
Neighbors for Interface Eth 1/18

MANDATORY TLVs
==============
Local Interface: Eth 1/18  (Local Interface MAC: 768e.f805.5816)
Remote Interface: Ethernet 2/25 (Remote Interface MAC: 768e.f807.610d)
Dead Interval: 120 secs
Remaining Life : 118 secs
Chassis ID: 768e.f807.6000
LLDP PDU Transmitted: 656  Received: 655

OPTIONAL TLVs
==============
Port Interface Description: Eth 2/25
System Name: R6
```

History

Release version	Command history
18x.1.00	This command was introduced.

show lldp statistics

Displays the LLDP statistics on all interfaces or a specified interface.

Syntax

show lldp statistics [**interface** [**ethernet***slot/port*]]

Parameters

ethernet

Use this parameter to specify an Ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify an interface, this command displays the LLDP statistics for all interfaces.

Examples

To display LLDP statistics on the specified interface:

```
device# show lldp statistics interface ethernet 1/18
LLDP Interface statistics for Eth 1/18
Frames transmitted: 659
Frames Aged out:    0
Frames Discarded:   0
Frames with Error:  0
Frames Recieved:    657
TLVs discarded:     0
TLVs unrecognized:  0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show logical-interface bridge-domain

Displays detailed or brief information regarding all logical interfaces (LIFs) associated with a bridge domain (BD).

Syntax

show logical-interface bridge-domain { *BD_ID* [**brief**]}

Parameters

BD_ID

Specifies a bridge domain ID.

brief

Displays brief information

Modes

Privileged EXEC mode

Command Output

The **show logical-interface bridge-domain** command displays the following information:

Output field	Description
AC LIF	
VFI LIF	
LIF ifindex	Interface index of the LIF
LIF Name	Name of the LIF
FLAG	Indicates status of tagging, administrative state, and protocol layer
Outer VLAN ID	ID of the outer VLAN
Inner VLAN ID	ID of the inner VLAN
Ingress Stats Index	
Egress Stats Index	

Examples

The following example displays detailed information.

```
device# show logical-interface bridge-domain 1
AC LIF Count: 3, VFI LIF Count:0
      logical-interface ethernet 1/2.100
      LIF ifindex: 0x2c000041, Service Instance:0x00000064
      LIF Name: AC_LIF_100
      IVID:4097 (0x1001), Encap ID: 0x2020
      FLAG:0x6
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
      Outer VLAN ID:100 (0x64), Inner VLAN ID:65535 (0xffff)
      Ingress Stats Index: Inv, Egress Stats Index: Inv

      logical-interface ethernet 1/2.101
      LIF ifindex: 0x2c000062, Service Instance:0x00000065
      LIF Name: AC_LIF_101
      IVID:4097 (0x1001), Encap ID: 0x2021
      FLAG:0x6
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
      Outer VLAN ID:101 (0x65), Inner VLAN ID:65535 (0xffff)
      Ingress Stats Index: Inv, Egress Stats Index: Inv

      logical-interface ethernet 1/2.102
      LIF ifindex: 0x2c000044, Service Instance:0x00000066
      LIF Name: AC_LIF_DUAL_TAG
      IVID:4097 (0x1001), Encap ID: 0x2030
      FLAG:0x6
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
      Outer VLAN ID:102 (0x64), Inner VLAN ID:200 (0xC8)
      Ingress Stats Index: Inv, Egress Stats Index: Inv
```

The following example displays brief information.

```
device# show logical-interface bridge-domain 1 brief
AC LIF Count: 3, VFI LIF Count:0
      logical-interface ethernet 1/2.100,  LIF ifindex: 0x2c000041, Outer VLAN ID:100, Inner VLAN
ID:None
      logical-interface ethernet 1/2.101,  LIF ifindex: 0x2c000062, Outer VLAN ID:101, Inner VLAN
ID:None
      logical-interface ethernet 1/2.102,  LIF ifindex: 0x2c000044, Outer VLAN ID:102, Inner VLAN ID:200
```

History

Release version	Command history
18x.1.00	This command was introduced.

show logical-interface ethernet

Displays detailed or brief information regarding all logical interfaces (LIFs) associated with an Ethernet interface.

Syntax

show logical-interface ethernet [*slot/port. service_instance*] [**brief**]}

Parameters

slot/port
Specifies an Ethernet interface.

service_instance
Specifies a service instance ID.

brief
Displays brief information

Modes

Privileged EXEC mode

Command Output

The **show logical-interface ethernet** command displays the following information:

Output field	Description
Main PHY interface ifindex	Interface index
flag	Indicates status of operational state, tagging, and mode
Topo CB instance ID	
Protocol state	
IVID	Internal VLAN ID
Encap ID	
AC LIF	
VFI LIF	
LIF ifindex	Interface index of the LIF
LIF Name	Name of the LIF
FLAG	Indicates status of tagging, administrative state, and protocol layer
Outer VLAN ID	ID of the outer VLAN
Inner VLAN ID	ID of the inner VLAN
Ingress Stats Index	
Egress Stats Index	

Examples

The following example displays detailed information for all interfaces.

```
device# show logical-interface ethernet
Main PHY Interface ifindex:0x18410002 (Ethernet 1/2)
   flag:0x5
           bit 0 = 1 - Main Interace is Operational
           bit 1 = 0 - Main Interace does not have Untagged LIF
           bit 2 = 1 - Main Interace is Trunk Mode
   no service cnt:0, L2 service cnt:2, OPF service cnt:0

   LIFs on L2 service tree:
    Topo CB Instance ID: 255, Protocol State: 1, Num LIFs: 2
      LIF ifindex: 0x2c000040, Service Instance:0x80000001
      LIF Name:
      IVID:1 (0x1), Encap ID: 0xffffffff
      FLAG:0x6
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
      Outer VLAN ID:1 (0x1), Inner VLAN ID:65535 (0xffff)
      Ingress Stats Index: Inv, Egress Stats Index: Inv

      LIF ifindex: 0x2c000041, Service Instance:0x00000064
      LIF Name: AC_LIF_100
      IVID:4097 (0x1001), Encap ID: 0x2020
      FLAG:0x6
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
      Outer VLAN ID:100 (0x64), Inner VLAN ID:65535 (0xffff)
      Ingress Stats Index: Inv, Egress Stats Index: Inv


Main PHY Interface ifindex:0x18458007 (Ethernet 1/11)
   flag:0x5
           bit 0 = 1 - Main Interace is Operational
           bit 1 = 0 - Main Interace does not have Untagged LIF
           bit 2 = 1 - Main Interace is Trunk Mode
   no service cnt:0, L2 service cnt:1, OPF service cnt:0

   LIFs on L2 service tree:
    Topo CB Instance ID: 255, Protocol State: 1, Num LIFs: 1
      LIF ifindex: 0x2c000080, Service Instance:0x80000001
      LIF Name:
      IVID:1 (0x1), Encap ID: 0x2040
      FLAG:0x26
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
           bit  5 = 1 - LIF Open Flow Config
      Outer VLAN ID:1 (0x1), Inner VLAN ID:65535 (0xffff)
      Ingress Stats Index: Inv, Egress Stats Index: Inv
```

The following example displays brief information for all interfaces.

```
device# show logical-interface ethernet brief
Main PHY Interface ifindex:0x18410002 (Ethernet 1/2)
   no service cnt:0, L2 service cnt:2, OPF service cnt:0
   LIFs on L2 service tree:
      LIF ifindex: 0x2c000040, Service Instance:0x80000001, Outer VLAN ID:1 (0x1),       Inner VLAN ID:
65535
      LIF ifindex: 0x2c000041, Service Instance:0x00000064, Outer VLAN ID:100 (0x64), Inner VLAN ID:
65535

Main PHY Interface ifindex:0x18458007 (Ethernet 1/11)
   no service cnt:0, L2 service cnt:1, OPF service cnt:0
   LIFs on L2 service tree:
      LIF ifindex: 0x2c000080, Service Instance:0x80000001, Outer VLAN ID:1 (0x1), Inner VLAN ID:65535
```

The following example displays detailed information for a specific interface.

```
device# show logical-interface ethernet 1/2
Main PHY Interface ifindex:0x18410002 (Ethernet 1/2)
   flag:0x5
           bit 0 = 1 - Main Interace is Operational
           bit 1 = 0 - Main Interace does not have Untagged LIF
           bit 2 = 1 - Main Interace is Trunk Mode
   no service cnt:0, L2 service cnt:2, OPF service cnt:0

   LIFs on L2 service tree:
    Topo CB Instance ID: 255, Protocol State: 1, Num LIFs: 2
      LIF ifindex: 0x2c000040, Service Instance:0x80000001
      LIF Name:
      IVID:1 (0x1), Encap ID: 0xffffffff
      FLAG:0x6
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
      Outer VLAN ID:1 (0x1), Inner VLAN ID:65535 (0xffff)
      Ingress Stats Index: Inv, Egress Stats Index: Inv

      LIF ifindex: 0x2c000041, Service Instance:0x00000064
      LIF Name: AC_LIF_100
      IVID:4097 (0x1001), Encap ID: 0x2020
      FLAG:0x6
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
      Outer VLAN ID:100 (0x64), Inner VLAN ID:65535 (0xffff)
      Ingress Stats Index: Inv, Egress Stats Index: Inv
```

The following example displays brief information for a specific interface.

```
device# show logical-interface ethernet 1/2 brief
Main PHY Interface ifindex:0x18410002 (Ethernet 1/2)
   no service cnt:0, L2 service cnt:2, OPF service cnt:0
   LIFs on L2 service tree:
      LIF ifindex: 0x2c000040, Service Instance:0x80000001, Outer VLAN ID:1 (0x1),       Inner VLAN ID:
65535
      LIF ifindex: 0x2c000041, Service Instance:0x00000064, Outer VLAN ID:100 (0x64), Inner VLAN ID:
65535
```

The following example displays detailed information for a logical interface.

```
device# show logical-interface ethernet 1/2.100

      LIF ifindex: 0x2c000041, Service Instance:0x00000064
      LIF Name: AC_LIF_100
      IVID:4097 (0x1001), Encap ID: 0x2020
      FLAG:0x6
           bit  0 = 0 - LIF is TAGGED
           bit  1 = 1 - Admin State is UP
           bit  2 = 1 - LIF is L2
      Outer VLAN ID:100 (0x64), Inner VLAN ID:65535 (0xffff)
      Ingress Stats Index: Inv, Egress Stats Index: Inv
```

History

Release version	Command history
18x.1.00	This command was introduced.

show logical-interface port-channel

Displays detailed or brief information regarding all logical interfaces (LIFs) associated with a port-channel (LAG) interface.

Syntax

show logical-interface port-channel [*number*. *service_instance*] [**brief**]}

Parameters

number
Specifies a port-channel interface.

service_instance
Specifies a service instance ID.

brief
Displays brief information

Modes

Privileged EXEC mode

Command Output

The **show logical-interface port-channel** command displays the following information:

Output field	Description
Main PHY interface ifindex	Interface index
flag	Indicates status of operational state, tagging, and mode
Topo CB instance ID	
Protocol state	
IVID	Internal VLAN ID
Encap ID	
AC LIF	
VFI LIF	
LIF ifindex	Interface index of the LIF
LIF Name	Name of the LIF
FLAG	Indicates status of tagging, administrative state, and protocol layer
Outer VLAN ID	ID of the outer VLAN
Inner VLAN ID	ID of the inner VLAN
Ingress Stats Index	
Egress Stats Index	

Examples

The following example displays detailed information.

```
device# show logical-interface port-channel
```

The following example displays brief information.

```
device# show logical-interface port-channel brief
```

The following example displays detailed information for a specific interface.

```
device# show logical-interface port-chbannel 10
```

The following example displays brief information for a specific interface.

```
device# show logical-interface port-channel 10 brief
```

The following example displays detailed information for a logical interface.

```
device# show logical-interface port-channel 10.100
```

History

Release version	Command history
18x.1.00	This command was introduced.

show logical-interface pseudo-wire

Displays detailed or brief information regarding all logical interfaces (LIFs) associated with a pseudo-wire (PW) interface.

Syntax

show logical-interface pseudo-wire [*number*. *service_instance*] [**brief**]}

Parameters

number
Specifies a PW interface.

service_instance
Specifies a service instance ID.

brief
Displays brief information

Modes

Privileged EXEC mode

Command Output

The **show logical-interface pseudo-wire** command displays the following information:

Output field	Description
Main PHY interface ifindex	Interface index
flag	Indicates status of operational state, tagging, and mode
Topo CB instance ID	
Protocol state	
IVID	Internal VLAN ID
Encap ID	
AC LIF	
VFI LIF	
LIF ifindex	Interface index of the LIF
LIF Name	Name of the LIF
FLAG	Indicates status of tagging, administrative state, and protocol layer
Outer VLAN ID	ID of the outer VLAN
Inner VLAN ID	ID of the inner VLAN
Ingress Stats Index	
Egress Stats Index	

Examples

The following example displays detailed information.

```
device# show logical-interface pseudo-wire
```

The following example displays brief information.

```
device# show logical-interface pseudo-wire brief
```

The following example displays detailed information for a specific interface.

```
device# show logical-interface pseudo-wire 10
```

The following example displays brief information for a specific interface.

```
device# show logical-interface pseudo-wire 10 brief
```

The following example displays detailed information for a logical interface.

```
device# show logical-interface pseudo-wire 10.100
```

History

Release version	Command history
18x.1.00	This command was introduced.

show loop-detection

Displays loop detection (LD) information at the system, interface (Ethernet or port-channel), or VLAN VXLAN tunnel level.

Syntax

show loop-detection [**disabled-ports** | **globals** | **interface** { **ethernet** *interface* | **port-channel** *interface* } | **vlan** *VLAN_ID BD-ID*]

Parameters

disabled-ports
Displays the ports that are disabled by LD.

globals
Displays global LD configuration values.

interface
Specifies an Ethernet or port-channel interface.

ethernet*interface*
Specifies an Ethernet interface.

port-channel*interface*
Specifies a port-channel interface.

vlan*VLAN_ID*
Specifies a VLAN.

Modes

Privileged EXEC mode

Examples

The following example displays LD information at the system level.

```
device# show loop-detection
Strict Mode:
------------------------

Number of loop-detection instances enabled: 1

Interface: eth 2/6
        Enabled on VLANs: 100
        Shutdown Disable:   No
        Interface status: UP
        Auto enable in: Never

Packet Statistics:
vlan            sent            rcvd        disable-count
100             100             0           0

Loose Mode:
------------------------

Number of LD instances:   2
Disabled Ports:                   2/7

Packet Statistics:
vlan            sent            rcvd        disable-count
100             100             0           0
```

The following example displays ports disabled by LD.

```
device# show loop-detection disabled-ports
Ports disabled by loop detection
-----------------------------------------
port       age(min)       disable cause
2/6        5              Disabled by Self
```

The following example displays global LD configuration values.

```
device# show loop-detection globals
Loop Detection:                 Disabled
Shutdown-time (minutes):        0
Hello-time (msec):              1000
Raslog-duration (minutes):      10
```

The following example displays LD configuration values for an Ethernet interface.

```
device# show loop-detection interface ethernet 2/6
Number of LD instances:  1
Enabled on VLANs:        100
Shutdown Disable:        No
Interface status:        UP
Auto enable in:          Never

Packet Statistics:
vlan            sent            rcvd        disable-count
100             100             0           0
```

The following example displays LD configuration values, including logical interfaces (LIFs), for a VLAN VXLAN tunnel.

```
device# show loop-detection vlan 20
Number of LD instances: 1
LIF (Logical Interface) Disabled on Ports: eth2/2,VxLAN Tunnel 61441

Packet Statistics:
vlan            sent            rcvd
20              44225           2
```

The following example displays LD configuration values for a VLAN VXLAN tunnel if LD shutdown is disabled.

```
device# show loop-detection vlan 20
Number of LD instances: 1
LIF (Logical Interface) ShutDown is disabled for VLAN 20

Packet Statistics:
vlan            sent            rcvd
20              10              10
```

History

Release version	Command history
18x.1.00	This command was introduced.

show mac-address-table

Displays MAC address table information.

Syntax

show mac-address-table

show mac-address-table bridge-domain [*id*]

show mac-address-table cluster *cluster-ID* [{ **bridge-domain** [*bd-ID*] } | [**client** *client-ID*] | **local** | **remote** | [**vlan** *vlan-ID*]]

show mac-address-table count [**bridge-domain** *id*]

show mac-address-table [**address** *mac-address*] [**aging-time**] | [**dynamic** [**address** *mac-address*] | [**interface ethernet** *slot/port* | **port-channel** *interface number*] | **vlan** *vlan id*]] | [**interface** {**ethernet** *slot/port* | **port-channel** *number*} | **tunnel** *tunnel id*] | [**mdb** [*mac-address*] | **client** *<client-name>* | **vlan** *<vlan-id>*]] | [**static** [**address** *mac-address*] | [**interface** { **ethernet** *slot/port* | **port-channel** *number* }] | [**vlan***vlan id*] | [**vlan***vlan id*]

Parameters

bridge-domain *id*
: Specifies the displaying of MAC addresses learned under a bridge domain. When a bridge domain identifier is not specified, information is displayed about MAC addresses learned under all bridge domains.

cluster *cluster-ID*
: Displays the MAC addresses learned under the specified MCT cluster ID.

  bridge-domain *id*
  : Displays the MAC addresses learned for the bridge domain of the MCT cluster. When a bridge domain identifier is not specified, information is displayed about MAC addresses learned under all bridge domains.

  client *client-ID*
  : Displays the MAC addresses learned for the client ID of the MCT cluster.

  local
  : Displays the local MAC addresses for the cluster or the specified client ID.

  remote
  : Displays the remote MAC addresses for the cluster or the specified client ID.

  vlan *vlan-ID*
  : Displays the MAC addresses for the client VLAN ID of the MCT cluster.

address *MAC-address*
: Displays forwarding information for a 48-bit MAC address. The valid format is *H.H.H* (available in Privileged EXEC mode only).

aging-time
: Displays aging-time.

dynamic address *MAC-address*
: Specifies the dynamic MAC addresses for an ethernet interface, port-channel, or VLAN. The valid format is *H.H.H* (available in Privileged EXEC mode only).

interface ethernet *slot/port*
Specifies the ethernet interface with a valid slot number/port number.

port-channel *number*
Specifies the port channel interface number. The range is from 1 - 512 based on the platform.

vlan *vlan id*
Specifies the VLAN interface. The VLAN ID range is from 1 - 4090.

tunnel *tunnel id*
Specifies the tunnel interface. The tunnel ID range is from 1 - 100000.

mdb *MAC-address*
Specifies the MDB information for the cluster client specific macs. The valid format is *H.H.H* (available in Privileged EXEC mode only).

client *client-name*
Displays the client instance. Specify the client name with a maximum of 64 characters.

static address *mac-address*
Specifies the static MAC address for an ethernet interface , port-channel, or VLAN. The valid format is *H.H.H* (available in Privileged EXEC mode only).

Modes

Privileged EXEC mode.

Usage Guidelines

The MAC Type for an MCT cluster displays the following information:

- For the client MAC behavior, MAC addresses are learned as CCL on the local MCT node and CCR on the remote MCT node pointing to the CCEP interface.
- Static MAC addresses configured on CEP AC end points are learned as Static. The corresponding remote MAC addresses are learned as EVPN-Sticky in the remote node.
- For static MAC addresses over client interfaces, Static-CCL and CCR are displayed.

Examples

The following example shows how to display MAC table information for all bridge domains.

```
device# show mac-address-table bridge-domain

VlanId/BD-Id   Mac-address           Type     State     Ports/LIF/peer-ip
629(B)            0011.2222.5555     Dynamic  Active    eth 1/3.100
629(B)            0011.2222.6666     Dynamic  Inactive  eth 1/1.500
629(B)            0011.2222.1122     Dynamic  Active    10.12.12.12
629(B)            0011.2222.3333     static   Inactive  po 5.700
629(B)            0011.0101.5555     Dynamic  Active    eth 1/2.400

Total MAC addresses : 5
```

The following example shows the number of forwarding entries in the MAC address table for bridge domain 1.

```
device# show mac-address-table count bridge-domain 1

Total MAC addresses : 5
```

The following example shows how to display the MAC address table aging time.

```
device# show mac-address-table aging-time
     MAC Aging-time : 300 seconds
```

The following example shows how to display the MAC address table for an MCT cluster.

```
device# show mac-address-table cluster 1
Vlan/BD'Id Mac-address     Type        State    Ports
100(V)     0010.a111.aaaa  CCL         Active   ETH3/1
100(V)     0010.a111.aa22  Static-CCL  Active   ETH3/1
100(V)     0010.a111.bbbb  CCR         Active   ETH3/1
200(V)     003d.a111.1111  Dynamic     Active   Eth 1/1
200(V)     003d.a111.1122  Static      Active   Eth 1/1
200(V)     003d.a111.3333  EVPN        Active   10.2.2.2
200(V)     003d.a111.3322  EVPN-Static Active   10.2.2.2
```

History

Release version	Command history
18x.1.00	This command was introduced.

show mac-address-table endpoint-tracking

Displays authenticated or nonauthenticated MAC addresses that are learned on ports enabled for endpoint tracking.

Syntax

show mac-address-table endpoint-tracking { **authenticated** | **authentication-failed** } [**interface** *interface*]

Parameters

authenticated
Displays authenticated MAC addresses that are learned.

authentication-failed
Displays nonauthenticated MAC addresses that are learned.

interface*interface*
Specifies an Ethernet interface that is configured as a switchport.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

This example displays all ports where MAC authentication succeeds.

```
device# show mac-address-table endpoint-tracking authenticated
VlanId/BDId  Mac-address     Type      State(R-Radius,F-FailOpen)           Ports
100 (V)      0001.0100.0001  Dynamic   Authenticated(R)                     Eth 0/5
```

This example displays all ports where MAC authentication fails.

```
device# show mac-address-table endpoint-tracking authentication-failed
VlanId/BDId   Mac-address       Type             State      Ports
100 (V)       0001.0100.0001    Dynamic          Pending    Eth 0/5
100 (V)       0001.0100.0002    Dynamic          Failed     Eth 0/5
```

This example displays a specified port where MAC authentication succeeds.

```
device# show mac-address-table endpoint-tracking authenticated interface ethernet 0/5
VlanId/BDId  Mac-address     Type      State(R-Radius,F-FailOpen)           Ports
100 (V)      0001.0100.0001  Dynamic   Authenticated(R)                     Eth 0/5
```

This example displays a specified port where MAC authentication fails.

```
device# show mac-address-table endpoint-tracking authentication-failed interface ethernet 0/5
VlanId/BDId   Mac-address       Type             State      Ports
100 (V)       0001.0100.0001    Dynamic          Pending    Eth 0/5
100 (V)       0001.0100.0002    Dynamic          Failed     Eth 0/5
```

History

Release version	Command history
18x.1.00	This command was introduced.

show media

Displays the SFP information for all the interfaces present on a device.

Syntax

show media

Modes

Privileged EXEC mode

Usage Guidelines

The command output will be several pages long.

Examples

To display all SFP information, use the following command:

```
device# show media
  Ethernet 0/1
  Identifier     3    SFP
  Connector      7    LC
  Transceiver    0000000000000010 10_GB/s
  Name           id
  Encoding       6
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0   (units km)
  Length 9u      0   (units 100 meters)
  Length 50u     8   (units 10 meters)
  Length 62.5u   3   (units 10 meters)
  Length Cu      0   (units 1 meter)
  Vendor Name    EXTREME
  Vendor OUI     42:52:4f
  Vendor PN      57-0000075-01
  Vendor Rev     A
  Wavelength     850 (units nm)
  Options        001a Loss_of_Sig,Tx_Fault,Tx_Disable
  BR Max         0
  BR Min         0
  Serial No      AAA108454100431
  Date Code      081108
  Optical Monitor yes
  Temperature    44 Centigrade
  Voltage        3246.8  (Volts)
  Current        0.002  (mAmps)
  TX Power       0.1  (uWatts)
  RX Power       0.1  (uWatts)
(Output truncated)
```

History

Release version	Command history
18x.1.00	This command was introduced.

show media interface

Displays the SFP information for a specific interface.

Syntax

show media interface [<*N*>**ethernet** *slot* / *port*

Parameters

<*N*>**ethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>es a 1-Gb Ethernet port.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display SPF information, use the following command:

```
switch# show media interface ethernet 5/1

  Interface       Ethernet 5/1
  Identifier      2    On-board
  Connector       34   CAT-5 copper cable
  Transceiver     1000 BASE-T Gigabit Ethernet
  Name            cu
  Encoding        5    IEEE 802.3ab
  Length          max 100 m
  Copper Speed    1GB/s Fixed
  Copper Duplex   Full Duplex
  Sync status     Valid/No
  Vendor Name     Broadcom
  Vendor OUI      00:1B:E9
  Vendor model    02:0F
  Vendor Rev      01
  Options         001a Remote fault/Jabber detect/copper link up
  Temperature threshold/val    55 Centigrade
  Voltage threshold/val        3289.9  (mVolts)
```

History

Release version	Command history
17r.2.00	This command was introduced.

show media tunable-optic-sfpp

Displays the channels on which the tunable optic interfaces are currently operating.

Syntax

show media tunable-optic-sfpp [**channel** *channel_number*]

Parameters

channel *channel_number*

The channel number to display. The range of valid values is from 0 through 102.

Modes

Privileged EXEC mode

Command Output

The **show media tunable-optic-sfpp** command displays the following information:

Output field	Description
Channel	The number assigned to the channel.
Wavelength	The wavelength on which the optic interface is operating.

Examples

Sample output for a single channel.

```
device# show media tunable-optic-sfpp channel 2
command is show-media-tunable-optic-sfpp-channel-2.
  Channel   Wavelength
  ========= ==============
  2         1568.36
```

Sample output for all channels.

```
device# show media tunable-optic-sfpp
command is show-media-tunable-optic-sfpp.
  Channel   Wavelength
  ========= ==============
  1         1568.77
  2         1568.36
  3         1567.95
  4         1567.54
  5         1567.13
  6         1566.72
  7         1566.31
  8         1565.90
  9         1565.50
  10        1565.09
  11        1564.68
  12        1564.27
  13        1563.86
  14        1563.45
  15        1563.05
  16        1562.64
  17        1562.23
  18        1561.83
  19        1561.42
  20        1561.01
(Output truncated for brevity.)
```

History

Release version	Command history
18x.1.00	This command was introduced.

show monitor

Displays the monitoring information for all Port Mirroring sessions or for a single session.

Syntax

show monitor [**session** *session_number*]

Parameters

session *session_number*

Specifies a session identification number. Valid values range from 0 through 511.

Modes

Privileged EXEC mode

Command Output

The **show monitor** command displays the following information:

Output field	Description
Session	The identifying value applied to the session
Type	The type of session.
Description	The session description.
State	The current state of the session.
Source interface	The interface that the session is using to access the device.
Destination interface	The destination for the session.
Direction	Displays whether the interface is receiving, transmitting, or both.

Examples

To display monitoring information for all Port Mirroring sessions:

```
device# show monitor

Session                         :1
Type                            :Remote source session
Description                     :Test monitor session
State                           :Enabled
Source interface                :eth 0/1 (Up)
Destination interface           :Vlan x
Direction                       :Rx
```

History

Release version	Command history
18x.1.00	This command was introduced.

show netconf

Displays NETCONF session.

Syntax

show netconf

Modes

Privileged EXEC mode

Usage Guidelines

The text output is extensive. Extreme Networks recommends redirecting the output to a text file.

Examples

Typical NETCONF session output.

```
device# show netconf
netconf-state capabilities capability urn:ietf:params:netconf:base:1.0
netconf-state capabilities capability urn:ietf:params:netconf:base:1.1
netconf-state capabilities capability urn:ietf:params:netconf:capability:writable-running:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:startup:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:xpath:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.1
netconf-state capabilities capability http://tail-f.com/ns/netconf/actions/1.0
<output truncated>
```

History

Release version	Command history
18x.1.00	This command was introduced.

show netconf capabilities

Displays the capabilities associated with each NETCONF session.

Syntax

show netconf capabilities

Modes

Privileged EXEC mode

Usage Guidelines

Examples

Typical command example of output.

```
device# show netconf capabilities
netconf-state capabilities capability urn:ietf:params:netconf:base:1.0
netconf-state capabilities capability urn:ietf:params:netconf:base:1.1
netconf-state capabilities capability urn:ietf:params:netconf:capability:writable-running:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:startup:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:xpath:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.1
netconf-state capabilities capability http://tail-f.com/ns/netconf/actions/1.0
<output truncated>
```

History

Release version	Command history
18x.1.00	This command was introduced.

show notification stream

Displays notifications about the event stream.

Syntax

show notification stream ?

Modes

Privileged EXEC mode

Examples

Typical output example for this command.

```
device# show notification stream ?
Possible completions:
  no event streams present
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ntp status

Displays the Network Time Protocol (NTP) status.

Syntax

show ntp status

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

Use this command to display the active NTP server. If an NTP server is not configured, the command output displays the server as "LOCL". Otherwise, the command displays the NTP server IP address.

Examples

To show the local device NTP status when an NTP server is not configured:

```
device# show ntp status

active ntp server is LOCL
```

To show the configured NTP server:

```
device# show ntp status

active ntp server is 10.21.2.80
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ntp status association detail

This command lists detailed NTP server and peer association information. You can view detailed information of one NTP server and peer.

Syntax

show ntp status association detail { **ipv4 address** | **ipv6 address** }

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

Use this command to view detailed information of one NTP server and peer.

Examples

To show the NTP status association details.

```
device# show ntp status association detail

131.216.1.101 configured server, sys peer, stratum 2
 ref ID 204.123.2.5, time d21da706.1ed27000 (16:14:22.517107712 GMT+05:30 Fri Jan 20 2017)
 our mode client, peer mode server, our poll intvl 6, peer poll intvl 6,
 root delay 0.02256774 msec, root disp 0.01150512, reach 377, root dist 0.36969603
 delay 290.94232711 msec, offset -1.08355772 msec, dispersion 4.58729275,
 precision 2**-16, version 4
 org time d21da713.f8f25000 (16:14:35.4176629760 GMT+05:30 Fri Jan 6 2017)
 rcv time d21da714.2602742a (16:14:36.637695018 GMT+05:30 Fri Jan 6 2017)
 xmt time d21da713.d31f723f (16:14:35.3542053439 GMT+05:30 Fri Jan 6 2017)
 filter delay    296.5594  322.7792  323.5571  297.6697  290.9942  303.5554  305.9971  295.0019
 filter offset     0.4430  -13.4441  -14.2241   -4.0003   -1.0083   -1.4414   -3.0034    1.9941
 filter disp       1.9984    1.0025    0.0035    6.8889    5.8899    4.8895    3.9920    2.9944
 filter epoch        5779      5843      5909      5452      5518      5585      5650      5715
```

The output fields are:	
server	Indicates server is statically configured.
symmetric active peer	Indicates peer is statically configured.
symmetric passive peer	Indicates peer is dynamically configured.
sys_peer	This peer is the system peer.
candidate	survivor in the selection algorithm. This peer is chosen as candidate in the combine algorithm.
reject	This peer is rejected by the selection algorithm.
falsetick	This peer is dropped as falseticker by the selection algorithm.
outlyer	This peer is dropped as outlyer by the clustering algorithm.
Stratum	Stratum number
ref ID	IPv4 address or hash of IPv6 address of the upstream time server to which the peer is synchronized.
Time	Last time stamp that the peer received from its master.
our mode	This system's mode relative to peer (active /passive /client /server / bdcast /bdcast client).
peer mode	Mode of peer relative to this system.
our poll intvl	This system's poll interval to this peer.
peer poll intvl	Poll interval of peer to this system.
root delay	The delay along path to root (the final stratum 1 time source).
root disp	Dispersion of path to root.
reach peer	The peer reachability (bit string in octal).
Delay	Round-trip delay to peer.
offset	Offset of peer clock relative to this clock.
Dispersion	Dispersion of peer clock.
precision	Precision of peer clock.
version	Peer NTP version number.
org time	Originate time stamp of the last packet.
rcv time	Receive time stamp of the last packet.
xmt time	Transmit time stamp of the last packet.
filter delay	Round-trip delay in milliseconds of last 8 samples.

The output fields are:	
filter offset	Clock offset in milliseconds of last 8 samples.
filter error	Approximate error of last 8 samples.

History

Release version	Command history
18x.1.00	This command was introduced.

show ntp status associations

This command lists the NTP servers and peers association.

Syntax

show ntp associations

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

Use this command to display NTP server status associations.

Examples

To show the NTP server status associations.

```
device# show ntp status associations
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
2620:100:0:f404  .PPS.            1 u   20   64   17    0.460   -4.844   0.897
+216.45.57.38    20.162.227.208   2 u  502 1024  377  241.941   12.103  10.920
-172.19.69.1     172.82.134.51    3 u  741 1024  377  223.985   -7.426   2.571
*216.45.57.38    128.252.19.1     2 u  884 1024  377  230.046    1.422   5.871
+10.0.017        208.75.89.4      3 u  858 1024  377  211.094   -1.801   6.431

* synced, # selected, + candidate, - outlayer, x falseticker
```

The character in the left margin indicates the fate of this server/peer in the clock selection process.

The output fields are:	
<space>	Discarded as not valid (TEST10-TEST13).
x	Discarded as falseticker in the selection algorithm.
-	Discarded as outlier in the clustering algorithm.
+	Candidate in the combine algorithm.
#	Survivor in the selection algorithm.
remote	IPv4 or IPv6 address of the peer.
refid	Reference clock type or address for the peer or kisscode.
st	Stratum setting for the peer.
when	Sec/min/hr since last received packet
poll	Poll interval (log2 s)
reach	Reach shift register (octal)
delay	Round-trip delay to peer, in milliseconds.
offset	Relative time difference between a peer clock and a local clock, in milliseconds.
jitter	Jitter

History

Release version	Command history
18x.1.00	This command was introduced.

show overlay-gateway

Displays status and statistics for the VXLAN overlay-gateway instance.

Syntax

show overlay-gateway [**name** *name* [**vlan statistics** | **statistics**]

Parameters

name

Name of the configured VXLAN gateway.

vlan statistics

Displays statistics for each VLAN for the VXLAN gateway. Statistics include transmitted and received packet counts and byte counts exchanged for each exported VLAN. Because each exported VLAN maps to a VXLAN, these statistics apply on a per-VXLAN-counters basis. Per-VLAN counters are not enabled by default. You need to first run the **enable statistics direction** command for the gateway to enable statistics for specified VLAN IDs.

statistics

Displays statistics for the VXLAN gateway. Statistics include transmitted and received packet counts and byte counts. These counters are derived by aggregating tunnel counters for all the tunnels of the gateway.

Modes

Privileged EXEC mode

Usage Guidelines

Output includes the gateway name, the system-assigned gateway ID, source IP address, VRF, administration state, and number of tunnels associated.

If you specify the gateway name, the gateway must already be configured.

Examples

To show the status for a gateway instance that is configured for Layer 2 extension with a loopback interface:

```
device# show overlay-gateway

Overlay Gateway "GW1", ID 1
Type layer2-extension, Admin state up
IP address 10.10.10.1 (Loopback 10), Vrf default-vrf
Number of tunnels 2
Packet count: RX 0               TX 0
Byte count  : RX (NA)            TX 0
```

To show statistics for the gateway instance:

```
device# show overlay-gateway statistics

Gateway Name         RX packets      TX packets      RX bytes        TX bytes
==================== =============== =============== ========= ==============
GW1                  200000          10000           22227772        1110111
```

To display statistics for VLANs attached to the VXLAN gateway:

```
device# show overlay-gateway name GW1 vlan statistics

                              Packets          Bytes
VLAN    VNI     Tx      Rx        Tx         Rx
-----------------------------------------------------
10      1010   10000   200000    1110111    22227772
11      1011   2200    -         221334     -
21      1021   -       1         -          100


device# show overlay-gateway name test vlan statistics
VLAN ID   RX packets           TX packets
========= ==================== ====================
30        0                    0
40        3696                 3696
```

History

Release version	Command history
18x.1.00	This command was introduced.

show policy-map

Displays configured policy maps and class-map policer parameters applied to the interfaces or globally.

Syntax

show policy-map [**details** *policyname* | [{**interface ethernet** *slot/port* } | **system**] [**input** | **output**]]

Parameters

details *policyname*
Displays the detail configuration of the policy map along with binding information.

interface ethernet *slot/port*
Specifies a a valid slot and port number for an Ethernet interface.

system
Displays the information for the globally-applied policy map.

input
Inbound - direction where the policy map is applied.

output
Outbound - direction where the policy map is applied.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command without identifying an interface and direction of traffic to display policy map binding for all interfaces on the device.

Command Output

The **show policy-map** command displays the following information:

Output field	Description
Interface	The interface for which rate limiting information is being displayed.
Direction	The traffic direction for which rate limiting is applied.
police-priority-map	Remarked priority map used for Policer application (802.1 p priority remarked map).
Conform	The traffic in bytes that has been forwarded from this interface that is within the CIR bandwidth limits.
Exceeded	The traffic that has been exceeded the bandwidth available in the CIR limits and has not exceed the EIR limits for this rate-limit policy.
Violated	The traffic that has exceeded the bandwidth available in the CIR and EIR limits.

Examples

The following example displays the interface-specific policy-map information.

```
device# show policy-map interface ethernet 1/1 in

Ingress Direction :
Policy-Map p2
Class c2
matches 7867567 packets 1007048576 bytes
Police cir 1000000
       Stats:
         Operational cir:1010000 cbs:149999 eir:0 ebs:0
         Conform Byte:1180928 Exceed Byte:0 Violate Byte:1005867648
```

To display policy map binding information for all interfaces:

```
device# show policy-map
Number of policy maps : 46
Policy-Map P1-DEFAULT-RL
  Bound To:None
Policy-Map P2-DEFAULT-RL-10000000000
  Bound To: Eth 1/27(in)
Policy-Map P3-DEFAULT-RL-1500000000
  Bound To:None
```

The following example displays the system-specific policy-map information.

```
device# # show policy-map system map-name pm1

Ingress Direction :
Policy-Map pm1
Class cm1
matches 480661 packets 61524608 bytes
Police cir 100000
Stats:
 Operational cir:109000 cbs:14999 eir:0 ebs:0
  Conform Byte:265088 Exceed Byte:0 Violate Byte:0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show port port-channel ethernet

Displays the detailed LACP attributes that are configured and negotiated with its partner.

Syntax

show port port-channel ethernet *slot* **/** *port*

Parameters

slot

Specifies a valid slot. Must be `0`.

port

Specifies a valid port.

Modes

Privileged EXEC mode

Examples

The following example displays the LACP attributes for an Ethernet interface:

```
device# show port port-channel ethernet 0/6
 LACP link info: eth 0/6 - 0x118430006
 Actor System ID: 0x8000,01-e0-52-00-00-01
 Partner System ID: 0x0000,00-00-00-00-00-00
 Actor port priority: 0x8000 (32768)
 Admin key: 0x0003 (3) Oper key: 0x0003 (3)
 Receive machine state : Defaulted
 Periodic Transmission machine state : Fast periodic
 Mux machine state : Waiting
 Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
 Oper state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
 Partner oper state: ACT:0 TIM:1 AGG:1 SYN:1 COL:0 DIS:0 DEF:1 EXP:0
 Partner oper port: 0
 Selected: :2
 Defaulted State Action: No Default-Up
```

History

Release version	Command history
18x.1.00	This command was introduced.

show port-channel

Displays the Link Aggregation Group (LAG) information for a port-channel.

Syntax

show port-channel [*channel-group-number* | **detail** | **load-balance** | **summary**]

Parameters

channel-group-number
Specifies a port-channel number to display. Range is from 1 through 64.

detail
Displays detailed LAG information for a port-channel.

load-balance
Displays the load-balance or frame-distribution scheme among ports in the port-channel.

summary
Displays the summary information per channel-group.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a port-channel, all port-channels are displayed.

Examples

The following example displays the output of the basic **show port-channel** command.

NOTE

For the current release, ignore "* - Primary link in port-channel", if displayed.

```
device# show port-channel
 LACP Aggregator: Po 11
 Aggregator type: Standard
 Number of Ports: 1
 Member ports:
   Eth 0/49

 LACP Aggregator: Po 12
 Aggregator type: Standard
 Number of Ports: 1
 Member ports:
   Eth 0/50

 LACP Aggregator: Po 13
 Aggregator type: Standard
 Number of Ports: 2
 Member ports:
   Eth 0/51
   Eth 0/52

 Static Aggregator: Po 14
 Aggregator type: Standard
```

The following example displays detailed port-channel information.

```
device# show port-channel detail
 Static Aggregator: Po 14
 Aggregator type: Standard


 LACP Aggregator: Po 11
 Aggregator type: Standard
  Actor System ID - 0x8000,00-04-96-9f-5d-5c
  Admin Key: 0011 - Oper Key 0011
  Receive link count: 0 - Transmit link count: 0
  Individual: 0 - Ready: 0
  Partner System ID - 0x0000,00-00-00-00-00-00
  Partner Oper Key 0000
 Number of Ports: 1
 Member ports:
   Link: Eth 0/49 (0xC062100) sync: 0


 LACP Aggregator: Po 12
 Aggregator type: Standard
  Actor System ID - 0x8000,00-04-96-9f-5d-5c
  Admin Key: 0012 - Oper Key 0012
  Receive link count: 1 - Transmit link count: 1
  Individual: 0 - Ready: 1
  Partner System ID - 0x8000,00-04-96-9f-69-ca
  Partner Oper Key 0012
 Number of Ports: 1
 Member ports:
   Link: Eth 0/50 (0xC064100) sync: 1


 LACP Aggregator: Po 13
 Aggregator type: Standard
  Actor System ID - 0x8000,00-04-96-9f-5d-5c
  Admin Key: 0013 - Oper Key 0013
  Receive link count: 0 - Transmit link count: 0
  Individual: 0 - Ready: 0
  Partner System ID - 0x0000,00-00-00-00-00-00
  Partner Oper Key 0000
 Number of Ports: 2
 Member ports:
   Link: Eth 0/51 (0xC066100) sync: 0
   Link: Eth 0/52 (0xC068100) sync: 0
```

The following example displays port-channel load-balance information.

```
device# show port-channel load-balance Header parameters
Ethernet Mask: sa-mac da-mac etype vlan
ip: src-ip dst-ip protocol src-l4-port dst-l4-port
ipv6: ipv6-src-ip ipv6-dst-ip ipv6-next-hdr ipv6-src-l4-port ipv6-dst-l4-port

Hash Settings
hdr-start:FWD, hdr-count:3, bos-start:0, bos-skip:0, skip-cw:0
normalize:0, rotate:3, include_src_port:0, Disable: L2 0, ipv4 0, ipv6 0,
load-balance-type hash-based
```

The following example displays summary output.

```
device# show port-channel summary
Flags:  D - Down                P - Up in port-channel (members)
        U - Up (port-channel)
        S - Switched            I - Insight Enabled
        M - Not in use. Min-links not met
===== =============== ========== ===============
Group Port-channel    Protocol   Member ports
===== =============== ========== ===============
11    Po 11   (SD)    LACP       Eth 0/49 (D)
12    Po 12   (SU)    LACP       Eth 0/50 (P)
13    Po 13   (SD)    LACP       Eth 0/51 (D)
                                 Eth 0/52 (D)
14    Po 14   (SD)    None
```

History

Release version	Command history
18x.1.00	This command was introduced.

show port-security

Displays the configuration information related to port security.

Syntax

show port-security [**addresses** | **interface ethernet** *slot/port*]

Modes

Privileged EXEC mode

Interface configuration mode

Command Output

The **show port-security** command displays the following information:

Output field	Description
Secure Port	The port on which port MAC security is enabled.
MaxSecureAddress (count)	The maximum limit for the number of secure MAC addresses allowed on the interface.
StaticSec (count)	The number of MAC addresses that are manually configured.
Violated	The status that shows whether the port security violation has occurred.
Action	The configured response action that will be taken when a port security violation occurs.
Sticky	The status that shows whether sticky MAC learning is enabled.
Port Security	The status that shows whether port MAC security is enabled.
Port Status	The status of the port.
Violation Mode	The configured response action that will be taken when a port security violation occurs.
Violated	The status that shows whether the port security violation has occurred.
Sticky Enabled	The status that shows whether sticky MAC learning is enabled.
Maximum MAC addresses	The maximum limit for the number of secure MAC addresses allowed on the interface.
Total MAC addresses	The total number of secure MAC addresses learned on the interface.
Configured MAC addresses	The total number of secure MAC addresses configured on the interface manually.
Last violation time	The time when the last port security violation occurred.
Shutdown time (in Minutes)	The configured auto recovery time for port security violation.
Vlan	The VLAN to which the port is mapped.
Mac-address	The secured MAC address.
Type	The types of secure MAC addresses that are used in port MAC security.
Ports	The port on which port MAC security is enabled.

Examples

To display the port MAC security configuration details across ports on the device, enter the following command:

```
device(conf-if-eth-3/2)# do show port-security
Secure    MaxSecureAddr  CurrentAddr  StaticSec  Violated  Action   Sticky
Port         (count)       (count)     (count)
Eth 3/2       10           0            1           No     Shutdown  No
```

To display the statistics of the port MAC security configured for an interface, enter the following command:

```
device(conf-if-eth-3/2)# do show port-security interface ethernet 3/2
Port Security               : Enabled
Port Status                 : Up
Violation Mode              : Shutdown
Violated                    : No
Sticky Enabled              : No
Maximum MAC addresses       : 10
Total MAC addresses         : 0
Configured MAC addresses    : 1
Last violation time         :
Shutdown time (in Minutes)  : 0
```

To list the secure MAC addresses configured on the device, enter the following command.

```
device(conf-if-eth-3/2)# do show port-security addresses
                    Secure Mac Address Table
------------------------------------------------------------------
Vlan       Mac-address            Type                     Ports
250        3200.1110.0002         Secure-Static            Eth 3/2
```

History

Release version	Command history
18x.1.00	This command was introduced.

show process cpu

Displays information about the active processes in the switch and their corresponding CPU utilization statistics.

Syntax

show process cpu [**summary**] [**history**] [**top**] [**all-partitions**]

Parameters

summary
: Displays a summary view of cpu usage.

history
: Displays the history of CPU usage.

top
: Displays current CPU utilization.

all-partitions
: Displays a summary view of all partitions.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

For an explanation of process states, refer to the UNIX manual page for the **ps** command.

Examples

To show the information for all processes:

```
device# show process cpu summary
 Realtime Statistics:
Total CPU Utilization: 0% (user procs:0%, system-kernel:0%, iowait:0%)
Load Average: One minute: 0.00; Five minutes: 0.03; Fifteen minutes: 0.01
```

To show CPU usage information by individual processes:

```
device# show process cpu
 Realtime Statistics:
Total CPU Utilization: 0% (user procs:0%, system-kernel:0%, iowait:0%)
Load Average: One minute: 0.00; Five minutes: 0.02; Fifteen minutes: 0.00
Active Processes Lifetime Statistic:
  PID   Process          CPU%  State      Started
17169   sh                1.00    S       13:44:27 Jul  1, 2012
 2060   emd               0.80    S       21:52:27 Jun 29, 2012
 2462   SWITCH_TMR_0      0.60    S       21:53:08 Jun 29, 2012
17170   imishow_proc_cp   0.50    S       13:44:27 Jul  1, 2012
 2207   ospfd             0.20    S       21:52:41 Jun 29, 2012
 2211   mstpd             0.20    S       21:52:41 Jun 29, 2012
 2208   rtmd              0.10    S       21:52:41 Jun 29, 2012
(Output truncated)
```

To show the information for all partitions:

```
device# show process cpu all-partitions
Load Average:
L1/0:    2.81    2.27    2.15
L1/1:    2.00    2.00    2.00
L2/0:    2.00    2.01    2.00
L2/1:    2.06    2.03    2.00

Total CPU Utilization (in %):
L1/0:    4.39    0.14    3.83    0.41
L1/1:    0.5    0.00    0.08    0.42
L2/0:    0.49    0.01    0.05    0.44
L2/1:    0.5    0.01    0.05    0.44
```

History

Release version	Command history
18x.1.00	This command was introduced.

show process info

Displays system processes hierarchically.

Syntax

show process info]

Command Default

This command is executed on the local switch.

Modes

Privileged EXEC mode

Usage Guidelines

Pagination is not supported with this command. Use **more** in the terminal window to display the output one page at a time.

This command is supported only on the local switch.

Examples

To display system processes hierarchically:

```
device# show process info

PID     CMD
2       kthreadd
3       \_ migration/0
4       \_ ksoftirqd/0
5       \_ watchdog/0
6       \_ migration/1
7       \_ ksoftirqd/1
8       \_ watchdog/1
9       \_ migration/2
10      \_ ksoftirqd/2
11      \_ watchdog/2
12      \_ migration/3
13      \_ ksoftirqd/3
14      \_ watchdog/3
15      \_ migration/4
16      \_ ksoftirqd/4
17      \_ watchdog/4
18      \_ migration/5
19      \_ ksoftirqd/5
20      \_ watchdog/5
21      \_ migration/6
22      \_ ksoftirqd/6
[Output truncated]
```

History

Release version	Command history
18x.1.00	This command was introduced.

show process memory

Displays the memory usage information based on processes running in the system.

Syntax

show process memory [**summary**]

Parameters

summary

Displays a summary view of memory usage.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

Examples

To show memory usage information by individual processes:

```
device# show process memory
%Memory Used: 24.8368%; TotalMemory: 8080312 KB; Total Used: 2006888 KB
Total Free: 6073424 KB; Low Free: 271728 KB; High Free: 4906964 KB; Cached: 747948 KB
  PID   Process          MEM%        VSIZE(KB)       RSS(KB)       PSS(KB)
 6954   hslagtd          3.30         707412         268644         264050
 4405   Dcmd             2.20         385352         182672         152818
 4652   postgres         2.10         216252         173192         143609
 4752   Mcdsd            0.90         235628          75204          47126
 5725   ribmgr           0.80         299724          71828          44743
 6958   fibagt           0.80         246888          69828          42998
 5726   srm              0.80         209512          67516          40639
 5718   nsm              0.60         323520          56376          28656
 5723   ospfd            0.60         326592          54836          27710
 5747   ospf6d           0.60         326364          54488          27389
 5738   arpd             0.60         239348          54328          27438
 5734   mstpd            0.60         214624          51368          24154
 5722   bgpd             0.60         340812          50976          23826
 4647   postgres         0.60         157476          48840          24130
 3623   raslogd          0.50         160440          47968          22327
 5739   iphelpd          0.50         259464          47112          20244
 5729   pimd             0.50         315092          46972          19983
 3640   snmpd            0.50         237116          46656          15292
 5730   mc_hms           0.50         299128          46496          19167
 5727   rpsd             0.50         296804          45580          18620
 5735   vrrpd            0.50         254660          44384          17446
 5750   bfdd             0.50         319116          44348          17457
 2594   confd            0.50          54236          43568          42450
 5724   mctd             0.50         232356          43224          16240
 5732   qosd             0.50         201584          41272          14225
 5744   sflowd           0.50         218208          41192          14140
 5749   tnlmgrd          0.50         220264          40988          14230
 6956   mcagtd           0.50         275560          40444          13511
 5731   ssmd             0.40         203412          40392          13322
 3626   pemd             0.40         229504          39972           9939
 5736   dauthd           0.40         192548          39544          12202
 5742   ptpd             0.40         191572          38372          11763
 5751   ctpd             0.40         205632          38076          11403
 5728   radv             0.40         181964          38060          11246
 5740   onmd             0.40         200644          37940          10597
 5720   l2sysd           0.40         190976          37792          10911
 5737   igmpd            0.40         193056          37576          10373
 5733   lacpd            0.40         183620          37364          10106
 5743   rmond            0.40         183568          37308          10059
 5721   mcast_ssd        0.40         216288          36624           9737
 6955   l2agtd           0.40         210108          36384           9697
 5741   eldd             0.40         188508          36292           9441
 5746   udldd            0.40         188404          36040           9272
 5745   pcapd            0.40         188492          36032           9347
 6959   tnlagtd          0.40         191432          35036           8593
 3630   pdmd             0.40         172824          34352           8118
 6957   qosagtd          0.30          99716          29360           7477
 3642   tsd              0.30         106700          27628           5874
 4877   postgres         0.30         166956          27572          21316
[output omitted, as will vary by device]
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos cpu cfg

Displays information about the current CPU protection configuration for individual slots.

Syntax

show qos cpu cfg { **slot***slot_id* } [**burst** | **shaper** | **rate**]

Parameters

slot*slot_id*
Specifies a slot number. The ranges are 0 on pizzabox platforms, 1 through 4 on F4 platforms, and 1 through 8 on F8 platforms.

burst
Specifies port and group traffic burst rates for IPv6 subnet rate limiting.

shaper
Specifies port and group traffic shaper rates for IPv6 subnet rate limiting.

rate
Specifies shaping rate for IPv6 subnet rate limiting.

Modes

Privileged EXEC mode

Usage Guidelines

ipv6 subnet-rate-limit

Examples

To display information about the CPU configuration for slot 1.

```
device# show qos cpu cfg slot 1
Slot 1 CPU QoS Config

CPU Port shaper rate: 5000 Kbps
CPU Group shaper rates (Kbps)
Group  Aggr   P0     P1     P2     P3     P4     P5     P6     P7
-------------------------------------------------------------------
  0    5000   5000   5000   5000   5000   5000   5000   5000   5000
  1    5000   5000   5000   5000   5000   5000   5000   5000   5000
  2    5000   5000   5000   5000   5000   5000   5000   5000   5000
  3    5000   5000   5000   5000   5000   5000   5000   5000   5000
  4    5000   5000   5000   5000   5000   5000   5000   5000   5000
  5    5000   5000   5000   5000   5000   5000   5000   5000   5000
  6    5000   5000   5000   5000   5000   5000   5000   5000   5000
  7    5000   5000   5000   5000   5000   5000   5000   5000   5000
  8    5000   5000   5000   5000   5000   5000   5000   5000   5000
  9    5000   5000   5000   5000   5000   5000   5000   5000   5000
 10    5000   5000   5000   5000   5000   5000   5000   5000   5000
 11    5000   5000   5000   5000   5000   5000   5000   5000   5000

CPU Port burst size: 1 Kbytes
CPU Group burst size (Kbytes)
Group  Aggr  P0    P1    P2    P3    P4    P5    P6    P7
-----------------------------------------------------------
  0    1     1     1     1     1     1     1     1     1
  1    1     1     1     1     1     1     1     1     1
  2    1     1     1     1     1     1     1     1     1
  3    1     1     1     1     1     1     1     1     1
  4    1     1     1     1     1     1     1     1     1
  5    1     1     1     1     1     1     1     1     1
  6    1     1     1     1     1     1     1     1     1
  7    1     1     1     1     1     1     1     1     1
  8    1     1     1     1     1     1     1     1     1
  9    1     1     1     1     1     1     1     1     1
 10    1     1     1     1     1     1     1     1     1
 11    1     1     1     1     1     1     1     1     1

CPU Group WFQ values
Group  Aggr  P0    P1    P2    P3    P4    P5    P6    P7
-----------------------------------------------------------
  0    1     20    50    50    50    50    50    50    100
  1    1     20    50    50    50    50    50    50    100
  2    1     20    50    50    50    50    50    50    100
  3    1     20    50    50    50    50    50    50    100
  4    1     20    50    50    50    50    50    50    100
  5    1     20    50    50    50    50    50    50    100
  6    1     20    50    50    50    50    50    50    100
  7    1     20    50    50    50    50    50    50    100
  8    1     20    50    50    50    50    50    50    100
  9    1     20    50    50    50    50    50    50    100
 10    1     20    50    50    50    50    50    50    100
 11    1     20    50    50    50    50    50    50    100
```

To display information only about the IPv6 subnet rate-limiting traffic shaper configuration for slot 1.

```
device# show qos cpu cfg slot 1 shaper
Slot 1 CPU QoS Config

CPU Port shaper rate: 5000 Kbps
CPU Group shaper rates (Kbps)
Group  Aggr   P0     P1     P2     P3     P4     P5     P6     P7
-----------------------------------------------------------------
  0    5000   5000   5000   5000   5000   5000   5000   5000   5000
  1    5000   5000   5000   5000   5000   5000   5000   5000   5000
  2    5000   5000   5000   5000   5000   5000   5000   5000   5000
  3    5000   5000   5000   5000   5000   5000   5000   5000   5000
  4    5000   5000   5000   5000   5000   5000   5000   5000   5000
  5    5000   5000   5000   5000   5000   5000   5000   5000   5000
  6    5000   5000   5000   5000   5000   5000   5000   5000   5000
  7    5000   5000   5000   5000   5000   5000   5000   5000   5000
  8    5000   5000   5000   5000   5000   5000   5000   5000   5000
  9    5000   5000   5000   5000   5000   5000   5000   5000   5000
 10    5000   5000   5000   5000   5000   5000   5000   5000   5000
 11    5000   5000   5000   5000   5000   5000   5000   5000   5000
```

To display information only about the IPv6 subnet shaping rate configuration for slot 1.

```
device# show qos cpu cfg slot 1 rate
Slot 1 CPU QoS Config

Name                  Egid   Group        Pkts       Bytes          PPS         bps
-------------------------------------------------------------------------------
Protocol              7f80   0            0          0              0           0
Management            7f81   1
IP Host               7f82   2            11907      173855778      724         845632
MC RPF Fail           7f83   3            0          0              0           0
MC LHR                7f84   4            0          0              0           0
```

History

Release version	Command history
18x.1.00	This command was modified to support IPv6 subnet rate limiting.

show qos cpu info

Displays information on CPU groups and effective group IDs (EGID).

Syntax

show qos cpu info

Modes

Privileged EXEC mode.

Examples

To show CPU group information use the following command.

```
device# show qos cpu info

Name                  Egid  Group  Description
-----------------------------------------------
Protocol              7f80    0    Protocol Packets (ARP, L2, etc)
Management            7f81    1    Management (ping, local route)
IP Host               7f82    2    IP Host (subnet route)
MC RPF Fail           7f83    3    Multicast RPF failure
MC LHR                7f84    4    Multicast RP and LHR
MC FHR                7f85    5    Multicast FHR
SFlow Port            7f86    6    SFlow Packets (Port sflow)
SFlow ACL In          7f87    6    ACL sflow ingress permit
SFlow ACL In Deny     7f88    6    ACL sFlow ingress deny
SFlow ACL Eg          7f89    6    ACL sflow egress permit
SFlow ACL Eg Deny     7f8a    6    ACL sflow egress deny
VXLAN Snoop           7f8b    6    VXLAN Visibility Snoop
ACL Log               7f8c    7    ACL Logging
ACL Log In            7f8d    7    ACL Logging ingress permit
ACL Log In Deny       7f8e    7    ACL Logging ingress deny
ACL Log Eg            7f8f    7    ACL Logging egress permit
ACL Log Eg Deny       7f90    7    ACL Logging egress deny
Snoop                 7f91    8    Snoop (VxLAN)
Diagnostics           7f92    9    Diagnostics and debug
OAM                   7f93   10    OAM and CFM
Openflow              7f94   11    OpenFlow packets
Exceptions            7f96   12    Errors, Exceptions (TTL, MTU)
ICMP Redirect         7f95   12    ICMP Redirect
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos flowcontrol interface

Displays the configured flow control information for a specific interface, port channel, or all interfaces on the device.

Syntax

show qos flowcontrol interface { **all** | **ethernet** *slot/port* | **port-channel** *number* }

Parameters

all

Displays the flow control information on all interfaces.

ethernet *slot/port*

Displays the flow control information on the specified interface.

port-channel *number*

Displays the flow control information on the interface for the specified port channel.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the flow control mode, generation (Tx) and reception (Rx) status, and Tx and Rx PAUSE frame counts.

Examples

The following example displays the flow control information for all interfaces.

```
device# show qos flowcontrol interface all
Interface Ethernet 1/1
  Mode Off
Interface Ethernet 1/2
  Mode Off
Interface Ethernet 1/3
  Mode Off
Interface Ethernet 1/4
  Mode Off
...
Interface Ethernet 3/18
  Mode 802.3x
     TX    RX          TX Output Paused    RX
  Admin Admin      Frames  512 BitTimes     Frames
  ------------------------------------------------
     Off   On           0                        0
```

The following example displays the flow control information on a specific interface.

```
device# show qos flowcontrol interface ethernet 3/18
Interface Ethernet 3/18
  Mode 802.3x
     TX    RX          TX Output Paused    RX
  Admin Admin      Frames  512 BitTimes     Frames
  ------------------------------------------------
     Off   On           0                       0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos interface all

Displays QoS configuration information about Ethernet, Virtual Ethernet, and port-channel interfaces.

Syntax

show qos interface all

Modes

Privileged EXEC mode.

Usage Guidelines

This command can produce pages of output.

Examples

To show QoS information for all interfaces use the following command.

```
device# show qos interface all
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ve 20
  Provisioning Mode: none

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

...

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 2/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
      ---------------------------------------
             Out-TC: 0  1  2  3  4  5  6  7
             Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
              In-TC: 0  1  2  3  4  5  6  7
      ---------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  5  6  7
      Out-CoS(DP=1): 0  1  2  3  4  5  6  7
      Out-CoS(DP=2): 0  1  2  3  4  5  6  7
      Out-CoS(DP=3): 0  1  2  3  4  5  6  7
```

```
  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      -------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 1/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
      ---------------------------------------
             Out-TC: 0  1  2  3  4  5  6  7
             Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
              In-TC: 0  1  2  3  4  5  6  7
      ---------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  5  6  7
      Out-CoS(DP=1): 0  1  2  3  4  5  6  7
      Out-CoS(DP=2): 0  1  2  3  4  5  6  7
      Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
```

```
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      -------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
            TC:      0       1       2       3       4       5       6       7
      ------------------------------------------------------------------------
      Threshold:     0       0       0       0       0       0       0       0

  Flow control mode Off

... <output truncated>
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos interface ethernet

Displays QoS configuration information for a specific Ethernet interface.

Syntax

show qos interface ethernet *slot/port*

Parameters

slot/port

A specific Ethernet interface slot and port number.

Modes

Privileged EXEC mode.

Examples

To display the QoS configuration for a specific interface use the following command.

```
device# show qos interface ethernet 1/19
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 1/19
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
         ---------------------------------------
             Out-TC: 0  1  2  3  4  5  6  7
             Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
              In-TC: 0  1  2  3  4  5  6  7
         ---------------------------------------
         Out-CoS(DP=0): 0  1  2  3  4  5  6  7
         Out-CoS(DP=1): 0  1  2  3  4  5  6  7
         Out-CoS(DP=2): 0  1  2  3  4  5  6  7
         Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
         d1 :  d2 0  1  2  3  4  5  6  7  8  9
         ---------------------------------------
          0 :    00 01 02 03 04 05 06 07 08 09
          1 :    10 11 12 13 14 15 16 17 18 19
          2 :    20 21 22 23 24 25 26 27 28 29
          3 :    30 31 32 33 34 35 36 37 38 39
          4 :    40 41 42 43 44 45 46 47 48 49
          5 :    50 51 52 53 54 55 56 57 58 59
          6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
         d1 :  d2  0   1   2   3   4   5   6   7   8   9
         -------------------------------------------------
          0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
          1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
          2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
          3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
          4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
          5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
          6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
         d1 :  d2 0  1  2  3  4  5  6  7  8  9
         ---------------------------------------
          0 :    00 00 00 00 00 00 00 00 01 01
          1 :    01 01 01 01 01 01 02 02 02 02
          2 :    02 02 02 02 03 03 03 03 03 03
          3 :    03 03 04 04 04 04 04 04 04 04
          4 :    05 05 05 05 05 05 05 05 06 06
          5 :    06 06 06 06 06 06 07 07 07 07
          6 :    07 07 07 07

    RED Enabled on the following Priorities:
      TC: 0, Profile Id: 100
      TC: 1, Profile Id: 101
      TC: 2, Profile Id: 102
      TC: 3, Profile Id: 103
      TC: 4, Profile Id: 104
      TC: 5, Profile Id: 105
      TC: 6, Profile Id: 106
      TC: 7, Profile Id: 107

Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0      1      2      3      4      5      6      7
         ------------------------------------------------------------------
         Threshold:      0      0      0      0      0      0      0      0
```

```
Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos interface ve

Displays QoS configuration information about a specific Virtual Ethernet interface.

Syntax

show qos interface ve *ve_number*

Parameters

ve_number

A specific Virtual Ethernet number.

Modes

Privileged EXEC mode.

Examples

Follow this example to view information about a specific VE interface.

```
device# show qos interface ve 20
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ve 20
  Provisioning Mode: none

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0       1       2       3       4       5       6       7
      ------------------------------------------------------------------------
      Threshold:      0       0       0       0       0       0       0       0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos maps cos-traffic-class

Displays configured CoS-to-traffic class mutation maps.

Syntax

show qos maps cos-traffic-class

Modes

Privileged EXEC mode.

Examples

To display information on defined QoS CoS-to-traffic class mutation maps and where they are applied, use this command.

```
device# show qos maps cos-traffic-class

Cos-to-Traffic Class map 'cosTCMap'
In-Cos        : 0 1 2 3 4 5 6 7
-------------------------------------
TrafficClass  : 0 1 2 3 3 6 6 6
DropPrecedence: 0 0 0 0 0 1 0 1

Enabled on the following interfaces:
    Eth 1/4
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos maps dscp-cos

Displays configured DSCP to CoS mutation maps.

Syntax

show qos maps dscp-cos

Modes

Privileged EXEC mode

Examples

To display information on defined QoS DSCP to CoS mutation maps and where they are applied, use this command.

```
device# show qos maps dscp-cos

Dscp-to-CoS map 'dscpCoS' (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-------------------------------------
0 :    00 00 00 00 00 00 00 00 01 01
1 :    01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 04 03 03 03 03 03 03
3 :    03 03 04 04 04 04 04 04 04 04
4 :    05 05 05 05 05 05 05 05 06 06
5 :    06 06 06 06 06 06 07 07 07 07
6 :    07 07 07 07

   Enabled on the following interfaces:
    Eth 1/3
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos maps dscp-mutation

Displays configured DSCP mutation maps.

Syntax

show qos maps dscp-mutation [*map-name*]

Modes

Privileged EXEC mode

Examples

To display information on defined QoS DSCP mutation maps and where they are applied, use this command.

```
device# show qos maps dscp-mutation

Dscp-to-Dscp Mutation map 'dscpMut' (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-------------------------------------
0 :    00 01 02 03 04 05 06 07 08 09
1 :    10 11 12 13 14 15 16 17 18 19
2 :    20 21 22 23 24 25 26 27 28 29
3 :    30 31 32 33 34 35 36 37 38 39
4 :    40 41 42 43 44 45 46 47 48 49
5 :    50 51 52 53 54 55 56 57 58 59
6 :    40 61 62 63

   Enabled on the following interfaces:
    Eth 1/3
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos maps dscp-traffic-class

Displays configured DSCP to traffic class mutation maps.

Syntax

show qos maps dscp-traffic-class

Modes

Privileged EXEC mode

Examples

To display information on defined QoS DSCP to traffic class mutation maps and where they are applied, use this command.

```
device# show qos maps dscp-traffic-class

Dscp-to-Traffic-Class map 'dscpTC'
{x/y: traffic-class = x, drop-precedence = y & dscp = d1d2}
d1 :  d2  0   1   2   3   4   5   6   7   8   9
---------------------------------------------------
0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 4/2 1/0
1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
6 :     7/0 7/0 7/0 7/0

   Enabled on the following interfaces:
    Eth 1/4
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos maps traffic-class-cos

Displays configured traffic class to CoS mutation maps.

Syntax

show qos maps traffic-class-cos

Modes

Privileged EXEC mode

Examples

To display information on defined QoS DSCP to traffic class to CoS mutation maps and where they are applied, use this command.

```
device# show qos maps traffic-class-cos

Traffic Class-to-Cos map 'tcCoS' (drop-precedence = dp0 to dp3)
   TrafficClass  : 0  1  2  3  4  5  6  7
   ---------------------------------------
   Out-Cos(dp0)  : 0  1  2  3  4  5  6  7
   Out-Cos(dp1)  : 0  1  2  3  4  5  6  7
   Out-Cos(dp2)  : 0  1  2  3  4  4  6  7
   Out-Cos(dp3)  : 0  1  2  3  4  5  6  7

   Enabled on the following interfaces:
    Eth 1/4
```

History

Release version	Command history
18x.1.00	This command was introduced.

show qos tx-queue interface

Displays a summary of the runtime egress queue state information applied to a Layer 2 interface.

Syntax

show qos tx-queue interface { **ethernet** *slot/port* }

Parameters

ethernet

Represents a valid, physical Ethernet interface.

slot

Specifies a valid slot number. The only valid value is 0.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display the runtime egress queue state information retrieved from the dataplane:

```
device# show qos tx-queue interface ethernet 0/1
Interface Ethernet 0/1
          In-use        Max             TX        Dropped               TX           Dropped
  TC       Bytes      Bytes        Packets       Packets            Bytes             Bytes
  ----------------------------------------------------------------------------------------
    0          0     748288              0             0                0                 0
    1          0     748288    35739153669             0     1133120185038                 0
    2          0     748288              0             0                0                 0
    3          0     748288              0             0                0                 0
    4          0     748288              0             0                0                 0
    5          0     748288              0             0                0                 0
    6          0     748288              0             0                0                 0
    7          0     748288       30715725             2       2765239372               164
```

History

Release version	Command history
18s.1.01	This command was introduced.

show rmon

Displays the current RMON status on the device.

Syntax

show rmon [**alarms** [*number*] [**brief**] | **events** [*number*] [**brief**] | **logs** [*event_number*] | **statistics** [*number*] [**brief**]]

Parameters

alarms

Specifies to display the RMON alarm table.

number

Specifies the alarm index identification number. Valid values range from 1 through 65535.

brief

Specifies to display a brief summary of the output.

events

Specifies to display the RMON events table.

number

Specifies the event index identification number. Valid values range from 1 through 65535.

brief

Specifies to display a brief summary of the output.

logs

Specifies to display the RMON log table.

event_number

Specifies the event log index identification number. Valid values range from 1 through 65535.

statistics

Specifies to display the statistics identification number.

number

Specifies the statistics identification number. Valid values range from 1 through 65535.

brief

Specifies a brief summary of the output.

Modes

Privileged EXEC mode

Examples

To display the RMON statistics:

```
device# show rmon statistics

rmon collection index 4
    Interface index is Id: 67108864 , Name : Ethernet 0/13
    Receive Statistics:
        218903 packets, 14015626 bytes,  0 packs dropped
        Multicasts: 218884, Broadcasts: 18
        Under-size : 0, Jabbers: 0, CRC: 0
        Fragments: 0, Collisions: 0
             64 byte pkts: 218722, 65-127 byte pkts: 174
        128-255 byte pkts: 0, 256-511 byte pkts: 6
        512-1023 byte pkts: 0, 1024-1518 byte pkts: 0
        Over 1518-byte pkts(Oversize - Jumbo): 0
    Owner: RMON_SNMP
    Status: ok(1)
```

To display the RMON events:

```
device# show rmon events

event Index = 4
        Description "My Description"
        Event type Log & SnmpTrap
        Event community name admin
        Last Time Sent = 00:00:00
        Owner  admin
```

History

Release version	Command history
18x.1.00	This command was introduced.

show rmon history

Displays information gathered by rmon event and rmon alarm commands.

Syntax

show rmon history [**statistics** | *history_index*]

Parameters

statistics

Displays a more detailed synopsis.

history_index

Specifies the RMON history identification number. Valid values range from 1 through 65535.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display a synopsis of the statistics collected by the **rmon event** and **rmon alarm** commands.

Add the **statistics** parameter to display the detailed history.

Examples

To display the RMON history:

```
device# show rmon history

RMON history control entry 1
interface: ifIndex.1745682445 Ethernet 0/13
buckets requested: 20
buckets granted: 20
sampling interval: 10
Owner: jsmith
```

History

Release version	Command history
18x.1.00	This command was introduced.

show route-map

Displays route-map configuration details.

Syntax

show route-map [*name*]

show route-map interface [**ethernet** *slot/port* | **port-channel** *index* | **ve** *ve-number*]

Parameters

name
Specifies the name of the route-map.

interface
Specifies an interface.

ethernet *slot/port*
Specifies a physical interface.

port-channel *index*
Specifies a port-channel.

ve *ve-number*
Specifies a virtual Ethernet interface.

Modes

Privileged EXEC mode

Command Output

The **show route-map** command displays the following information:

Output field	Description
Active/Inactive	Indicates the instantiation of the route-map configuration into the underlying hardware. Possible meanings for inactive may be no room in the TCAM for programming the ACL, or the exhaustion of next-hop entries within the hardware next-hop table.
Selected	Indicates which of the configured next hops is currently being used by the policy. If the keyword selected is absent from the display, it indicates that none of the next hops in the list is being used and the packet is being routed by the standard routing mechanism.
Policy routing matches	Provides a summary of the number of times any of the match criteria within the specific ACL have been hit. If the ACL binding was unable to allocate a counter for the ACL (due to resource exhaustion) the count value will show "Counter not available" otherwise an actual counter value will be displayed.

Examples

The following example displays route-map details for all route-maps.

```
device# show route-map
Interface Ethernet 1/6
 ip policy route-map route1
```

The following example displays route-map details for a specific route-map.

```
device# show route-map route1
Interface Ethernet 1/6
ip policy route-map route1 permit 1 (Active)
    match ip address acl test1
    set ip next-hop 6.0.0.1 (selected)
    Policy routing matches: 1443 packets
```

The following example displays route-map details on a specific interface.

```
device# show route-map interface ethernet 1/6
Interface Ethernet 1/6
ip policy route-map route1 permit 1 (Active)
    match ip address acl test1
    set ip next-hop 6.0.0.1 (selected)
    Policy routing matches: 1543 packets
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config

Displays the contents of the running configuration.

Syntax

show running-config

Parameters

Refer to the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the running configuration.

This command is supported only on the local device.

To display the list of available configuration entries, enter **show running-config ?**.

The **show running-config** option displays the global configuration and also the configuration on all interfaces.

The **show running-config interface** options display only the configuration for the interfaces specified.

Examples

The following command example displays the contents of the device running configuration.

```
device# show running-config
```

The following example displays the running configuration for an Ethernet interface. This example is for Network Packet Broker (NPB) mode, on an interface with 802.1BR header-stripping enabled.

```
device# show running-config interface ethernet 1/3
interface Ethernet 1/3
 strip-802-1br
 shutdown
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config aaa

Displays the configuration attributes for the authentication, authorization, and accounting (AAA) server from the configuration database.

Syntax

show running-config aaa [**accounting** [**commands** | **exec**] | **authentication** [**login**]]

Parameters

accounting

Configures Login or Command accounting

commands

Enable/Disable Command accounting

exec

Enable/Disable Login accounting

authentication

Configures preferred order of Authentication output modifiers

login

Configures the order of sources for login (default = 'local')

Modes

Privileged EXEC mode

Usage Guidelines

Refer to the **aaa authentication** command for a description of the displayed attributes.

Examples

To display the authentication mode:

```
device# show running-config aaa
aaa authentication radius local
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none

device# show running-config aaa authentication
aaa authentication login radius local

device# show running-config aaa authentication
aaa authentication login ldap local-auth-fallback
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config aaa accounting

Displays the AAA server accounting configuration.

Syntax

show running-config aaa accounting

Modes

Privileged EXEC mode

Usage Guidelines

Refer to the **aaa authentication** command for a description of the displayed attributes.

Examples

To displaying the authentication mode:

```
device# show running-config aaa accounting
aaa accounting exec default start-stop tacacs+
aaa accounting commands default start-stop tacacs+
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config aaa command authorization

Displays the current status for TACACS+ authorization of command privileges for the user role.

Syntax

show running-config aaa command authorization

Modes

Privileged EXEC mode

Usage Guidelines

Examples

Example of the active status:

```
device# show running-config aaa command authorization
aaa command authorization tacacs+
```

Example of the inactive status:

```
device# show running-config aaa authorization
aaa command authorization none
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config arp

Displays static ARP entries created in the running configuration, using the **arp** command, with an option to display ARP ACLs.

Syntax

show running-config arp

show running-config arp *ip-address* [**ethernet** *slot* **/** *port* | **ve** *ve-id*]

show running-config arp access-list

show running-config arp access-list *arp-acl-name* [**permit ip host** [*host-ip-address* [**mac host** [*host-mac-address*]]]

Parameters

ip-address
Specifies the IPv4 address of a static ARP.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

ve *ve-id*
Specifies a virtual ethernet (VE) interface.

access-list *arp-acl-name*
Specifies the name of an ARP ACL defined on the device.

permit ip host *host-ip-address*
Specifies rules that permit ARP messages from hosts specified by both IPv4 and MAC addresses.

host-ip-address
Specifies the IPv4 address.

mac host *host-mac-address*
Specifies the MAC address.

Modes

Privileged EXEC mode

Examples

The following example displays a sample run of the **show running-config arp** command.

```
device# arp 12.1.1.2 0000.0000.0001 interface Ethernet 0/1
```

The following example displays a sample run of the **show running-config arp access-list** option.

```
device# arp access-list acl1
 permit ip host 13.1.1.2 mac host 0000.0000.0002
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config dpod

Displays Dynamic Ports on Demand (DPOD) license information.

Syntax

show running-config dpod [*slot/port*]

Command Default

Displays all port reservations on the local switch.

Parameters

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display port reservations for a specified port or for all ports on the local switch.

Examples

To display port reservations for all ports on the local switch:

```
device# show running-config dpod 8/15
dpod 8/15
 reserve
!
switch# show running-config dpod 8/16
dpod 8/16
 reserve
```

To display port reservations on a switch that does not support the DPOD feature:

```
device# show running-config dpod

%No entries found
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config event-handler

Displays details of one or all event-handler profiles configured on the device. You can filter the results by description, Python-script action, or trigger ID. You can also display the Python-script action associated with a profile.

Syntax

show running-config event-handler [*event-handler-name*]

show running-config event-handler *event-handler-name* **description**

show running-config event-handler *event-handler-name* **action**

show running-config event-handler *event-handler-name* **trigger** [*trigger-id* [**raslog** *raslog-id* [**pattern** *posix-ext-regex*]]]

Parameters

event-handler-name
Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

action
Displays by Python script file-names.

description
Describes the event-handler profile. The string can be 1 through 128 characters in length.

trigger *trigger-id*
Specifies an event-handler trigger. When the trigger-condition occurs, a Python script is run.

raslog *raslog-id*
Specifies a RASlog message ID as the trigger.

pattern *posix-ext-regex*
Specifies a POSIX extended regular expression to search for a match within the specified RASlog message ID. For examples, refer to the "trigger" topic.

Modes

Privileged EXEC mode

Command Output

The **show running-config event-handler** command displays the following information:

Output field	Description
event-handler	Displays the event-handler name.
action python-script	Displays the name of the Python script called if the event handler is triggered.
trigger	Displays a trigger name and definitions

Examples

The following example displays the details of all triggers defined for a specified event-handler.

```
device# show running-config event-handler evh1 trigger
event-handler evh1
 trigger 1 raslog NSM-1001
```

The following example displays the details of the action defined for a specified event-handler.

```
device# show running-config event-handler evh1 action
event-handler evh1
 action python-script vlan.py
```

The following example displays the details of all defined event-handlers.

```
device# show running-config event-handler
event-handler evh2
 trigger 100 raslog NSM-1001
 action python-script vlan.py
!
```

show running-config ip access-list

Displays a list of IPv4 ACLs defined on the switch, including the rules they contain.

Syntax

show running-config ip access-list [{ **standard** | **extended** } [*ACL_name*]]

Parameters

standard
Specifies the standard ACL type.

extended
Specifies the extended ACL type.

ACL_name
Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all IPv4 ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of IPv4 ACLs bound to interfaces, use the **show access-list ip** command.

Examples

The following example displays the IPv4 ACLs defined on the switch.

```
device# show running-config ip access-list

ip access-list standard stdACL3
  seq 5 permit host 10.20.33.4
  seq 7 permit any
ip access-list extended extdACL5
  seq 5 deny tcp host 10.24.26.145 any eq 23
  seq 7 deny tcp any any eq 80
  seq 10 deny udp any any range 10 25
  seq 15 permit tcp any
ip access-list extended extdACLwithNoRules
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config ip receive

Syntax

show running-config ip receive [**access-group**]

Parameters

access-group
Specifies an IPv4 ACL applied at device-level.

acl-name
Specifies an IPv4 standard or extended ACL.

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config ipv6

Displays global ipv6 configurations.

Syntax

show running-config ipv6 [**access-list** [**extended** | **standard**] *ipv6-acl-name* **seq** *sequence-number*]

show running-config ipv6 [**import routes**]

show running-config ipv6 [**nd** [**global-suppress-ra** | **ra-dns-server** | **ra-domain-name**]]

show running-config ipv6 [**prefix-list** [**ge** | **le**] *prefix-length*]

show running-config ipv6 [**protocol** [**vrrp** | **vrrp-extended**]

show running-config ipv6 [**receive access-group**]

show running-config ipv6 [**route**]

show running-config ipv6 [**router ospf** [**vrf**]]

Parameters

access-list
Specifies the access-control list (ACL)

extended
Specifies the extended IP ACL.

standard
Specifies the standard IP ACL.

ipv6-acl-name
The IPv6 ACL name.

seq *sequence-number*
Specifies the sequence number.

import routes
Specifies import IPv6 routes.

nd
Displays neighbor discovery commands.

global-suppress-ra
Sets the suppress-ra option globally .

ra-dns-server
Sets the global DNS server option applied on all ND6.

ra-domain-name
Set the global domain name option that applied on all ND6 interfaces.

prefix-list
Specifies the prefix-list.

ge
Specifies the minimum IPv6 prefix length.

prefix-length
The IPv6 prefix length. The range is from 1 through 128.

le
Specifies the maximum IPv6 prefix length.

protocol
Set the global domain name option that applied on all ND6 interfaces.

vrrp
Specifies the Virtual Router Redundancy Protocol IPv6 (VRRPv3).

vrrp-extended
Specifies the Virtual Router Redundancy Protocol IPv6 Extended (VRRPv3-E).

receive
Specifies the receive ACL.

access-group
Specifies to bind or unbind the existing ACL.

route
Specifies the IPv6 unicast static route.

router
Specifies the IPv6 router.

ospf
Specifies the Open Shortest Path First (OSPF) version 3.

vrf
Specifies the VRF instance.

Modes

Privileged EXEC mode

Examples

The following is an example of the **show running-config ipv6** command output.

```
device# show running-config ipv6
ipv6 route 3063:6363::/64 fe80::52eb:1aff:fe97:cf51 ve 4050
ipv6 nd ra-dns-server 2000:1234:122:ffff::ffee
ipv6 nd ra-dns-server 3500:35:0:35::1
ipv6 nd ra-domain-name extreme.com
ipv6 nd ra-domain-name user.co.in
ipv6 nd ra-domain-name netiron.com
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config ipv6 access-list

Displays a list of IPv6 ACLs defined on the switch, including the rules they contain.

Syntax

show running-config ipv6 access-list [{ **standard** | **extended** } [*ACL_name*]]

Parameters

standard
Specifies the standard ACL type.

extended
Specifies the extended ACL type.

ACL_name
Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all IPv6 ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of all IPv6 ACLs bound to interfaces, use the **show access-list ipv6** command.

Examples

The following example displays all standard IPv6 ACLs defined on the switch:

```
device# show running-config ipv6 access-list standard
ipv6 access-list standard distList
 seq 10 deny 2001:125:132:35::/64
 seq 20 deny 2001:54:131::/64
 seq 30 deny 2001:5409:2004::/64
 seq 40 permit any
!
ipv6 access-list standard ipv6_acl_std_1
 seq 10 deny 2001:2001::/64 count log
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config lag hash

Displays non-default LAG hash values.

show running-config lag hash [**hdr-count**] [**hdr-start**] [**srcport**]

Parameters

hdr-count *count*
: Specifies the number of headers to be considered for LAG hashing. Values range from 1 through 3. The default is 1.

hdr-start
: Specifies where to start picking headers for the key generation.

srcport
: Includes the source port in the hashing configuration. The default is not to include it.

Modes

Privileged EXEC mode

Usage Guidelines

To display all configured values (including defaults), enter the **show port-channel load-balance** command.

Examples

The following example displays the output of the basic **show running-config lag hash** command.

```
device# show running-config lag hash
lag hash hdr-start term
lag hash hdr-count 2
lag hash srcport
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config ldap-server

Displays the SSH server status in the running-config.

Syntax

show running-config ldap-server [**host** *ipaddr* | **host-name**]

Parameters

host

Identifies the IPv4 address of the host.

ipaddress

IPv4 address of the host.

host-name

Name of the host.

Modes

Privileged EXEC mode

Usage Guidelines

LDAP server configuration is placed at the beginning of the running-config and is part of the global configuration of the device. LDAP is enabled by default and no entry is shown in the running-config when set to default.

Attributes with default values will not be displayed.

Examples

```
device# show running-config ldap-server host 10.24.65.6
ldap-server host 10.24.65.6 use-vrf mgmt-vrf
port 3890 retries 3 timeout 8 basedn security.extreme.com
device#
```

History

Release version	Command history
18x.1.00	This command was added.

show running-config mac access-list

Displays a list of MAC ACLs defined on the switch, including the rules they contain.

Syntax

show running-config mac access-list [{ **standard** | **extended** } [*ACL_name*]]

Parameters

standard
Specifies the standard ACL type.

extended
Specifies the extended ACL type.

ACL_name
Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all MAC ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of all MAC ACLs bound to interfaces, use the **show access-list mac** command.

Examples

The following example displays all MAC ACLs defined on the switch.

```
device# show running-config mac access-list
mac access-list standard stdmacaclin
seq 11 permit 1111.1112.1113 7777.7777.7777 count log
seq 12 permit 1111.1112.1114 7777.7777.7777 count log
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config password-attributes

Displays global password attributes.

Syntax

show running-config password-attributes [**admin-lockout**] [**max-lockout-duration**] [**max-retry**] [**min-length**]

show running-config password-attributes character-restriction [**lower** | **numeric** | **special-char** | **upper**]

Parameters

admin-lockout
Displays lockout for admin role accounts.

max-retry
Displays the number of failed password logins permitted before a user is locked out. Values range from 0 through 16 attempted logins. The default value is 0.

min-length
Displays the minimum length of the password. Valid values range from 8 through 32 characters. The default is 8 characters.

max-lockout-duration
Displays the maximum number of minutes after which the user account is unlocked. Range is from 0 through 99999. The default is 0, representing an infinite duration.

character-restriction
Displays the restriction on various types of characters.

lower
Displays the minimum number of lowercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

numeric
Displays the minimum number of numeric characters that must occur in the password. Values range from 0 through 32 characters. The default is 0.

special-char
Displays the number of punctuation characters that must occur in the password. All printable, nonalphanumeric punctuation characters, except colon (:) are allowed. Values range from 0 through 32 characters. The default value is 0.

upper
Displays the minimum number of uppercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

Modes

Privileged EXEC mode

Usage Guidelines

The attributes are not displayed when they hold default values.

Examples

The following example displays all global password attributes.

```
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
password-attributes max-lockout-duration 5000
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config radius-server

Displays the local device configuration for the RADIUS server from the configuration database.

Syntax

show running-config radius-server host { *ip-address* | *hostname* }

Parameters

host

Identifies the RADIUS server by host name or IP address.

hostname

Specifies the host name of the RADIUS server.

ip-address

Specifies the IP address of the RADIUS server. IPv4 and IPv6 are supported.

Modes

Privileged EXEC mode

Examples

```
device# show running-config radius-server host 10.38.37.180

radius-server host 10.38.37.180
protocol   pap
key          changedsec
timeout    3
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config rmon

Displays Remote Monitor configuration information.

Syntax

show running-config rmon [**alarm** | **event**]

Parameters

alarm

Displays the Remote Monitor alarm configuration.

event

Displays the Remote Monitor event configuration

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config role

Displays name and description of the configured roles.

Syntax

show running-config role [**name** *role_name* [**desc**]]

Parameters

name *role_name*

Displays roles defined for users.

desc

Displays role descriptions.

Modes

Privileged EXEC mode

Examples

The following example displays all roles configured on the device.

```
device# show running-config role
role name admin desc Administrator
role name user desc User
role name VLANAdmin desc "Manages security CLIs"
role name NetworkAdmin desc "Manages Network CLIs"
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config rule

Displays configured access rules.

Syntax

show running-config rule [*index*]

show running-config rule *index* { **action** | **command** *command_name* | **operation** | **role** }

show running-config rule { **action** { **reject** | **accept** } | **command** *command_name* | **operation** { **read-only** | **read-write** } | **role** *role-name* }

Parameters

index

Displays the rule with the specified index number. Values range from 1 through 512.

action reject | **accept**

Following the *index* parameter, indicates whether **reject** or **accept** is specified for that rule. If the *index* parameter is not specified, displays all rules with the specified action.

command *command_name*

Displays rule configuration for the specified command. To display a list of supported commands, type a question mark (?). This list varies according to whether or not you specify a rule index.

operation read-only | **read-write**

Following the *index* parameter, indicates whether **read-only** or **read-write** is specified for that rule. If the *index* parameter is not specified, displays all rules with the specified operation.

role *role-name*

Displays rule configuration for the specified role.

Modes

Privileged EXEC mode

Examples

The following example displays the configured roles and their rules.

```
device# show running-config rule

rule 30 action accept operation read-write role NetworkSecurityAdmin
rule 30 command role
!
rule 31 action accept operation read-write role NetworkSecurityAdmin
rule 31 command rule
!
rule 32 action accept operation read-write role NetworkSecurityAdmin
rule 32 command username
!
rule 33 action accept operation read-write role NetworkSecurityAdmin
rule 33 command aaa
!
rule 34 action accept operation read-write role NetworkSecurityAdmin
rule 34 command radius-server
!
rule 35 action accept operation read-write role NetworkSecurityAdmin
rule 35 command configure
```

The following example displays a single rule.

```
device# show running-config rule 30

rule 30
 action accept operation read-write role NetworkSecurityAdmin command role
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config ssh

Displays the Secure Shell (SSH) status in the running-config.

Syntax

show running-config ssh

Modes

Privileged EXEC mode

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config ssh server

Displays the SSH server status in the running-config.

Syntax

show running-config ssh server

Modes

Privileged EXEC mode

Usage Guidelines

SSH server configuration is placed at the beginning of the running-config and is part of the global configuration of the device. SSH is enabled by default and no entry is shown in the running-config when set to default.

Examples

When SSH service is shut down:

```
device# show running-config ssh server
ssh server shutdown
device# show running-config ssh server
ssh server shutdown
ssh server key-exchange dh-group-14
```

When SSH service is enabled:

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config ssh server key-exchange

Displays the SSH server key-exchange status in the running-config.

Syntax

show running-config ssh server key-exchange

Modes

Privileged EXEC mode

Examples

Typical command output:

```
device# show running-config ssh server key-exchange
 ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange is configured to DH Group 14:

```
device# show running-config ssh server key-exchange
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange method has the default value:

```
device# show running-config ssh server key-exchange
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config telemetry collector

Displays the current configuration of telemetry collectors.

Syntax

show running-config telemetry collector

Modes

Privileged EXEC mode

Usage Guidelines

The output includes the settings for the currently configured collectors.

Examples

Typical command example:

```
device# show running-config telemetry collector
telemetry collector <collector-profile-1>
  ip <ipv4address1> port <portNum>
  profile system-profile default_system_utilization_statistics
  profile interface-profile default_interface_statistics
  use-vrf mgmt-vrf
  encoding json
  activate
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config telemetry profile

Displays the current configuration settings of Telemetry profiles.

Syntax

show running-config telemetry profile [**enhanced-queue-discard-pkts** | **enhanced-queue-max-queue-depth** | **queue**]

Modes

Privileged EXEC mode

Parameters

enhanced-queue-discard-pkts

Displays a subset of the data highlighting discarded packet information.

enhanced-queue-max-queue-depth

Displays a subset of the data highlighting maximum queue depth information.

queue

Displays the field configuration information for the current telemetry profile queue.

Usage Guidelines

The output includes all default profiles and any custom defined telemetry profiles.

Command Output

The **show running-config telemetry profile** command displays the following information:

Output field	Description
profile-type	Each profile is identified by a unique profile type.
interval	Interval at which the profile information is streamed to interested clients or collectors.
add field-id	Indicates field identifier available for streaming.
interface intf-range	When applicable to a profile-type, will have additional required parameters.

Examples

Typical command example.

```
device# show running-config telemetry profile
telemetry profile system-utilization default_system_utilization_statistics
  interval 60
  add total-system-memory
  add total-used-memory
  …
 add uptime
telemetry profile interface default_interface_statistics
  interval 30
  interface 0/1-20
  add out-pkts
  add in-pkts
  …
  add out-discards
  add in-discards
!
```

Example using the **enhanced-queue-discard-pkts** keyword.

```
device# show running-config telemetry profile enhanced-queue-discard-pkts
telemetry profile enhanced-queue-discard-pkts default_enhanced_queue_discard_pkts_statistics
interval 240
interface-range 0/1-2,0/3:1-2
add discard-pkts
```

Example using the **enhanced-queue-max-queue-depth** keyword.

```
device# show running-config telemetry profile enhanced-queue-max-queue-depth
telemetry profile enhanced-queue-max-queue-depth default_enhanced_queue_max_queue_depth_statistics
interval 240
interface-range 0/4-5,0/6
add max-queue-depth
```

Example using the **queue** keyword.

```
device# show running-config telemetry profile queue
telemetry profile queue default_queue_statistics
interval 240
interface-range 0/1-2,0/3:1-2
add enq-pkt-count
add enq-byte-count
add discard-pkt-count
add discard-byte-count
add current-queue-size
add max-queue-depth-size
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config telemetry server

Displays the current configuration of the Telemetry server.

Syntax

show running-config telemetry server [**use-vrf**]

Parameters

use-vrf

Displays all VRF configurations. By default, only the default mgmt-vrf is displayed.

Modes

Privileged EXEC mode

Usage Guidelines

The output displays the current configuration for the Telemetry server.

Examples

Typical command example.

```
device# show running-config telemetry server
device# show running-config telemetry server
telemetry server use-vrf mgmt-vrf
 transport tcp
 port 50051
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

show running-config username

Displays the user accounts on the device.

Syntax

show running-config username [*username*] [**access-time**] [**desc**] [**enable**] [**encryption-level**] [**expire**] [**password**] [**role**]

Parameters

username
Displays the configuration of a specified username. The maximum number of characters is 40.

access-time
Displays access-time configuration.

desc
Displays the description of the user configuration.

enable
Displays the account enablement status.

encryption-level
Password encryption level. Values are 0 through 7. The default is 0.

expire
Date until the password remains valid in YYYY-MM-DD format. Valid year values range from 1902 through 2037. By default, passwords do not expire.

password
Account password.

role
The role associated with the account.

Modes

Privileged EXEC mode

Usage Guidelines

To display details for one user only, specify *username* . Otherwise, this command displays all user accounts on the device.

Use the various parameters to query the specified account details.

This command does not display the root account.

Defaults are not displayed.

Examples

The following example displays the user accounts on the device.

```
device# show running-config username

username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role admin desc Administrator
username user password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role user desc User
```

The following example displays a specific user account.

```
device# show running-config username admin

username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role admin desc Administrator
```

The following example displays the enabled status for a specific user account.

```
device# show running-config username admin enable

username admin enable true
```

The following example displays user access on the device.

```
device# show running-config username access-time
username admin access-time ""
username jsmith access-time 0000
username user access-time ""
username user1 access-time 1700
```

History

Release version	Command history
18x.1.00	This command was introduced.

show sflow

Displays sFlow configuration information and statistics.

Syntax

show sflow interface | all

Command Default

sFlow is disabled on all interfaces.

Parameters

all

Displays all sFlow information and statistics.

interface

Displays sFlow information for an Ethernet interface.

Modes

Privileged EXEC mode

Examples

The following example displays sFlow information.

```
device# show sflow
sFlow services are:                     enabled
sFlow null0 sampling:                   enabled
Global default sampling rate:           2048 pkts
Global default counter polling interval: 20 secs
sFlow Agent-ID address:                 21.21.21.21
sFlow Source Interface:                 management 0
Collector server address                       Vrf-Name      Sflow datagrams sent
-------------------------------------------------------------------------------
                          10.1.3.2:6343        default-vrf                  438
                     172.22.108.57:6343        mgmt-vrf                     438
                    2001:10:1:4::2:6343        default-vrf                  438

ACL based samples collected (permit):    0
ACL based samples collected (deny):      0
VxLAN Visibility samples collected:      0
VxLAN Gateway samples collected:         0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show span path session

Displays the SPAN path information.

Syntax

show span path session *session-number*

Parameters

session-number

Specifies the SPAN session.

Modes

Privileged EXEC mode

Examples

The following example displays the SPAN path information.

```
device# show span path session 1

Session                          :1
Path                       :Eth 0/10 -> Eth 0/1 (ISL-exit port) -> Eth 0/16
```

History

Release version	Command history
18x.1.00	This command was introduced.

show spanning-tree

Displays Spanning Tree Protocol (STP) information.

Syntax

show spanning-tree [**brief** | **interface** { **ethernet** *slot/port* | **port-channel** *port_channel_number* } | **pvst** | **mst** [**brief** | **detail** | **instance** *instance_id* | **interface**] **mst-config** | **vlan** *vlan_id*]

Parameters

brief
Display brief spanning tree information.

interface
Display iinformation about the spanning tree configuration on an interface.

ethernet *slot/port*
Display spanning tree information about a specific Ethernet interface.

port-channel *port_channel_number*
Display spanning tree information about a port channel interface.

pvst
Display PVST+ information.

mst
Display MSTP information.

detail
Display detailed MSTP tree information.

instance *instance_id*
Display MSTP information about a specivic instance.

mst-config
Display MSTP region configuration information.

vlan *vlan_id*
Display spanning tree information about a specific VLAN.

Modes

Privileged EXEC mode.

Usage Guidelines

NOTE
Extreme Networks supports the PVST+ and R-PVST+ protocols. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples

To display spanning tree information:

```
device# show spanning-tree brief

 Spanning-tree Mode: Spanning Tree Protocol

      Root ID      Priority 4096
                   Address 768e.f805.5800
                   Hello Time 8, Max Age 25, Forward Delay 20

      Bridge ID    Priority 4096
                   Address 768e.f805.5800
                   Hello Time 8, Max Age 25, Forward Delay 20

 Interface     Role  Sts  Cost       Prio  Link-type        Edge
 ------------------------------------------------------------------------
 Eth 2/32      DES   FWD  2000       128   P2P               No
 Eth 2/66      DES   FWD  2000       128   P2P               No
 Po 7          DES   FWD  2000       128   P2P               No
 Po 8          DES   FWD  2000       128   P2P               No
 Po 21         DES   LIS  500        128   P2P               No
 Po 141        BKUP  BLK  1000       128   P2P               No
 Po 151        DES   FWD  10000      128   P2P               No
 Po 154        DES   FWD  285        128   P2P               No
 Po 172        BKUP  BLK  1000       128   P2P               No
 Po 173        BKUP  BLK  500        128   P2P               No
```

Release version	Command history
18x.1.00	This command was introduced.

show ssh client status

Displays the current Secure Shell (SSH) client key-exchange status.

Syntax

show ssh client status

Modes

Privileged EXEC mode

Examples

When SSH server is enabled:

```
device# show ssh client status
SSH client status: Enabled
```

History

Release version	Command history
18x.1.00	This command was introduced.

show ssh server status

Displays the current Secure Shell (SSH) server key-exchange status.

Syntax

show ssh server status

Modes

Privileged EXEC mode

Examples

When SSH server is enabled:

```
device# show ssh server status
SSH server status: Enabled
```

History

Release version	Command history
18x.1.00	This command was introduced.

show startup-config

Displays the contents of the startup configuration.

Syntax

show startup-config

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

Examples

The following example displays the contents of the startup configuration file.

```
device# show startup-config
```

History

Release version	Command history
18x.1.00	This command was introduced.

show startup-database

Displays the startup database information.

Syntax

show startup-database

Modes

Privileged EXEC mode

Usage Guidelines

Enter **show startup-database ?** to display the list of available database entries.

Examples

To display the logging configuration in the startup database:

```
device# show startup-db logging
logging raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
logging syslog-client localip CHASSIS_IP
```

History

Release version	Command history
18x.1.00	This command was introduced.

show statistics access-list

For an ACL type and inbound/outbound direction, displays ACL statistical information. You can show statistics for a specified ACL or only for that ACL on a specified interface. You can also display statistical information for all ACLs bound to a specified device interface, VLAN or VE. You can also display statistical information for IPv4 or IPv6 receive-path ACLs.

Syntax

show statistics access-list { **ip** | **ipv6** | **mac** } *name* { **in** | **out** }

show statistics access-list interface { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id* | **vlan** *vlan_id* } { **in** | **out** }

show statistics access-list { **ip** | **ipv6** } *name* **interface** [**ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id*] { **in** | **out** }

show statistics access-list mac *name* **interface** [**ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan_id*] { **in** | **out** }

show statistics access-list receive { **ip** | **ipv6** }

Parameters

interface
Filter by interface.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *index*
Specifies a port-channel interface.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface.

vlan *vlan_id*
Specifies a VLAN interface.

in | **out**
Specifies the ACL binding direction (incoming or outgoing).

ip | **ipv6** | **mac**
Specifies the network protocol.

overlay type vxlan
Not supported for this release.

uda
Not supported for this release.

name
Specifies the ACL name.

receive

Specifies IPv4 or IPv6 receive-path traffic.

Modes

Privileged EXEC mode

Usage Guidelines

Statistics are displayed only for rules that contain the **count** keyword.

When ACLs of multiple types are applied to an interface, for multiple matches the counter is incremented only for the higher priority match. Processing priority is as follows: rACLs > Layer 3 ACLs > Layer 2 ACLs.

Command Output

The **show statistics access-list** command displays the following information:

Output field	Description
Unaccountable	The counter resource is not allocated. This is typically seen if counting is not supported or if the hardware resources limit is reached.
Unwritten	The rule is inactive and is not programmed in the hardware. This is typically seen when the hardware resources limit is reached.

Examples

The following example displays inbound ACL statistics for a named IPv4 ACL.

```
device# show statistics access-list ip l3ext in
ip access-list l3ext Ethernet 0/8 in
seq 76 deny ip 10.10.75.10 0.0.0.0 any count log (795239 frames)
seq 77 hard-drop ip 10.10.75.10 0.0.0.0 10.10.11.0 0.0.0.255 count log (0 frames)
seq 78 hard-drop ip any 10.10.11.0 0.0.0.255 count log (0 frames)
seq 79 hard-drop ip any 10.10.0.0 0.0.255.255 count log (0 frames)
seq 80 hard-drop ip 10.10.75.10 0.0.0.0 any count log (0 frames)
seq 81 hard-drop ip 10.10.75.0 0.0.0.0 10.10.0.0 0.0.255.255 count log (0 frames)
seq 91 hard-drop ip any any count (0 frames)
seq 100 deny udp 10.10.75.0 0.0.0.255 10.10.76.0 0.0.0.255 count log (0 frames)
seq 1000 permit ip any any count log (0 frames)
```

The following example displays inbound ACL statistics for a specified interface. The ACL named ipv6-std-acl is applied on interface 0/1 to filter incoming routed traffic only.

```
device# show statistics access-list interface ethernet 0/1 in
ipv6 routed access-list ipv6-std-acl on Ethernet 0/1 at Ingress (From User)
    seq 10 permit host 0:1::1
    seq 20 deny 0:2::/64
    seq 30 deny any count (100 frames)
```

The following example displays inbound statistics for all ACLs bound to a specified VE interface.

```
device# show statistics access-list interface ve 3010 in
ipv6 access-list ip_acl_3 on Ve 3010 at Ingress (From User)
    seq 10 deny ipv6 2001:3010:131:35::/64 2001:1001:1234:1::/64 count (0 frames)
    seq 20 permit ipv6 2001:3010:131:35::/64 2001:3001:1234:1::/64
```

History

Release version	Command history
18x.1.00	This command was introduced.

show statistics bridge-domain

Displays statistics for logical interfaces in bridge domains.

Syntax

show statistics bridge-domain *bd-id*

Parameters

bd-id

The bridge domain ID.

Modes

Privileged EXEC mode

Usage Guidelines

Enter the **show statistics bridge-domain** *bd- id* command to view the statistics for a specific bridge domain.

Command Output

The **show statistics bridge-domain** command displays the following information:

Field	Description
Interface	The interface whose counter statistics are displayed.
RxPkts	The number of packets received at the specified interface.
RxBytes	The number of bytes received at the specified interface.
TxPkts	The number of packets transmitted from the specified interface.
TxBytes	The number of bytes transmitted from the specified interface.

Examples

The following example displays statistics for all logical interfaces in all bridge domains.

```
device# show statistics bridge-domain

Bridge Domain 1 Statistics
Interface                    RxPkts          RxBytes          TxPkts          TxBytes
eth 1/1.100       821729          821729          95940360        95940360
eth 1/21.200      884484          885855          95969584        95484555
po  1.300           8884            8855             9684            9955

Bridge Domain 20 Statistics
Interface                    RxPkts          RxBytes          TxPkts          TxBytes
eth 1/6.400       821729          821729          95940360        95940360
eth 1/21.100        8884            8855             9684            9955
po  2.40          884484          885855          95969584        95484555
```

The following example displays statistics for all logical interfaces in the bridge domain 1.

```
device# show statistics bridge-domain 1

Bridge Domain 1 Statistics
Interface                    RxPkts           RxBytes          TxPkts           TxBytes
eth 1/1.100       821729           821729           95940360         95940360
eth 1/21.200      884484           885855           95969584         95484555
po  1.300           8884             8855               9684             9955
```

History

Release version	Command history
18x.1.00	This command was introduced.

show statistics vlan

Displays the statistics for all ports and port channels on configured VLANs.

Syntax

show statistics vlan *vlan id*

Parameters

vlan ID

The specific VLAN ID.

Modes

Privileged EXEC mode

Usage Guidelines

Enter the **show statistics vlan** *vlan- id* command to view the statistics for all ports and port channels on a specific VLAN.

Command Output

The **show statistics vlan** command displays the following information:

Field	Description
Interface	The interface whose counter statistics are displayed.
RxPkts	The number of packets received at the specified port.
RxBytes	The number of bytes received at the specified port.
TxPkts	The number of packets transmitted from the specified port.
TxBytes	The number of bytes transmitted from the specified port.

Examples

The following example displays statistics for all ports and port channels on configured VLANs.

```
device# show statistics vlan

Vlan 10 Statistics
Interface     RxPkts          RxBytes          TxPkts          TxBytes
eth 1/1       821729          821729           95940360        95940360
eth 1/2       884484          885855           95969584        95484555
po  1        8884            8855              9684            9955

Vlan 20 Statistics
Interface     RxPkts          RxBytes          TxPkts          TxBytes
eth 1/6       821729          821729           95940360        95940360
eth 1/21     8884            8855              9684            9955
po  2      884484          885855          95969584        95484555
```

The following example displays statistics for all ports and port channels in the VLAN 10.

```
device# show statistics vlan 10

Vlan 10 Statistics
Interface     RxPkts          RxBytes          TxPkts          TxBytes
eth 1/1       821729          821729           95940360        95940360
eth 1/2       884484          885855           95969584        95484555
po  1        8884            8855              9684            9955
```

History

Release version	Command history
18x.1.00	This command was introduced.

show statistics vpn

Displays the VPN statistics for a VRF.

Syntax

show statistics vpn vrf *vrf-id*

Modes

Privileged EXEC mode

Command Output

The **show statistics vpn** command displays the following information:

Output field	Description
Tnl In-Pkt	Displays in packets.
Tnl Out-Pkt	Displays out packets.

Examples

This example displays the VPN statistic for a VRF.

```
device# show statistics vpn
Output:
VRF Name               Tnl In-Pkt      Tnl Out-Pkt
red                         0               0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show storm-control

Displays all BUM (broadcast, unknown unicast and multicast)-related information in the system.

Syntax

show storm-control [**broadcast** | **multicast** | **unknown-unicast**] [**interface ethernet** *slot/port*]

Parameters

storm-control
Displays all BUM-related information in the system.

broadcast
Displays all BUM-related information in the system for the broadcast traffic type.

multicast
Displays all BUM-related information in the system for the multicast traffic type.

unknown-unicast
Displays all BUM-related information in the system for the unknown-unicast traffic type.

interface ethernet *slot/port*
Displays all BUM-related information in the system for the specified interface.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display BUM storm-control-related configuration for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on a specified interface.

Examples

To display storm control information for broadcast traffic on an Ethernet interface:

```
device# show storm-control broadcast interface ethernet 2/1

Interface   Type            Rate (bps)   Conformed    Violated      Total
Et 2/1      broadcast       100000       12500000000  12500000000   25000000000
```

To display storm control information for all traffic on an Ethernet interface.

```
device# show storm-control interface ethernet 2/1

Interface   Type            Rate (bps)   Conformed   Violated    Total
Et 2/1      broadcast       100000       12500000000 12500000000 25000000000
Et 2/1      unknown-unicast 100000       12500000000 12500000000 25000000000
Et 2/1      multicast       100000       12500000000 12500000000 25000000000
```

To display storm control information for all traffic in the system:

```
device# show storm-control

Interface   Type             Rate (bps)   Conformed   Violated    Total
Et 2/1      broadcast        100000       12500000000 12500000000 25000000000

Et 2/1      unknown-unicast  100000       12500000000 12500000000 25000000000

Et 2/1      multicast        100000       12500000000 12500000000 25000000000

Et 2/2      broadcast        100000       12500000000 12500000000 25000000000

Et 2/3      broadcast        100000       12500000000 12500000000 25000000000

Et 2/4      unknown-unicast  100000       12500000000 12500000000 25000000000
```

To display storm control information for all broadcast traffic in the system:

```
device# show storm-control broadcast

Interface   Type             Rate (bps)   Conformed   Violated    Total
Et 2/1      broadcast        100000       12500000000 12500000000 25000000000
Et 2/2      broadcast        100000       12500000000 12500000000 25000000000
Et 2/3      broadcast        100000       12500000000 12500000000 25000000000
```

History

Release version	Command history
18x.1.00	This command was introduced.

show support

Displays a list of core files on the device.

Syntax

show support

Command Default

Displays information for the local device.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

Pagination is not supported with this command. Use the **More** option to display the output one page at a time.

Examples

To display the core files:

```
device# show support
 No core or FFDC data files found!
```

History

Release version	Command history
18x.1.00	This command was introduced.

show system monitor tm

Displays the system monitoring configuration for the Traffic Manager (TM) device deleted or discarded packets, or Virtual Output Queue (VOQ) discarded packets.

Syntax

show system monitor tm delete-packets | **discard-packets** | **discard-voq-packets**

Parameters

delete-packets
Displays the monitoring configuration of the TM device deleted packets.

discard-packets
Displays the monitoring configuration of the TM device discarded packets.

discard-voq-packets
Displays the monitoring configuration of the VOQ discarded packets.

Modes

Privileged EXEC

Command Output

The **show system monitor tm** command displays the following information:

Output field	Description
Logging-interval	Logging interval in minutes in which a RASlog message is generated.
Threshold	Threshold number of deleted or discarded packets. When the threshold is exceeded, a RASlog message is generated.

Examples

The following example displays the monitoring configuration of the VOQ discarded packets.

```
device# show system monitor tm discard-voq-packet
Discard VOQ packet count monitoring configuration:
Logging-interval :  60 minutes
Threshold        :  10 packets
```

History

Release version	Command history
18x.1.00	This command was introduced.

show telemetry collector name

Displays the status of the specified telemetry collector.

Syntax

show telemetry collector name { *collector_name* }

Parameters

collector_name

Specifies the name assigned to the telemetry collector profile.

Modes

Privileged EXEC mode

Command Output

The **show telemetry collector name** command displays the following information:

Output field	Description
Profiles Streamed	The name of the telemetry profile assigned to the collector.
Interval	The configured interval delay for the collector.
Uptime <DD/HH:MM:SS>	The current uptime for the collector.
Last Streamed	The last time the collector was executed.

Examples

The following example displays the status of a collector.

```
device# show telemetry collector name col1

Telemetry data is being streamed to  <col1>  on 10.24.12.96:8080

Profiles Streamed                     Interval  Uptime     Last Streamed
-----------------                     --------  ------     -------------------
default_interface_statistics          30 sec    0/0:12:52  2018-12-12 01:26:47
default_system_utilization_statistics 60 sec    0/0:12:52  2018-12-12 01:26:59
```

History

Release version	Command history
18x.1.00	This command was introduced.

show telemetry collector summary

Displays a summary of the telemetry collector configuration.

Syntax

show telemetry collector summary

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the status of the currently active telemetry collector sessions. These are initiated with collectors in the "activated" state.

Command Output

The **show telemetry collector summary** command displays the following information:

Output field	Description
Name	The collector name.
IP Address:Port	The IPv4 address and port assigned to the collector.
Streaming/Connection Status	The current status of the activated collector.

Examples

Example output of the collector configuration summary.

```
device# show telemetry collector status

Activated Collectors:
---------------------
Name                    IP Address:Port           Streaming/Connection Status
--------------------    ------------------       ---------------------------
Collector_3333          10.70.12.112:33333         starting_profiles
Collector_4444          10.70.12.112:44444         streaming
Collector_2345          10.70.12.112:33333         streaming_errored
```

History

Release version	Command history
18x.1.00	This command was introduced.

show telemetry server status

Displays the status of the telemetry server.

Syntax

show telemetry server status

Modes

Privileged EXEC mode

Command Output

The **show telemetry server status** command displays the following information:

Output field	Description
Clients	Clients of the telemetry server.
Profiles Streamed	The profiles assigned to the telemetry server
Interval	The configured interval delay for the telemetry server.
Connected Time	The time when the connection between the telemetry server and the client was established.
Last Streamed	The last time the telemetry profile was streamed.

Examples

Example of typical command output with no errors.

```
device# show telemetry server status
Telemetry Server running on port 50051, with transport as tcp

Clients                  Profile Streamed                       Interval  Connected Time    Last
Streamed
 --------------------    --------------------                   --------  --------------
-------------
ipv4:10.37.73.180:39056  default_system_utilization_statistics  70  2018-12-05 14:11:13 2018-12-05
14:17:10
ipv4:10.37.73.180:39062  default_interface_statistics           30  2018-12-05 14:17:25 2018-12-05
14:17:55
```

History

Release version	Command history
18x.1.00	This command was introduced.

show telnet server status

Displays the current Telnet server status.

Syntax

show telnet server status

Modes

Privileged EXEC mode

Examples

To display Telnet server status:

```
device# show telnet server status
VRF-Name: mgmt-vrf      Status: Enabled
VRF-Name: default-vrf   Status: Enabled
```

History

Release version	Command history
18x.1.00	This command was introduced.

show threshold monitor

Displays the current status of environmental thresholds and alerts for interfaces, security, and SFPs.

Syntax

show threshold monitor [**interface all area** | **security area** [**login-violation** | **telnet-violation**] | **sfp all area** [**current** | **rxp** | **temperature** | **txp** | **voltage**]

Parameters

interface all area
Displays status of interface thresholds and alerts.

security area
Displays status of security thresholds and alerts.

login-violation
Displays status of login violations.

telnet-violation
Displays status of Telnet violations.

sfp all area
Displays status of SFP thresholds and alerts.

current
Amount of current supplied to the SFP transceiver.

rxp
Amount of incoming laser power, in microWatts (µW).

temperature
Temperature of the SFP, in degrees Celsius.

txp
Amount of outgoing laser power, in microWatts (µW).

voltage
Amount of voltage supplied to the SFP.

Modes

Privileged EXEC mode

Examples

```
device# show threshold monitor sfp all area temperature
Interface                               Type            Area            Value           Status
Monitoring Status
-------------------------------------------------------------------------------------------------------
---------------
Eth 0/3                                 10GSR           Temperature     26 Centigrade   In Range
Monitoring
Eth 0/4                                 10GSR           Temperature     24 Centigrade   In Range
Monitoring
```

History

Release version	Command history
18x.1.00	This command was introduced.

show tm voq-stat ingress-device all discards

Displays a summary of the traffic management VOQ discard count for all towers.

Syntax

show tm voq-stat ingress-device all discards [**priority** *traffic_class*] [**max-display** *max_display_number*]

Parameters

priority *traffic_class*
: Displays discards for the specified traffic class priority. Enter an integer from 0 through 7.

max-display *max_display_number*
: Displays the specified maximum number of discard entries. Enter an integer from 1 through 32.

Modes

Privileged EXEC mode.

Usage Guidelines

The entries are sorted by the highest number of discards.

If you do not enter the **max-display** *max_display_number* option, a maximum of eight entries is displayed.

Examples

The following example displays the traffic management VOQ ingress discard statistics.

```
device# show tm voq-stat ingress-device all discards

---------------SLOT 3 TOWER 2-------------------
Dest Port   |  Prio  |  Queue  |    Discards
-----------------------------------------------
3/1         |   0    |   320   |     2473804
2/4         |   0    |   224   |     1867789
4/2         |   2    |   434   |     1023452
4/8         |   4    |   487   |      920349
1/2         |   1    |   120   |      858723
1/3         |   1    |   128   |       75328
2/5         |   0    |   260   |       22234
2/6         |   0    |   268   |        5248
```

The following example displays the traffic management VOQ ingress discard statistics for a specific traffic class priority.

```
device# show tm voq-stat ingress-device all discards priority 0

---------------SLOT 3 TOWER 2-------------------
Dest Port   |  Prio  |  Queue  |    Discards
-----------------------------------------------
3/1         |   0    |   320   |     2473804
2/4         |   0    |   224   |     1867789
2/5         |   0    |   260   |       22234
2/6         |   0    |   268   |        5248
```

History

Release version	Command history
18x.1.00	This command was introduced.

show tm voq-stat ingress-device all egress-port ethernet

Displays traffic management Virtual output queue (VOQ) statistics for all towers of an egress Ethernet interface.

Syntax

show tm voq-stat ingress-device all egress-port ethernet *slot/port* [**priority** *number*]

Parameters

slot/port

Specifies the slot and port of the interface.

priority *number*

Optionally specifies the traffic-class priority of the VOQ statistics. Enter an integer from 0 through 7. If you do not include this option, all priorities are displayed.

Modes

Privileged EXEC

Usage Guidelines

Command Output

The **show tm voq-stat ingress-device all egress-port ethernet** command displays the following information:

Output field	Description
Priority	Traffic-class priority number of the VOQ statistics.
EnQue Pkt Count	The count of all packets entering ingress queues on this traffic manager.
EnQue Bytes Count	The count of all bytes entering ingress queues on this traffic manager.
Total Discard Pkt Count	The count of all packets failing to enter ingress queues on this traffic manager.
Total Discard Bytes Count	The count of all bytes failing to enter ingress queues on this traffic manager.
Current Queue Depth	The current queue depth.
Maximum Queue Depth since Last read	The maximum queue depth since last access to read.

Examples

The following example displays the VOQ statistics for traffic-class priority 0 on Ethernet interface 1/4.

```
show tm voq-stat ingress-device all egress-port ethernet 1/4 priority 0

VOQ-Counters:
==================================================

Priority 0
------------------------------------------
EnQue Pkt Count                          0
EnQue Bytes Count                        0
Total Discard Pkt Count                  0
Total Discard Bytes Count                0
Current Queue Depth                      0
Maximum Queue Depth since Last read      0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show tm voq-stat ingress-device all max-buffer-util

Displays the traffic management VOQ maximum buffer size and utilization statistics for all towers.

Syntax

show tm voq-stat ingress-device all max-buffer-util

Modes

Privileged EXEC mode.

Examples

The following example displays the VOQ maximum buffer utilization statistics.

```
device# show tm voq-stat ingress-device all max-buffer-util

--------- Slot 1 Tower 1 ---------
  Max Buffer Size |  Max Buffer Util
-----------------------------------
       6007013804 |       96%
....
```

History

Release version	Command history
18x.1.00	This command was introduced.

show tm voq-stat ingress-device all max-queue-depth

Displays the traffic management VOQ max-queue-depth statistics for all towers.

Syntax

show tm voq-stat ingress-device all max-queue-depth [**max-display** *max_display_number*] [**min-threshold** *filter_number*] [**priority** *traffic_class*]

Parameters

max-display *max_display_number*
Specifies the maximum displayed entries. Enter an integer from 1 to 32.

min-threshold *filter_number*
Ignores the maximum queue depths below the specified min-threshold filter in bytes. Enter an integer from 1 through 1048640.

priority *traffic_class*
Displays only the specified traffic-class priority. Enter an integer from 0 through 7.

Modes

Privileged EXEC mode.

Usage Guidelines

The entries are sorted by the highest number of discards.

If you do not enter the **max-display** *max_display_number* option, a maximum of eight entries is displayed.

Examples

The following example displays the traffic management VOQ maximum queue depth statistics.

```
device# # show tm voq-stat ingress-device all max-queue-depth

------------------ Slot 1 Tower 1 --------------------
Dest Port   |  Prio  |  Queue  |   Max Depth  |  Max Util
-----------------------------------------------------------
3/1         |   0    |   320   |     1013804  |     96%
2/4         |   0    |   224   |      902789  |     86%
4/2         |   2    |   434   |      543440  |     51%
4/8         |   4    |   487   |      220349  |     21%
1/2         |   1    |   120   |      138723  |     13%
1/3         |   1    |   128   |       97328  |      9%
2/5         |   0    |   260   |       34234  |      3%
2/6         |   0    |   268   |       11723  |      1%

....
```

History

Release version	Command history
18x.1.00	This command was introduced.

show tm voq-stat ingress-device ethernet

Displays traffic management VOQ statistics for a specific ingress Ethernet interface.

Syntax

show tm voq-stat ingress-device ethernet *slot/port* { **discards** [**max-display** *max_display_number* | **priority** *traffic_class*] | **egress-port ethernet** *slot/port* [**priority** *traffic_class*] | **max-buffer-util** | **max-queue-depth** [**max-display** *max_display_number* | **min-threshold** *minimum_threshold* [**max-display** *max_display_number* | **priority** *traffic_class*] | **priority** *traffic_class*] }

Parameters

slot/port
The Ethernet slot and port

discards
Specifies discarded

max-display
Limits the display of discards.

max_display_number
The discard display limit. The values range from one to a maximum of 32.

priority
Displays discards by their traffic class priority.

traffic_class
Traffic class priorities range from 0 through 7.

egress-port *slot/port*
The outbound port.

max-buffer-util
Displays a summary of traffic management VOQ maximum buffer utilization.

max-queue-depth
Displays a summary of traffic management VOQ maximum queue depth statistics.

max-display
Limit the output to a maximum number of display entries

max_display_number
The output that the display is limited to. The range is from 1 to 64 entries.

min-threshold
Specifies that the results leave out **max-queue-depths** below the mimimum Byte threshold.

minimum_threshold
The mimum threshold filter value in bytes. Thew range is from 1 to 1048640.

Modes

Privileged EXEC mode.

Examples

Follow this example to display traffic management VOQ statistics for an egress interface.

```
device# show tm voq-stat ingress-device ethernet 2/1 egress-port ethernet 2/7 priority 2

VOQ-Counters:
==================================================

Priority 2
------------------------------------------
EnQue Pkt Count                          67404602
EnQue Bytes Count                        1768413221
Total Discard Pkt Count                  0
Total Discard Bytes Count                0
Current Queue Depth                      0
Maximum Queue Depth since Last read      160
```

Follow this example to display a summary of traffic management VOQ maximum queue depth statistics for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 max-queue-depth

------------------ Ports 1/1 - 1/36 --------------------
Dest Port   |  Prio  |  Queue  |   Max Depth  |  Max Util
-----------------------------------------------------------
3/1         |   0    |   320   |     1013804  |     96%
2/4         |   0    |   224   |      902789  |     86%
4/2         |   2    |   434   |      543440  |     51%
4/8         |   4    |   487   |      220349  |     21%
1/2         |   1    |   120   |      138723  |     13%
1/3         |   1    |   128   |       97328  |      9%
2/5         |   0    |   260   |       34234  |      3%
2/6         |   0    |   268   |       11723  |      1%
```

Follow this example to display a summary of traffic management VOQ maximum buffer utilization for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 max-buffer-util

--------- Ports 1/1 - 1/36 ---------
  Max Buffer Size |  Max Buffer Util
-----------------------------------
       6007013804 |       96%
```

Follow this example to display a summary of traffic management VOQ discards for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 discards

---------------- Ports 1/1 - 1/36 --------------------
Dest Port   |  Prio  |  Queue  |    Discards
-----------------------------------------------------
3/1         |   0    |   320   |     2473804
2/4         |   0    |   224   |     1867789
4/2         |   2    |   434   |     1023452
4/8         |   4    |   487   |      920349
1/2         |   1    |   120   |      858723
1/3         |   1    |   128   |       75328
2/5         |   0    |   260   |       22234
2/6         |   0    |   268   |        5248
```

History

Release version	Command history
18x.1.00	This command was introduced.

show tm voq-stat slot

Displays the traffic management VOQ statistics for a line card (LC) in a named slot.

Syntax

show tm voq-stat slot *slot_number* [**cpu-group** [*cpu_group_id* | **all**]

Parameters

slot_number
The LC slot.

cpu-group *cpu_group_id*
The ID number for the CPU group.

Modes

Privileged EXEC mode.

Examples

To display information about the VOQ for the LC in slot 1 CPU group 1 use the following command.

```
device# show tm voq-stat slot 1 cpu-group 1
CPU Group 1 Prio 0
    EnQue Pkt Count                                      100
    EnQue Bytes Count                                  22400
    Total Discard Pkt Count                        0
    Total Discard Bytes Count                      0
    Current Queue Depth                                0
    Maximum Queue Depth since last read         0

  CPU Group 1 Prio 1
    EnQue Pkt Count                                    100
    EnQue Bytes Count                                22400
    Total Discard Pkt Count                      0
    Total Discard Bytes Count                    0
    Current Queue Depth                              0
    Maximum Queue Depth since last read        0

  CPU Group 1 Prio 2
    EnQue Pkt Count                                    100
    EnQue Bytes Count                                22400
    Total Discard Pkt Count                      0
    Total Discard Bytes Count                    0
    Current Queue Depth                              0
    Maximum Queue Depth since last read        0

  CPU Group 1 Prio 3
    EnQue Pkt Count                                    100
    EnQue Bytes Count                                22400
    Total Discard Pkt Count                      0
    Total Discard Bytes Count                    0
    Current Queue Depth                              0
    Maximum Queue Depth since last read        0

  CPU Group 1 Prio 4
    EnQue Pkt Count                                    100
    EnQue Bytes Count                                22400
    Total Discard Pkt Count                      0
    Total Discard Bytes Count                    0
    Current Queue Depth                              0
    Maximum Queue Depth since last read        0

  CPU Group 1 Prio 5
    EnQue Pkt Count                                    100
    EnQue Bytes Count                                22400
    Total Discard Pkt Count                      0
    Total Discard Bytes Count                    0
    Current Queue Depth                              0
    Maximum Queue Depth since last read        0

  CPU Group 1 Prio 6
    EnQue Pkt Count                                    100
    EnQue Bytes Count                                22400
    Total Discard Pkt Count                      0
    Total Discard Bytes Count                    0
    Current Queue Depth                              0
    Maximum Queue Depth since last read        0

  CPU Group 1 Prio 7
    EnQue Pkt Count                                    100
    EnQue Bytes Count                                22400
    Total Discard Pkt Count                      0
    Total Discard Bytes Count                    0
    Current Queue Depth                              0
    Maximum Queue Depth since last read        0
```

History

Release version	Command history
18x.1.00	This command was introduced.

show topology-group

Displays topology group information.

Syntax

show topology-group [*group-id*]

Parameters

group-id

Displays the information of the topology group of the specified ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

Command Output

The **show topology-group** command displays the following information:

Output field	Description
master-vlan	The master VLAN for the topology group. The settings for STP, MRP, or VSRP on the control ports in the master VLAN apply to all control ports in the member VLANs within the topology group.
member-vlan	The member VLANs in the topology group.
Common control ports	The master VLAN ports that are configured with Layer 2 protocol information. The Layer 2 protocol configuration and state of these ports in the master VLAN applies to the same port numbers in all the member VLANs.
Per vlan free ports	The ports that are not controlled by the Layer 2 protocol information in the master VLAN.

Examples

The following example displays the topology group information.

```
device# show topology-group
Topology Group 3
================
master-vlan 2
member-vlan none
Common control ports       L2 protocol
ethernet 1/1/1             MRP
ethernet 1/1/2             MRP
ethernet 1/1/5             VSRP
ethernet 1/2/22            VSRP
Per vlan free ports
ethernet 1/2/3             Vlan 2
ethernet 1/1/4             Vlan 2
ethernet 1/2/11            Vlan 2
ethernet 1/2/12            Vlan 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

show tunnel

Displays information pertaining to a tunnel interface.

Syntax

show tunnel *tunnel-id*

Parameters

tunnel-id

Specifies the tunnel ID.

Modes

Privileged EXEC Mode

Examples

This example displays tunnel information.

```
device# show tunnel 10
Tunnel 10, mode GRE
Ifindex 0x7c40000a, Admin state up, Oper state up
Source IP 14.101.0.4, Vrf default-vrf
Destination IP 15.10.0.3
Tunnel IP Interface : Ve 501 up
Tunnel TTL 255      Tunnel DSCP 0
Tunnel QosMode PIPE
Keepalive Interval 10000  RetryCount 3 TimeRemaining 27861 msecs
GRE Keep Alive : RX 62      TX 62

Active next hops:
    IP: 13.10.0.3, Vrf: default-vrf
    Egress L3 port: Ve 10, Outer SMAC: 609c.9f0d.4a14
    Outer DMAC: 001b.ed9f.1700
    Egress L2 Port: Unknown, Outer ctag: 0, stag:0, Egress mode: Local
    BUM forwarder: no
```

History

Release version	Command history
18x.1.00	This command was introduced.

show tunnel statistics

Displays tunnel statistics.

Syntax

show tunnel statistics *tunnel-Id* **mode** [**gre**]

Parameters

tunnel-Id

Filters by the tunnel ID.

mode

FIlters by tunnel mode.

gre

Specifies GRE tunnels.

Modes

Privileged EXEC Mode

Examples

This example displays tunnel statistics filtered by the tunnel ID.

```
device# show tunnel statistics 11
Tnl ID   RX packets      TX packets      RX bytes        TX bytes
======== =============== =============== =============== ================
11       0               10               (NA)            640
```

This example displays tunnel statistics filtered by tunnel mode.

```
device# show tunnel statistics mode gre
Tnl ID   RX packets      TX packets      RX bytes        TX bytes
======== =============== =============== =============== ================
10       0               10               (NA)            640
11       0               20               (NA)            1280
12       0               50               (NA)            22000
```

History

Release version	Command history
18x.1.00	This command was introduced.

show users

Displays the users logged in to the system and locked user accounts.

Syntax

show users

Modes

Privileged EXEC mode

Examples

The following example displays active user sessions and locked user accounts.

```
device# show users
**USER SESSIONS**
Username    Role    Host IP       Device    Time Logged In
jsmith      user    192.0.2.0     Cli       2016-04-30 01:59:35
jdoe        admin   192.0.2.1     Cli       2016-05-30 01:57:41

**LOCKED USERS**
testUser
```

History

Release version	Command history
18x.1.00	This command was introduced.

show version

Displays the current firmware version.

Syntax

show version [**all-partitions**] [**brief**]

Parameters

all-partitions

Displays firmware information for both the active and the standby partitions. For each module, both partitions are displayed.

brief

Displays a brief version of the firmware information.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display firmware version information and build dates. The default command output includes the following information:

- Network Operating System Version—The firmware version number
- Firmware name—The label of the firmware image
- Build Time—The build date and time of the firmware
- Install time—The date and time of the firmware installation
- Host Version—The Linux host version.
- Host Kernel—The Linux kernel version
- Control Processor—The control processor model and memory

Examples

To display the firmware version:

```
SLX# sh version
SLX-OS Operating System Version: 18x.1.00
Copyright (c) 1995-2018 Extreme Networks.
Firmware name:     18x.1.00d
Build Time:        20:07:43 Apr 30, 2018
Install Time:      20:14:49 Apr 30, 2018
Kernel:            2.6.34.6
Control Processor: GenuineIntel
System Uptime:   1days 16hrs 34mins 0secs
Name     Primary/Secondary Versions
----------------------------------------
SLX-OS   18x.1.00d
         18x.1.00d
```

History

Release version	Command history
18x.1.00	This command was introduced.

show vlan brief

Displays basic information about the VLAN interfaces on the device. You can also filter to display only provisioned or unprovisioned VLANs.

Syntax

show vlan brief [**provisioned** | **unprovisioned**]

Parameters

provisioned
Displays provisioned VLANs.

unprovisioned
Displays unprovisioned VLANs.

Modes

Privileged EXEC mode

Command Output

The **show vlan brief** command displays the following information:

Output field	Description
VLAN	Displays the *vlan_ID*.
Name	Displays one of the following strings: • "default" • A name assigned to the VLAN using the **name** command • A default name automatically assigned to the VLAN, composed of "VLAN" and the *vlan_ID*. For example, if the *vlan_ID* is 1000, the default name is VLAN1000.
State	Displays "ACTIVE" for provisioned VLANs or "INACTIVE" for unprovisioned VLANs.
Config status	Displays the configuration status for the VLANs.
Ports	Displays the ports on which the VLAN is applied.
Classification	(Available only for provisioned).

Examples

The following example displays the status all VLANs including endpoint tracking and MVRP VLANs.

```
device# show vlan brief
Total Number of VLANs configured    : 4
VLAN             Name            State                       Config status         Ports
Classification
                                                                                   (u)-Untagged
                                                                                   (t)-Tagged
================ =============== =========================== ===================== ===============
====================
1                default         ACTIVE                      Static                Eth 1/5(t)
                                                                                   Po 60(t)

10               VLAN0010        ACTIVE                      Static                Eth 1/5(t)

100              VLAN0100        ACTIVE                      Dynamic (MVRP)        Po 60(t)

1000             VLAN1000        ACTIVE                      Dynamic (EP tracking) Po 60(t)
```

History

Release version	Command history
18x.1.00	This command was introduced.

show vlan detail

Displays detailed information on statically configured as well as dynamically created VLANs by EP-tracking or MVRP including the configuration status of each Ethernet or port-channel interface specifying if it was statically added or dynamically learned by EP-tracking or MVRP.

Syntax

show vlan detail

Modes

Privileged EXEC mode

Examples

The following example displays detailed VLAN information.

```
device# show vlan det
VLAN: 1, Name: default
Admin state: ACTIVE, Config status: Static
Number of interfaces: 7
      Eth 0/4, tagged, Static
      Eth 0/3, tagged, Static
      Eth 0/2, tagged, Static
      Eth 0/8, tagged, Static
      Eth 0/6, tagged, Static
      Eth 0/9, untagged, Static
      Po 20, tagged, Static
VLAN: 10, Name: VLAN0010
Admin state: ACTIVE, Config status: Static
Number of interfaces: 3
      Eth 0/3, tagged, Static
      Eth 0/2, tagged, Static
      Eth 0/4, tagged, Static
      Po 20, tagged, Static
VLAN: 11, Name: VLAN0011
Admin state: ACTIVE, Config status: Static
Number of interfaces: 3
      Eth 0/3, tagged, Static
      Eth 0/2, tagged, Static
      Eth 0/4, tagged, Dynamic (MVRP)
VLAN: 12, Name: VLAN0012
Admin state: ACTIVE, Config status: Dynamic (MVRP)
Number of interfaces: 1
      Eth 0/4, tagged, Dynamic (MVRP)
VLAN: 13, Name: VLAN0013
Admin state: ACTIVE, Config status: Dynamic (EP tracking)
Number of interfaces: 1
      Eth 0/6, tagged, Dynamic (EP tracking)
VLAN: 14, Name: VLAN0014
Admin state: INACTIVE(member port down), Config status: Static
Number of interfaces: 1
      Eth 0/8, tagged, Static
```

History

Release version	Command history
18x.1.00	This command was introduced.

show vrf

Displays Virtual Routing and Forwarding (VRF) configuration information.

Syntax

show vrf [*vrf-name* | **detail** | **interface** *interface*]]

Parameters

vrf-name

Specifies a named VRF. For the default VRF, enter **default-vrf**.

detail

Displays detailed information for all VRFs configured.

interface *interface*

Displays VRF information for an interface.

Modes

Privileged EXEC mode

Examples

The following example displays basic information for the default VRF.

```
device# show vrf default-vrf
VRF-Name: default-vrf, VRF-Id: 1
IP Router-Id: 50.50.50.1
Interfaces:
               Ve 40, Ve 84, Ve 85, Ve 150, Ve 211,
               Ve 501, Ve 503, Ve 504, Ve 505, Ve 1025,
               Ve 1059, Ve 2000, Lo 50
Address-family IPV4 unicast
               Max routes: -   Route count:134
   No import route-maps
   No export route-maps

Address-family IPV6 unicast
               Max routes: -   Route count:51
   No import route-maps
   No Export route-maps
```

The following example displays basic information for all VRFs.

```
device# show vrf
Total number of VRFs configured: 4
VrfName                          VrfId  V4-Ucast  V6-Ucast
blue                             3      Enabled     -
default-vrf                      1      Enabled   Enabled
mgmt-vrf                         0      Enabled   Enabled
red                              2        -       Enabled
```

The following example displays detailed information for all VRFs.

```
device# show vrf detail
Total number of VRFs configured: 4

VRF-Name: blue, VRF-Id: 3
IP Router-Id: 10.1.1.10
Interfaces:
    Ve 200
Address-family IPV4 unicast
    Max routes:-   Route count:134
   No import route-maps
   No export route-maps

VRF-Name: default-vrf, VRF-Id: 1
IP Router-Id: 30.1.1.1
Interfaces:
    Ve 300
Address-family IPV4 unicast
    Max routes:-   Route count:51
   No import route-maps
   No export route-maps

Address-family IPV6 unicast
    Max routes:-   Route count:2
   No import route-maps
   No Export route-maps

VRF-Name: mgmt-vrf, VRF-Id: 0
IP Router-Id: 0.0.0.0
Interfaces:
    mgmt 1, Null0
Address-family IPV4 unicast
    Max routes:-   Route count:3
   No import route-maps
   No export route-maps

Address-family IPV6 unicast
    Max routes:-   Route count:2
   No import route-maps
   No Export route-maps

VRF-Name: red, VRF-Id: 2
IP Router-Id: 0.0.0.0
Interfaces:
        Ve 100
Address-family IPV6 unicast
    Max routes:-   Route count:2
   No import route-maps
   No Export route-maps
```

The following example indicates which VRFs are available on which interfaces.

```
device# show vrf interface
VrfName                         Interfaces
blue                            Ve 200
default-vrf                     Ve 300
mgmt-vrf                        mgmt 1, Null0
red                             Ve 100
```

History

Release version	Command history
18x.1.00	This command was introduced.

show vrrp

Displays information about IPv4 VRRP and VRRP-E sessions.

Syntax

show vrrp

show vrrp *VRID* [**detail** | **summary**]

show vrrp detail

show vrrp interface { **ethernet** *slot*/*port* | **ve** *vlan_id* } [**detail** | **summary**]

show vrrp summary [**vrf** { *vrf-name* | **all** }]

Parameters

VRID
The virtual group ID about which to display information. The range is from 1 through 16.

detail
Displays all session information in detail, including session statistics.

summary
Displays session-information summaries.

interface
Displays information for an interface that you specify.

ethernet *slot port*
Specifies a valid, physical Ethernet interface with a slot and port number.

ve *vlan_id*
Specifies the VE VLAN number.

vrf
Specifies a VRF instance or all VRFs.

vrf-name
Specifies a VRF instance. For the default vrf, enter **default-vrf**.

all
Specifies all VRFs.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about VRRP and VRRP-E sessions, either in summary or full-detail format. You can also specify a particular virtual group ID or interface for which to display output.

This command is for VRRP and VRRP-E. VRRP-E supports only the VE interface type.

To display information for VRRP sessions using the default VRF, you can use the **show vrrp summary** command syntax (with no additional parameters).

For the default or a named VRF, you can use the **show vrrp summary vrf** command syntax with the *vrf-name* option.

To display information for all VRFs, use the **show vrrp summary vrf all** command.

Examples

The following example shows all VRRP session information in detail, including session statistics.

```
device# show vrrp detail

Total number of VRRP session(s)   : 2

VRID 14
  Interface: Ve 2018;  Ifindex: 1207961570
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 10.18.1.100
  Virtual MAC Address: 0000.5e00.0112
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========

  Global Statistics:
  ==================
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0

  Session Statistics:
  ===================
    Advertisements             : Rx: 0, Tx: 49
    Gratuitous ARP             : Tx: 1
    Session becoming master    : 1
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0

VRID 15
  Interface: Ve 2019;  Ifindex: 1207961571
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 10.19.1.100
  Virtual MAC Address: 0000.5e00.0113
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========

  Global Statistics:
  ==================
```

```
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0

  Session Statistics:
  ===================
    Advertisements             : Rx: 0, Tx: 81
    Gratuitous ARP             : Tx: 1
    Session becoming master    : 1
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0
```

The following example displays summary information for VRRP statistics on the VRF named Marketing.

```
device# show vrrp summary vrf Marketing

Total number of VRRP session(s)   : 1
Master session count  : 1
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
14    VRRP     Ve 2018    Enabled   100     Master
```

The following example displays summary information for VRRP statistics on all VRFs.

```
device# show vrrp summary vrf all

Total number of VRRP session(s)   : 2
Master session count  : 2
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface   Admin   Current   State    Short-path  Revert    SPF
                           State   Priority           Forwarding  Priority  Reverted
====  =======  =========   =====   ========  =====    ==========  ========  ========
14    VRRP     Ve 2018     Enabled 100       Master
15    VRRP     Ve 2019     Enabled 100       Master
```

The following example displays summary information for VRRP statistics on the default VRF. (This command is equivalent to **show vrrp summary**.)

```
device# show vrrp summary vrf default-vrf

Total number of VRRP session(s)   : 1
Master session count  : 1
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
15    VRRP     Ve 2019    Enabled 100       Master
```

The following example displays information for VRRP-E tracked networks.

```
device# show vrrp detail

Total number of VRRP session(s)   : 1

VRID 3
  Interface: Ve 100;  Ifindex: 1207959652
  Mode: VRRPE
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 10.1.1.100
  Virtual MAC Address: 02e0.523d.750a
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: DISABLE  (default: DISABLED)
  Advertise-backup: DISABLE  (default: DISABLED)
  Backup Advertisement interval: 60 sec  (default: 60 sec)
  Short-path-forwarding: Disabled
  Revert-Priority: unset; SPF Reverted: No
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========

  Tracknetwork:
    Network(s)                Priority  Status
    =========                 ========  ==========
    10.20.1.0/24              50        Up

  Global Statistics:
  ==================
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0

  Session Statistics:
  ===================
    Advertisements             : Rx: 0, Tx: 35
    Neighbor Advertisements           : Tx: 19
    Session becoming master    : 1
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0
    VRRPE backup advt sent     : 0
    VRRPE backup advt recvd    : 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

Commands Shu - Z

shutdown (interface)

Disables the current interface.

Syntax

shutdown

no shutdown

Command Default

The interface is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no shutdown** to enable the interface.

If you use in-band management only, you may choose to shut down the management interface (which is considered out of band). When the management interface is shut down, all services (such as ping, scp, telnet, ssh, snmp, firmwaredownload, and supportsave) through the management interface IP. Management interface shutdown is a persistent configuration, meaning that the interface remains down after a system reboot or failover.

Examples

The following example disables an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# shutdown
```

The following example enables an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# no shutdown
```

The following example disables a port-channel interface.

```
device# configure terminal
device(config)# interface port-channel 20
device(config-Port-channel-20)# shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

shutdown (LIF)

Removes a physical or port-channel interface on an edge port from participating in logical interface (LIF) data traffic without the need to shut down the interface.

Syntax

shutdown

no shutdown

Command Default

The LIF service instance is not shut down.

Modes

LIF configuration mode on a physical port or port-channel

Usage Guidelines

Use the **no** form of this command to restore the service instance status to the default.

Examples

The following example removes a service instance on an Ethernet port from participating in data traffic.

```
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# logical-interface ethernet 2/6.120
device(conf-if-eth-lif-2/6.120)# shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

shutdown-time

Specifies a shutdown time for loopback detection (LD).

Syntax

shutdown-time { *minutes* }

no shutdown-time

Command Default

See the Usage Guidelines.

Parameters

minutes

Shutdown time in minutes. Range is from 0 through 1440. The default is 0.

Modes

Protocol Loop Detection configuration mode

Usage Guidelines

By default the shutdown time is 0, which means that an LD-disabled logical interface (LIF) is never auto-enabled.

If the shutdown time is configured with a nonzero value, the LD-disabled LIF is auto-enabled following the specified shutdown time.

Use the **no** form of this command to revert to the default interval.

Examples

To specify a shutdown time of 20 minutes:

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# shutdown-time 1
2017/10/20-16:04:48, [ELD-1005], 3749, M2 | Active | DCE, INFO, SLX, Loop is detected on Ethernet 2/2 VLAN 20,
the LIF (logical interface) is shutdown.
2017/10/20-16:05:46, [ELD-1007], 3750, M2 | Active | DCE, INFO, SLX, Loop detection disabled LIF (Logical
interface) on Ethernet 2/2 VLAN 20 is auto-enabled.
```

To revert to the default interval:

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# no shutdown-time
```

History

Release version	Command history
18r.1.00	This command was introduced.

site

Creates a remote Layer 2 extension site in a VXLAN overlay gateway context and accesses site configuration mode.

Syntax

site *name*

no site *name*

Parameters

name

Site identifier. An ASCII character string up to 63 characters long, including the alphabet, numbers 0 through 9, hyphens (-), and underscores (_).

Modes

Overlay gateway configuration mode

Usage Guidelines

The VXLAN overlay gateway type must first be configured for Layer 2 extension, by means of the **type layer2-extension** command.

A site represents a remote fabric or the other end of the VXLAN tunnel. A site is associated with a "container," as data structure that includes the destination IPv4 address of the tunnel, the switchport VLANs, bridge domain, and the administrative state.

Use the **no site** command with a specified name to remove the tunnel that corresponds to the site.One you create the site instance, you enter VXLAN overlay gateway site configuration mode, where you can configure other properties for the site. The key commands available in this mode are summarized below:

TABLE 5 Key commands available in VXLAN overlay gateway site configuration mode

Command	Description
bfd	Configures Bidirectional Forwarding Detection (BFD) on a tunnel in VXLAN overlay gateway configurations.
bfd interval	Configures BFD session parameters on a tunnel in VXLAN overlay gateway configurations.
extend bridge-domain	Configures a bridge domain for the tunnels to the containing site in a VXLAN overlay gateway configurations.
extend vlan	Configures switchport VLANs for the tunnels to the containing site in a VXLAN overlay gateway configurations.
ip address	Specifies the IPv4 address of a destination tunnel in VXLAN overlay gateway configurations.
shutdown	Administratively shuts down tunnels to a VXLAN overlay gateway site.

Examples

The following example creates a VXLAN overlay gateway site and enters site configuration mode.

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# site mysite
switch(config-site-mysite)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server community

Sets the community string and associates it with the user-defined group name to restrict the access of MIB for SNMPv1 and SNMPv2c requests.

Syntax

snmp-server community *string* [**group** *group-name*]

no snmp-server community *string* [**group** *group-name*]

Command Default

None

Parameters

string
Specifies the community name string. Enter an alphanumeric string with 2 to 16 characters.

group *group-name*
Specifies the group name associated with the community name.

Modes

Global configuration mode

Usage Guidelines

Use a **no** form of this command to remove an community string or the group from the community.

The maximum number of SNMP communities supported is 256.

Examples

The following example adds the community string named public and associates the group name named user with it.

```
device(config)# snmp-server community public groupname user
```

History

Release version	Command history
18x. 1.00	This command was introduced.

snmp-server contact

Sets the SNMP server contact string.

Syntax

snmp-server contact *string*

no snmp-server contact

Command Default

The default contact string is "Operator 12345".

Parameters

string

Specifies the server contact. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to reset the default value.

Examples

The following example sets the SNMP server contact string to "Operator 12345".

```
device(config)# snmp-server contact "Operator 12345"
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server context

Maps the context name in an SNMPv3 packet protocol data unit (PDU) to the name of a VPN routing and forwarding (VRF) instance.

Syntax

snmp-server context *context_name* [**vrf-name** *vrf_name*]

no snmp-server context *context_name* [**vrf-name** *vrf_name*]

Command Default

None

Parameters

context_name
Specifies the context name that is passed in the SNMP PDU.

vrf-name *vrf_name*
Specifies the VRF instance that can be retrieved when an SNMP request is sent with the context name.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to delete the SNMP server context.

For SNMPv1 and SNMPv2, you must map the context with the community string. The SNMP agent supports 256 contexts to support context-to-VRF mapping.

For SNMPv3, you only need to map the context with the VRF. The SNMPv3 request PDU itself provisions for the context. Only one context is allowed for each VRF instance.

ATTENTION
SNMP SET requests work only on the default VRF.

Examples

The following example configures an SNMP server context to a VRF for SNMPv1 or SNMPv2.

```
device# configure terminal
device(config)# snmp-server community public groupname admin
device(config)# snmp-server context mycontext vrf myvrf
device(config)# snmp-server mib community-map public context mycontext
```

The following example configures an SNMP server context to a VRF for SNMPv3.

```
device# configure terminal
device(config)# snmp-server context mycontext1 vrf myvrf1
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server enable trap

Enables the SNMP traps.

Syntax

snmp-server enable trap

no snmp-server enable trap

Command Default

The SNMP server traps are enabled by default.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to disable the SNMP traps.

Examples

The following example disables the SNMP traps.

```
device# configure terminal
device(config)# no snmp-server enable trap
```

The following example enables the SNMP traps.

```
device# configure terminal
device(config)# snmp-server enable trap
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server engineid local

Configures an SNMP engine ID for the SNMP agent.

Syntax

snmp-server engineid local *engine_id*

no snmp-server engineid local

Command Default

A default engine ID is generated during system start up.

Modes

Global configuration mode

Usage Guidelines

A reboot is necessary for the configured engine ID to become active.

Use the **no** form of the command to remove the configured engine ID from database.

Examples

The following example configures an engine ID for the SNMP agent.

```
device(config)# snmp-server engineid local 10:00:00:05:33:51:A8:65:05:33:51:A8
```

The following example removes the configured engine ID from the database.

```
device(config)# no snmp-server engineid local
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server group

Creates user-defined groups for SNMPv1/v2/v3 and configures read, write, and notify permissions to access the MIB view.

Syntax

snmp-server group *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *viewname*] [**write** *viewname*] [**notify** *viewname*]

no snmp-server group *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *viewname*] [**write** *viewname*] [**notify** *viewname*]

Command Default

None

Parameters

groupname
Specifies the name of the SNMP group to be created.

v1 | **v2c** | **v3**
Specifies the version of SNMP.

auth | **noauth** | **priv**
Specifies the various security levels for SNMPv3.

auth
Specifies the authNoPriv security level. Password authentication is used based on either MD5 or SHA hash authentication and no encryption is used for communications between the devices.

noauth
Specifies the noAuthNoPriv security level. If no security level is specified, noauth is the default. This security level means that there is no authentication password exchanged and the communications between the agent and the server are not encrypted. The SNMP requests are authorized based on a username string match similar to the community string for SNMPv1/v2c.

priv
Specifies the authPriv security level. Password authentication is used based on either MD5 or SHA hash authentication and the communication between the agent and the server are also encrypted.

read *viewname*
Specifies the name of the view that enables you to provide read access.

write *viewname*
Specifies the name of the view that enables you to provide both read and write access.

notify *viewname*
Specifies the name of the view that enables you to provide access to the MIB for trap or inform.

Modes

Global configuration mode

Usage Guidelines

Maximum number of SNMP groups supported is 10.

Examples

The following example creates SNMP server group entries for SNMPv3 user group with auth or noauth permission.

```
device(config)# snmp-server group group1 v3 auth read myview write myview notify myview
device(config)# snmp-server group group2 v3 noauth read all write all notify all
device(config)# snmp-server group group3 v3 auth
```

The following example removes the configured SNMP server groups.

```
device(config)# no snmp-server group test1 v3 auth
device(config)# no snmp-server group TEST1 v3 auth read myview write myview
device(config)# no snmp-server group TEST2 v3 noauth read all write all notify all
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server host

Configures the SNMP trap server host attributes.

Parameters

host { **ipv4_host** | **ipv6_host** | **dns_host** }
Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

community_string
Specifies the community string associated with the host entry. The number of characters available for the string ranges from 1 through 64.

version { **1** | **2c** }
Selects version 1 or 2c traps to be sent to the specified trap host.

udp-port *port*
Specifies the UDP port where SNMP traps will be received. Valid port IDs range from 0 through 65535. The default port is 162.

severity-level { **none** | **debug** | **info** | **warning** | **error** | **critical** }
Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASLog (swEvent) traps can be filtered based on severity level. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of **none** is specified, all traps are filtered and no RASLog traps are received.

use-vrf *vrf-name*
Specifies a VRF though which to communicate with the SNMP host. By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Modes

Global configuration mode

Usage Guidelines

This command sets the trap destination IP addresses and SNMP version, associates a community string with a trap host community string (for v1 and v2c), and specifies the UDP destination port where SNMP traps will be received.

To configure SNMP trap hosts associated with community strings, you must create the community string using the **snmp-server community** command before configuring the host.

The host supports six communities and their associated trap recipients and trap recipient severity levels. The default value for the trap recipient of each community is 0.0.0.0. The length of the community string should be between 2 and 64 characters.

The **no snmp-server host** *host* **community-string** *string* **version 2c** command brings version 2c down to version 1.

The **no snmp-server host** *host* **community-string** *string* command removes the SNMP server host from the device configuration altogether.

Examples

The following example creates an entry for trap host 1050:0:0:0:5:600:300c:326b associated with community “public.” The trap host receives traps from the configured device.

```
device(config)# snmp-server host 1050:0:0:0:5:600:300c:326b public severity-level Info
```

The following example creates an entry for trap host brcd.extremenetworks.com associated with community “public.” The trap host receives traps from the configured device.

```
device(config)# snmp-server host brcd1.extremenetworks.com public severity-level info
```

The following example associates “commaccess” as a read-only community and set 10.32.147.6 as a trap recipient with SNMP version 2c on target port 162.

```
device(config)# snmp-server host 10.32.147.6 commaccess version 2c udp-port 162
```

The following example creates a trap host (10.23.23.45) associated with the community “public”, which will receive all traps with the severity level of Info.

```
device(config)# snmp-server host 10.23.23.45 public severity-level info
```

The following example resets the severity level to None.

```
device(config)# snmp-server host 10.23.23.45 public severity-level none
```

The following example specifies a VRF to communicate with the host.

```
device(config)# snmp-server host 10.24.61.10 public use-vrf myvrf
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server location

Sets the SNMP server location string.

Syntax

snmp-server location *string*

no snmp-server location

Command Default

The default location string is "Building 3 Room 214".

Parameters

location *string*

Specifies the SNMP server location string. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to reset the default value.

Examples

The following example sets the SNMP server location string to "Building 3 Room 214".

```
device(config)# snmp-server location "Building 3 Room 214"
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server mib community-map

Maps an SNMP community string to an SNMP context.

Syntax

snmp-server mib community-map *community-name* **context** *context-name*

no snmp-server mib community-map *community-name* **context** *context-name*

Command Default

None

Parameters

community-name
Specifies an SNMP community name.

context *context-name*
Specifies an SNMP context.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove a community string and its associated context name.

Any incoming SNMPv1/v2c requests with the specified community name uses the context name specified by this command. The context name can be used in SNMP requests for "ipCidrRouteTable."One community can be mapped to only one context. However, a single context can be mapped to multiple communities.

Before mapping the community to context, a valid context should be configured by using the **snmp-server context** command and a valid community string should be configured by using the **snmp-server community** command.

Examples

The following example maps an SNMP community string to a context name.

```
device# configure terminal
device(config)# snmp-server mib community-map public context mycontext
```

The following example removes an SNMP community string and its associated context name.

```
device(config)# no snmp-server mib community-map public context mycontext
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server sys-descr

Sets the Management Information Base (MIB-2) object identifier (OID) system description.

Syntax

snmp-server sys-descr *string*

no snmp-server sys-descr

Command Default

The system description is "Extreme BR-SLX9850-4 Router".

Parameters

string

The text for the system description. The string must be between 4 and 255 characters in length.

Modes

Global configuration mode

Usage Guidelines

Enter **no snmp-server sys-descr** to return to the default system description.

Examples

To set the system description OID to "Extreme BR-SLX9850-4 Router, use:

```
device(config)# snmp-server sys-descr "Extreme BR-SLX9850-4 Router"
```

To restore the system description OID to the default:

```
device(config)# no snmp-server sys-descr
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server user

Creates or changes the attributes of SNMPv3 users, and allows the SNMPv3 user to be associated with the user-defined group name.

Command Default

None

Parameters

username
The name of the user that connects to the agent. The name must be between 1 and 16 characters long.

groupname *group-name*
The name of the group to which the user is associated. The configured user is allowed to be associated with the user-defined groups created using the **snmp-server group** command.

auth
Initiates an authentication level setting session. The default level is **noauth** .

noauth
Specifies "No Authentication Protocol".

md5
The HMAC-MD5-96 authentication level.

sha
The HMAC-SHA-96 authentication level.

auth-password *string*
A string that enables the agent to receive packets from the host. Passwords are plain text and must be added each time for each configuration replay. The password must be between 1 and 32 characters long.

priv
Initiates a privacy authentication level setting session. The default level is **nopriv** .

DES
Specifies the DES privacy protocol.

AES128
Specifies the AES128 privacy protocol.

nopriv
Specifies "No Privacy Protocol".

priv-password *string*
Specifies a string (not to exceed 32 characters) that enables the host to encrypt the contents of the message that it sends to the agent. Passwords are plain text and must be added each time for each configuration replay. The privacy password alone cannot be configured. You configure the privacy password with the authentication password.

encrypted
Encrypts the input for auth/priv passwords. The encrypted key should be used only while entering the encrypted auth/priv passwords.

Modes

Global configuration mode

Usage Guidelines

This command configures SNMPv3 users that can be associated with a trap and inform response functionality. This command also allows configured user to be associated with user-defined SNMP groups created using the **snmp-server group** command. The maximum number of SNMP users that can be configured is 10. Optional encryption for **auth-password** and **priv-password** is also provided.

When creating a new SNMPv3 user without group name, by default there is no group name mapped with the SNMPv3 user. You must map the configured SNMPv3 user with any non-existing or existing group name available in the group CLI configuration to contact the device through SNMPv3.

This command may not be successful where encrypted passwords are generated by third-party or open-source tools.

Use a **no** form of this command to do one of more of the following:

- Remove the specified user and all entities associated with it
- Remove the groupname from the user

Examples

The following example configures a basic authentication policy.

```
device(config)# snmp-server user extreme groupname snmpadmin auth md5 auth-password user123 priv AES128
priv-password user456
```

The following example configures plain-text passwords.

```
device(config)# snmp-server user snmpadmin1 auth md5 auth-password private123 priv  DES priv-password
public123
```

The following example configures configure encrypted passwords.

```
device(config)# snmp-server user snmpadmin2 groupname snmpadmin auth md5 auth-password "MVb
+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted
```

The following example creates the SNMP users "user1" and "user2" associated with used-defined group "group1" under global configuration mode.

```
device(config)# snmp-server user user1 groupname group1
device(config)# snmp-server user user2 groupname group1 auth md5 auth-password password priv DES priv-
password password
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server v3host

Specifies the host recipient for SNMPv3 trap notification.

Syntax

snmp-server v3host { **ipv4_host** | **ipv6_host** | **dns_host** } *user_name* [**notifytype** { **traps** | **informs** }] [**engineid** *engine-id*] [**udp-port** *port_number*] [**severity-level** | { **none** | **debug** | **info** | **warning** | **error** | **critical** }] [**use-vrf** { **vrf-name**}]

no snmp-server v3host { **ipv4_host** | **ipv6_host** | **dns_host** } *user_name* [**notifytype** {**traps** | **informs**}] [**engineid** *engine-id*] [**udp-port** *port_number*] [**severity-level** | {**none** | **debug** | **info** | **warning** | **error** | **critical** }] [**use-vrf**]

Parameters

ipv4_host | **ipv6_host** | **dns_host**
: Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

user_name
: Specifies the SNMPv3 user name to be associated with the SNMPv3 host entry.

notifytype traps | **informs**
: Specifies the type of notification traps that are sent for the host. Traps and informs are supported. The default notify type is traps.

engineID *engine-id*
: Configures the remote engine ID to receive informs on a remote host.

udp-port *port_number*
: Specifies the UDP port of the host. The default UDP port number is 162.

severity-level { **none** | **debug** | **info** | **warning** | **error** | **critical** }
: Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASLog (swEvent) traps can be filtered based on severity level. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of None is specified, all traps are filtered and no RASLog traps are received. The default severity level is none.

use-vrf *vrf-name*
: Configures SNMP to use the specified VRF to communicate with the host. The default is mgmt-vrf.

Modes

Global configuration mode

Usage Guidelines

You can associate a global SNMPv3 host only with global SNMPv3 users and the local SNMPv3 host only with local SNMPv3 users. You cannot create a SNMPv3 host by associating with the local SNMPv3 users and vice versa.

Examples

The following example creates an entry for SNMPv3 trap IPv4 host 10.23.23.45 associated with SNMP user "snmpadmin1."

```
device(config)# snmp-server v3host 10.23.23.45 snmpadmin1 severity-level info
```

The following example creates an entry for SNMPv3 trap IPv6 host 1050:0:0:0:5:600:300c:326b associated with SNMP user "snmpadmin2." The trap host receives SNMPv3 traps from the configured device.

```
device(config)# snmp-server v3host 1050::5:600:300c:326b snmpadmin2 severity-level Info
```

The following example associates the default-vrf VRF for a trap host recipient.

```
device(config)# snmp-server v3host 10.24.61.10 public use-vrf default-vrf
```

History

Release version	Command history
18x.1.00	This command was introduced.

snmp-server view

Creates a view entry with MIB object IDs to be included or excluded for user access.

Syntax

snmp-server view *view-name mib_tree* **included** | **excluded**

no snmp-server view *view-name mib_tree* **included** | **excluded**

Command Default

None

Parameters

view-name
: Specifies the alphanumeric name to identify the view. The name should not contain spaces.

mib_tree
: Specifies the MIB object ID called Object Identifiers (OIDs) that represent the position of the object or sub-tree in the MIB hierarchy.

included | **excluded**
: Specifies whether the specified MIB object ID must be included in the view or excluded from the view.

Modes

Global configuration mode

Usage Guidelines

The maximum number of views supported with MIB tree entries is 10. Either a single view name associated with 10 different MIB object IDs or 10 different view names associated with each one of the MIB object IDs is allowed.

Examples

The following example creates an SNMP view entry "view1" with excluded permission for the MIB object ID "1.3.6.1.2.1.1.3."

```
device(config)# snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

The following example creates an SNMP view entry "view2" with included permission for the MIB object ID "1.3.6.1."

```
device(config)# snmp-server view view2 1.3.6.1 included
```

The following example removes the SNMP view entry "view1" from the configuration list.

```
device(config)# no snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

History

Release version	Command history
18x.1.00	This command was introduced.

source

Configures the source address or a source interface for a tunnel interface.

Syntax

source { *ip-address* | **ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id* }

no source

Command Default

No source address or interface is configured.

Parameters

ip-address
Specifies the IPv4 address of an interface.

ethernet *slot/port*
Specifies an Ethernet interface.

loopback *number*
Specifies a loopback port.

ve *vlan_id*
Specifies a VE interface.

Modes

Interface tunnel configuration mode

Usage Guidelines

The maximum number of tunnel source supported is 16.

Use the **no source** command to remove the configured source for the tunnel interface.

The tunnel source address should be one of the router IP addresses configured on a physical, loopback, or VE interface, through which the other end of the tunnel is reachable. The source interface must have at least one IP address configured on it.

When the physical/ve interface is specified as the source of the GRE tunnel, the lowest IP address of that interface is used as the tunnel source IP address. If the smallest IP address is removed from the interface, the next smallest IP address is used as the tunnel source.

Examples

This example configures the source address for the tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)#  source 10.1.2.4
```

This example sets an Ethernet interface as a source tunnel.

```
device# configure terminal
device(config)# interface tunnel 3
device(config-intf-tunnel-3)# source ethernet 3/1
```

History

Release version	Command history
18x.1.00	This command was introduced.

source-interface(RADIUS)

Configures a source IP address for Remote Authentication Dial-In User Service (RADIUS) packets that originate on the device.

Syntax

source-interface { **ethernet** | **loopback** } | **ve** *ve-num* }

no source-interface

Command Default

When a source interface is not configured for a RADIUS host, the IP address of the interface through which a RADIUS packet exits the device is used in the IP header as the source IP address.

Parameters

ethernet

Causes the ethernet interface to be used as the source interface for RADIUS packets that originate on the device.

loopback

Causes the loopback interface to be used as the source interface for RADIUS packets that originate on the device.

management

Causes a management interface to be used as the source interface for RADIUS packets that originate on the device.

0

Causes the chassis IP address to be used as the source IP address.

1

Causes the MM1 IP address to be used as the source IP address.

ve *ve-num*

Specifies a virtual ethernet interface value to be used as the source interface for RADIUS packets that originate on the device.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

NOTE

When an interface without an IP address is configured as the source interface, the egress interface IP address is used as the source interface.

NOTE

The source interface configuration should not conflict with the VRF specified for communications with the RADIUS server host; when the specified source interface is not part of the VRF configured for communications with the RADIUS server host, the egress interface IP address is used as the source interface.

Modifications to the interface (such as changing the IP address, VRF, and so on) that is configured as the source interface, do not affect existing connections unless the corresponding link is dropped due to these changes.

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure an Ethernet interface (0/2) as the source interface for RADIUS packets that originate on the device and are destined for the RADIUS server host 10.37.73.180.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# source-interface ethernet 0/2
```

History

Release version	Command history
18x.1.00	This command was introduced.

source-interface (TACACS+)

Configures a source IP address for TACACS+ packets that originate on the device.

Syntax

source-interface { **ethernet** *slot/port* | **loopback** *port* | **management** { **0** | **1** } | **ve** *ve-num* }

no source-interface

Command Default

When a source interface is not configured for a TACACS+ server host, the IP address of the interface through which a TACACS+ packet exits the device is used in the IP header as the source IP address.

Parameters

ethernet *slot/port*
: Causes the Ethernet interface to be used as the source interface for TACACS+ packets that originate on the device.

loopback *port*
: Causes the loopback interface to be used as the source interface for TACACS+ packets that originate on the device. Range is 1 through 255.

management
: Causes a management interface to be used as the source interface for TACACS+ packets that originate on the device. In pizza box platforms, the Chassis-IP is considered to be the same as MM-IP. That is, selecting either one of these uses the MM-IP.

  0
  : Causes the chassis IP address to be used as the source IP address.

  1
  : Causes the active MM management IP address to be used as the source IP address.

ve *ve-num*
: Specifies a virtual Ethernet interface value to be used as the source interface for TACACS+ packets that originate on the device. Range is 1 through 4096.

Modes

TACACS+ server host VRF configuration mode

Usage Guidelines

NOTE

When an interface without an IP address is configured as the source interface, the egress interface IP address is used as the source interface.

NOTE
The source interface configuration should not conflict with the VRF specified for communications with the TACACS+ server host; when the specified source interface is not part of the VRF configured for communications with the TACACS+ server host, the egress interface IP address is used as the source interface.

Modifications to the interface (such as changing the IP address, VRF, and so on) that is configured as the source interface, do not affect existing connections unless the corresponding link is dropped because of these changes.

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure an Ethernet interface (0/2) as the source interface for TACACS+ packets that originate on the device and are destined for the TACACS+ server host 10.1.1.2.

```
device# configure terminal
device(config)# tacacs-server 10.1.1.2 use-vrf default-vrf
device(config-host-10.1.1.2/default-vrf)# source-interface ethernet 0/2
```

The following example uses the **show running-config tacacs-server** command to confirm the configuration

```
device(config-host-10.1.1.2/default-vrf)# do show running-config tacacs-server
tacacs-server host 1.2.3.4 use-vrf default-vrf
 key "Yf0BKEhsc83gp+kIoGMQ/g==\n"
 encryption-level 7
 source-interface loopback 10
!
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree autoedge

Enables automatic edge detection.

Syntax

spanning-tree autoedge

no spanning-tree autoedge

Command Default

Auto detection is not enabled.

Modes

Interface configuration mode

Usage Guidelines

The port can become an edge port if no Bridge Protocol Data Unit (BPDU) is received.

Examples

To enable automatic edge detection:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree autoedge
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree bpdu-mac

Sets the MAC address of the Bridge Protocol Data Unit (BPDU).

Syntax

spanning-tree bpdu-mac [**0100.0ccc.cccd** | **0304.0800.0700**]

no spanning-tree bpdu-mac [**0100.0ccc.cccd** | **0304.0800.0700**]

Parameters

0100.0ccc.cccd
: Cisco Control Mac

0304.0800.0700
: Extreme Control Mac

Modes

Interface configuration mode

Usage Guidelines

This command will only take effect when the protocol is PVST+ or R-PVST+.

Extreme devices support PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Enter **no spanning-tree bpdu-mac 0100.0ccc.cccd** to remove the address.

Examples

To set the MAC address of the BPDU:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree bpdu-mac 0100.0ccc.cccd
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree cost

Changes an interface's spanning-tree port path cost.

Syntax

spanning-tree cost *cost*

no spanning-tree cost *cost*

Command Default

The default path cost is 200000000.

Parameters

cost

Specifies the path cost for the Spanning Tree Protocol (STP) calculations. Valid values range from 1 through 200000000.

Modes

Interface configuration mode

Usage Guidelines

Lower path cost indicates a greater chance of becoming root.

Examples

To set the port cost to 128:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree cost 128
```

spanning-tree edgeport

Enables the edge port on an interface to allow the interface to quickly transition to the forwarding state.

Syntax

spanning-tree edgeport [**bpdu-guard**]

no spanning-tree edgeport [**bpdu-guard**]

Command Default

Edge port is disabled.

Parameters

bpdu-guard

Guards the port against the reception of BPDUs.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is only for RSTP and MSTP. Use the **spanning-tree portfast** command for STP

Note the following details about edge ports and their behavior:

- A port can become an edge port if no BPDU is received.
- A port must become an edge port before it receives a BPDU.
- When an edge port receives a BPDU, it becomes a normal spanning-tree port and is no longer an edge port.
- Because ports directly connected to end stations cannot create bridging loops in the network, edge ports directly transition to the forwarding state, and skip the listening and learning states

Examples

To enable a port to quickly transition to the forwarding state:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree edgeport
```

To guard the port against reception of BPDUs:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree edgeport
device(conf-if-eth-1/5)# spanning-tree edgeport bpdu-guard
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree guard root

Enables the guard root to restrict which interface is allowed to be the spanning tree root port or the device's path-to-the-root.

Syntax

spanning-tree guard root [**vlan** *vlan_id*]

no spanning-tree guard root

Command Default

Guard root is disabled.

Parameters

vlan *vlan_id*
Specifies a VLAN.

Modes

Interface configuration mode

Usage Guidelines

Guard root protects the root bridge from malicious attacks and unintentional misconfigurations where a bridge device that is not intended to be the root bridge becomes the root bridge. This causes severe bottlenecks in the data path. Guard root ensures that the port on which it is enabled is a designated port. If the guard root enabled port receives a superior Bridge Protocol Data Unit (BPDU), it goes to a discarding state.

If the VLAN parameter is not provided, the guard root functionality is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

The root port provides the best path from the switch to the root switch.

Examples

To enable guard root:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree guard root
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree link-type

Enables and disables the rapid transition for the Spanning Tree Protocol (STP).

Syntax

spanning-tree link-type [**point-to-point** | **shared**]

Command Default

The **spanning-tree link-type** is set to **point-to-point**.

Parameters

point-to-point
Enables rapid transition.

shared
Disables rapid transition.

Modes

Interface subtype configuration mode

Usage Guidelines

This command overrides the default setting of the link type.

Examples

To specify the link type as shared:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree link-type shared
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree portfast

Enables the Port Fast feature on an interface to allow the interface to quickly transition to forwarding state.

Syntax

spanning-tree portfast [**bpdu-guard**]

no spanning-tree portfast [**bpdu-guard**]

Command Default

Port Fast is disabled.

Parameters

bpdu-guard

Guards the port against the reception of BPDUs.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is applicable the only for the Spanning Tree Protocol (STP). Port Fast immediately puts the interface into the forwarding state without having to wait for the standard forward time. Use the **spanning-tree edgeport** command for MSTP and RSTP.

BPDU guard disables all portfast-enabled ports should they ever receive BPDU frames. It does not prevent transmitting of BPDU frames.

If you enable **spanning-tree portfast bpdu-guard** on an interface and the interface receives a BPDU, the software disables the interface and puts the interface in the ERR_DISABLE state.

Enable Port Fast on ports connected to host. Enabling Port Fast on interfaces connected to switches, bridges, hubs, and so on can cause temporary bridging loops, in both trunking and nontrunking mode.

Examples

To enable a port to quickly transition to the forwarding state:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree portfast
```

To guard the port against reception of BPDUs:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree portfast
device(conf-if-eth-1/5)# spanning-tree portfast bpdu-guard
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree priority

Changes an interface's spanning-tree port priority.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

Command Default

The default value is 128.

Parameters

priority

Specifies the interface priority for the spanning tree. The range of valid values is from 0 through 240. Port priority is in increments of 16.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no spanning-tree priority** to return to the default setting.

Examples

To configure the port priority to 16:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree priority 16
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree restricted-role

Restricts the role of the port from becoming a root port.

Syntax

spanning-tree restricted-role

no spanning-tree restricted-role

Command Default

The restricted role is disabled.

Modes

Interface configuration mode

Usage Guidelines

Enter **no spanning-tree restricted-role** to return to the default setting.

Examples

To configure the port from becoming a root port:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree restricted-role
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree restricted-tcn

Restricts the Topology Change Notification (TCN) Bridge Protocol Data Units (BPDUs) sent on the port.

Syntax

spanning-tree restricted-tcn

no spanning-tree restricted-tcn

Command Default

The restricted TCN is disabled.

Modes

Interface configuration mode

Usage Guidelines

Enter **no spanning-tree restricted-tcn** to disable this parameter.

Examples

To restrict the TCN on a specific interface:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree restricted-tcn
```

History

Release version	Command history
18x.1.00	This command was introduced.

spanning-tree shutdown

Enables or disables spanning tree on the interface or VLAN.

Syntax

spanning-tree shutdown

no spanning-tree shutdown

Command Default

Spanning tree is disabled by default.

Modes

Interface (Ethernet or VLAN) configuration mode

Usage Guidelines

Enter **no spanning-tree shutdown** to enable spanning tree on the interface or VLAN.

Once all of the interfaces have been configured for a VLAN, you can enable Spanning Tree Protocol (STP) for all members of the VLAN with a single command. Whichever protocol is currently selected is used by the VLAN. Only one type of STP can be active at a time.

A physical interface (port) can be a member of multiple VLANs. For example, a physical port can be a member of VLAN 1002 and VLAN 55 simultaneously. In addition, VLAN 1002 can have STP enabled and VLAN 55 can have STP disabled simultaneously.

Vlan 1002 can not be enabled with the **spanning-tree shutdown** command.

Examples

To disable spanning tree on a specific interface:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

speed (Ethernet)

Sets the speed negotiation value on an Ethernet interface.

Syntax

speed { **100** | **1000** | **1000-auto** | **10000** | **auto** }

Command Default

The speed is set to **auto**.

Parameters

100
Forces the speed to 100 Mbps.

1000
Forces the speed to 1 Gbps.

1000-auto
Forces the speed to 1 Gbps AN (802.3 Clause 37 Auto-Negotiation)

10000
Forces the speed to 10 Gbps.

auto
Allows the interface to negotiate the speed setting.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **auto** keyword to reset the default setting.

Examples

The following example changes the speed to 1G with auto negotiation.

```
device# configure terminal
device(config)# interface Ethernet 2/1
device(config-if-eth-2/1)# speed 1000-auto
device(config-if-eth-2/1)# no shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

spt-threshold infinity

Configures all sources to use the shared rendezvous point (RP) tree.

Syntax

spt-threshold infinity

no spt-threshold

Command Default

SPT is used for sending packets.

Modes

Router PIM configuration mode.

Usage Guidelines

This command uses only the rendezvous point to send packets and does not switch over to SPT.

The **no** form of the command resets the default setting and uses SPT for sending packets.

Examples

The following example configures all sources to use the shared RP tree.

```
device(config)# router pim
device(config-pim-router)# spt-threshold infinity
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh

Connects to a remote server by means of the Secure Shell (SSH) protocol.

Syntax

ssh { *IP_address* | *hostname* } [**-c** | **-l** | **-m** | **interface** {**ethernet** *slot/port* | **management** | **ve** *vlan-id* } | **vrf** *vrf-name*] }

Command Default

SSH connects to port 22.

Parameters

IP_address

Specifies the server IP address in IPv4 or IPv6 format.

hostname

Specifies the host name, a string from 1 through 253 characters.

-c

Specifies the encryption algorithm for the SSH session. This parameter is optional. Supported algorithms include the following:

aes128-cbc

AES 128-bits

aes192-cbc

AES 192-bits

aes256-cbc

AES 256-bits

-l *username*

Login name for the remote server. This parameter is optional. If you specify a user name, you will be prompted for a password. If you do not specify a user name, the command assumes you are logging in as root and will prompt for the root password.

-m

Specifies the HMAC (Hash-based Message Authentication Code) message encryption algorithm. This parameter is optional; if no encryption algorithm is specified, the default (**hmac-md5**) is used. Supported algorithms include the following:

hmac-md5

MD5 128-bits. This is the default setting.

hmac-md5-96

MD5 96-bits

hmac-sha1

SHA1 160-bits

hmac-sha1-96

SHA1 96-bits

interface

Specifies an interface.

ethernet *slot/port*

Specifies an Ethernet interface slot and port number. The v valid value is 0.

management

Specifies a management interface.

ve *vlan-id*

Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

vrf *vrf-name*

Specifies a VRF instance. See the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to establish an encrypted SSH connection from a switch to a remote networking device. This implementation is based on SSH v2.

To use the **ssh** command on the management VRF, use the **vrf** keyword and enter **mgmt-vrf** manually.

The following features are not supported:

- Displaying SSH sessions
- Deleting stale SSH keys

Examples

To connect to a remote device using an SSH connection with default settings:

```
device# ssh 10.70.212.152

The authenticity of host '10.70.212.152 (10.70.212.152)' can't be established.
RSA key fingerprint is f0:2a:7e:48:60:cd:06:3d:f4:44:30:2a:ce:68:fe:1d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.70.212.152' (RSA) to the list of known hosts.
Password:
```

To connect to a remote device using an SSH connection with the management VRF:

```
device# ssh 10.70.212.152 vrf mgmt-vrf
```

To connect to a remote device using an SSH connection with a login name:

```
device# ssh -l admin 127.2.1.8

admin@127.2.1.8's password
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh client cipher

Sets the SSH client's cipher list for the SSH client.

Syntax

ssh client cipher *string*

no ssh client cipher

Parameters

string

The string name of the cipher. Refer to the device for the available options.

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh client cipher** command remove the cipher list from the ssh client.

Examples

Sets the SSH client's cipher list.

History

Release version	Command history
18x.1.00	This command was introduced.

ssh client cipher non-cbc

Sets the SSH client's cipher list to non-cbc ciphers for the SSH client.

Syntax

ssh client cipher non-cbc

no ssh client ciphe non-cbcr

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh client cipher non-cbc** command remove the non-cbc cipher list from the ssh client.

Examples

Sets the SSH client's cipher list to non-cbc ciphers.

```
device# configure terminal
device(config)# ssh client cipher non-cbc
device(config)# do show running-config ssh
ssh server non-cbc
ssh client non-cbc
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh client key-exchange

Specifies the method used for generating the one-time session keys for encryption and authentication with the Secure Shell (SSH) server and Diffie-Hellman group 14.

Syntax

ssh client key-exchange *string*

no ssh client key-exchange

Parameters

string

The string for the name of the algorithm diffie-hellman-group14-sha1, or a comma-separated list of supported Key-exchange algorithms; such as diffie-hellman-group14-sha1,diffie-hellman-group1-sha1, and so on.

Command Default

This command is not configured by default.

Modes

Global configuration mode

Usage Guidelines

You can configure the SSH client key-exchange method to DH Group 14. When the ssh client key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client end is also configured to DH Group 14. Enter **no ssh client key-exchange** to restore ssh client key-exchange to the default value.

For information on DH Group 14, refer to RFC 3526.

For backward compatibility, the string "dh-group-14" is also acceptable in place of "diffie-hellman-group14-sha1"

Examples

To set ssh client key-exchange to DH Group 14:

```
device(config)#ssh client key-exchange diffie-hellman-group14-sha1
```

To restore the ssh client key-exchange to default value:

```
device(config)# no ssh client key-exchange
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh client mac

Supports MAC configurations for the SSH client.

Syntax

ssh client mac *string*

no ssh client mac

Command Default

SSH server is enabled by default.

Parameters

string

The string name of the default MAC required. Your choices are hmac-md5, hmac-sha1, hmac-sha2-256, and hmac-sha2-512. The default MACs supported in FIPS mode are hmac-sha1, hmac-sha2-256, and hmac-sha2-512.

Modes

Global configuration mode

Usage Guidelines

The MAC hmac-md5 is not supported in FIPS mode.

Examples

Typical command example:

```
device# configure terminal
device(config)# ssh client mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
device(config)# do show running-config ssh client
ssh client mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
!
device(config)# do show ssh client status
SSH Client Mac: hmac-sha1,hmac-sha2-256,hmac-sha2-512
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh server cipher

Sets the SSH server's cipher list for the SSH server.

Syntax

ssh server cipher *string*

no ssh server cipher

Parameters

string

The string name of the cipher. Refer to the device for the available options.

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh server cipher** command remove the cipher list from the ssh client.

Examples

Sets the SSH server's cipher list.

```
device# configure terminal
device(config)# ssh server cipher aes256-ctr
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh server cipher non-cbc

Sets the SSH server's cipher list to non-cbc ciphers for the SSH server.

Syntax

ssh server cipher non-cbc

no ssh server cipher non-cbc

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh server cipher non-cbc** command remove the non-cbc cipher list from the ssh client.

Examples

Sets the SSH server's cipher list to non-cbc ciphers.

```
device# configure terminal
device(config)# ssh server cipher non-cbc
device(config)# do show running-config ssh
ssh server non-cbc
ssh client non-cbc
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh server key

Generates or zeroizes SSH crypto keys on the device. All three keys can be active simultaneously.

Syntax

ssh server key {**dsa** | **rsa** [**1024** | **2048**] | **ecdsa 256**}

no ssh server key {**dsa** | **rsa** | **ecdsa**}

Command Default

The default values of SSH keys are:

- DSA is active
- ECDSA value is 256
- RSA value is 2048

Parameters

dsa
Generates the DSA key.

rsa [**1024** | **2048**]
Generates the RSA key, in either the 1024 or 2048 bit size.

ecdsa 256
Generates the ECDSA key at 256 bits.

Modes

Global configuration mode

Usage Guidelines

The **no ssh server key** command zeroizes the SSH keys on the device.

If you generate and delete SSH crypto keys, you must restart the SSH server using the **no ssh server shutdown** command to enable the configuration.

Examples

Typical DSA command example:

```
device(config)# ssh server key dsa
```

Typical RSA command example:

```
device(config)# ssh server key rsa 1024
```

Typical ECDSA command example:

Typical zeroizing example:

```
device(config)# no ssh server key dsa
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh server key-exchange

Specifies the method used for generating the one-time session keys for encryption and authentication with the Secure Shell (SSH) server and Diffie-Hellman group 14.

Syntax

ssh server key-exchange *string*

no ssh server key-exchange

Parameters

string

The string for the name of the algorithm diffie-hellman-group14-sha1, or a comma-separated list of supported Key-exchange algorithms; such as diffie-hellman-group14-sha1,diffie-hellman-group1-sha1, and so on.

Command Default

This command is not configured by default.

Modes

Global configuration mode

Usage Guidelines

You can configure the SSH server key-exchange method to DH Group 14. When the SSH server key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client end is also configured to DH Group 14. Enter **no ssh server key-exchange** to restore SSH server key-exchange to the default value.

For information on DH Group 14, refer to RFC 3526.

For backward compatibility, the string "dh-group-14" is also acceptable in place of "diffie-hellman-group14-sha1"

Examples

To set SSH server key-exchange to DH Group 14:

```
device(config)# ssh server key-exchange diffie-hellman-group14-sha1
```

To restore the SSH server key-exchange to default value:

```
device(config)# no ssh server key-exchange
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh server mac

Supports MAC configurations for the SSH server.

Syntax

ssh server mac *string*

no ssh server mac

Parameters

string

The string name of the default MAC required. Your choices are hmac-md5, hmac-sha1, hmac-sha2-256, and hmac-sha2-512. The default MACs supported in FIPS mode are hmac-sha1, hmac-sha2-256, and hmac-sha2-512.

Modes

Global configuration mode

Usage Guidelines

The MAC hmac-md5 is not supported in FIPS mode.

Examples

Typical command example:

```
device# configure terminal
device(config)# ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
device(config)# do show running-config ssh server
ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
ssh server key rsa 2048
ssh server key ecdsa 256
ssh server key dsa
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh server max-sessions

Specifies the maximum number of open Secure Shell (SSH) sessions per SSH network connection.

Syntax

ssh server max-sessions *number*

no ssh server max-sessions

Command Default

The default number of sessions is 1 unless it is changed by this command.

Parameters

number

Maximum number of sessions. Range is from 1 through 10.

Modes

Global configuration mode

Usage Guidelines

After executing this command, in order to use the new number of sessions, you must first shut down the SSH server, by means of the **ssh server use-vrf shutdown** command, and then restart it, by means of the **no ssh server use-vrf shutdown** command.

The maximum number of sessions specified by this command is synchronized to the standby management module (MM). However, to make the change effective on the standby MM, you must first disable service on that module by means of the **no ssh server standby enable** command, and then reenable service by means of the **ssh server standby enable** command.

A downgrade to a previous release is blocked if this command has been executed in the running configuration.

Use the **no ssh server max-sessions** command to revert to the default of 1 session. You must also stop and restart service as in the Usage Guidelines above.

Examples

To change the maximum number of supported SSH sessions from the default to 7, and confirm the configuration:

```
device# configure terminal
device(config)# ssh server max-sessions 7
device(config)# do show running-config ssh server
ssh server max-sessions 7
ssh server key rsa 2048
ssh server key ecdsa 256
ssh server key dsa
```

To revert to the default number of sessions (1):

```
device(config)# no ssh server max-sessions
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssh server rekey-interval

Configures the Secure Shell (SSH) server rekey-interval.

Syntax

ssh server rekey-interval *interval*

no ssh server rekey-interval

Parameters

interval

The value for the rekey interval. Range is from 900 to 3600 seconds.

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh server rekey-interval** command to remove the rekey-interval.

History

Release version	Command history
18x.1.00	This command was introduced.

ssh server shutdown

Disables SSH service.

Syntax

ssh server [**use-vrf** *vrf-name*] **shutdown**

no ssh server [**use-vrf** *vrf-name*] **shutdown**

Parameters

use-vrf *vrf-name*

Specifies a user-defined VRF, or built-in VRFs such as mgmt-vrf or default-vrf.

Modes

Global configuration mode

Usage Guidelines

Enter **no ssh server shutdown** to enable SSH service.

The use of the **use-vrf** keyword brings down the server only for the specified VRF. The user can shut down any server in any VRF, including the management and default VRF.

When this command is executed and a VRF is not specified by means of the **use-vrf** keyword, the server is brought down only in the management VRF ("mgmt-vrf") (the default VRF for this command).

Examples

To shut down SSH service on the management VRF:

```
device(config)# ssh server shutdown
```

To shut down SSH service for a user-defined VRF:

```
device(config)# ssh server use-vrf myvrf shutdown
```

To enable SSH service on the management VRF:

```
device(config)# no ssh server shutdown
```

To enable SSH service:

```
device(config)# no ssh server shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

ssm-enable

Enables or disables the SSM mode for PIM.

Syntax

ssm-enable range*IP prefix list name*

no ssm-enable range *IP prefix list name*

Parameters

range
Specifies the range of the SSM map.

IP prefix list name
Specifies the name of the IP prefix list.

Modes

Router PIM configuration mode

Usage Guidelines

PIM Source Specific Multicast (SSM) is a subset of the PIM SM protocol. In the PIM SSM mode, the shortest path tree (SPT) is created at the source. The SP is created between the receiver and source, but the SPT is built without the help of the RP. The router closest to the interested receiver host is notified of the unicast IP address of the source for the multicast traffic. PIM SSM goes directly to the source-based distribution tree without the need of the RP connection. PIM SSM is different from PIM SM because it forms its own SP tree, without forming a shared tree.

Examples

The following example enables SSM and applies the default SSM range - 232.0.0.0/8.

```
device(config)# router pim
devic(config-pim-router)# ssm-enable
```

The following example enables SSM and configures an SSM map at the global level.

```
 device(config)# ip igmp ssm-map enable
device(config)# ip igmp ssm-map ssm-map-230-to-232 203.0.0.10
device(config)# ip igmp ssm-map ssm-map-233-to-234 204.0.0.10
```

The following example configures the SSM range at the router PIM configuration level.

```
device(config)# router pim
device(config-pim-router)# ssm-enable range PL_ssm_range -230-to-234
```

History

Release version	Command history
18x.1.00	This command was introduced.

start (CFM)

Defines the start time for a delay measurement receiver session.

Syntax

start { **now** | **after** *HH:MM:SS* | *HH:MM:SS* **daily** }

no start

Command Default

The start time is not defined

Parameters

now

The session is initiated immediately.

after *HH:MM:SS*

Initiates the one-way delay measurement receiver session after a period of time has elapsed, in hours, minutes, and seconds.

HH:MM:SS **daily**

Initiates the one-way delay measurement receiver session at the specified time every day.

Modes

CFM protocol configuration mode

Usage Guidelines

The **no start** command deletes the start time.

Relative time is converted to absolute time. Otherwise, the system would not point to the expected time after a reboot.

Examples

Example of starting the session after one hour and thirty minutes.

```
device(config-cfm-oneway-dm-receiver-1)#  start after 01:30:00
```

Example of starting the session daily at 3:30 pm.

```
device(config-cfm-oneway-dm-receiver-1)#  start daily 15:30:00
```

History

Release version	Command history
18x.1.00	This command was introduced.

start (Y1731)

Configure the start time.

Syntax

start at *hh:mm:ss* **daily**

start after *hh:mm:ss* **daily**

no start

Parameters:

at

Spcifies the time to start at.

hh:mm:ss

Specifies the time in hour, minute, and second format.

after

Specifies the measurement interval in minutes.

daily

Specifies time to start daily.

Command Default

The default value is start after 00:05:00 (After).

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the start configuration.

Examples

This example shows how to configure the start time.

```
device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
```

History

Release version	Command history
18x.1.00	This command was introduced.

static-network

Configures a static BGP4 network, creating a stable network in the core.

Syntax

static-network *network/mask* [**distance** *num*]

no static-network *network/mask* [**distance** *num*]

Parameters

network/mask
Network and mask in CIDR notation.

distance *num*
Specifies an administrative distance value for this network. Valid values range from 1 through 255. The default is 200.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

While a route configured with this command will never flap unless it is deleted manually, a static BGP4 network will not interrupt the normal BGP4 decision process on other learned routes that are installed in the Routing Table Manager (RTM). Consequently, when there is a route that can be resolved, it will be installed into the RTM.

Examples

The following example configures a static network and sets an administrative distance of 300.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# static-network 10.11.12.0/32 distance 300
```

History

Release version	Command history
18x.1.00	This command was introduced.

statistics

Enables statistics on the tunnel interface.

Syntax

statistics

no statistics

Command Default

Statistics is disabled on a tunnel interface.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no** form of this command to disable statistics on the tunnel interface.

Note that traffic loss might occur when you enable or disable statistics on a tunnel interface.

Examples

This example enables statistics on the tunnel interface.

```
device# configure terminal
device (config)# interface tunnel 5
device(config-intf-tunnel-5)# statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

statistics (bridge domain)

Enables ingress and egress statistics on a bridge domain.

Syntax

statistics

no statistics

Parameters

None

Command Default

Statistics are disabled.

Modes

Bridge-domain configuration mode

Usage Guidelines

The **no** form of the command disables statistics on the bridge domain.

Examples

The following example shows how to enable ingress and egress statistics on bridge domain 2.

```
device# config terminal
device(config)# bridge-domain 2
device(config-bridge-domain-2)# statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

statistics (VLAN)

Enables statistics on a VLAN.

Syntax

statistics

no statistics

Command Default

Statistics are disabled.

Parameters

None

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command disables statistics on a VLAN.

Examples

The following example shows how to enable statistics on VLAN 10.

```
device# config terminal
device(config)# vlan 10
device(config-Vlan-10)# statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

stop (CFM)

Defines the stop time for a delay measurement receiver session.

Syntax

stop { **now** | **after** *HH:MM:SS* | *HH:MM:SS* **daily** }

no stop

Command Default

The stop time is not defined

Parameters

now

The session is halted immediately.

after *HH:MM:SS*

Halts the one-way delay measurement receiver session after a period of time has elapsed, in hours, minutes, and seconds.

HH:MM:SS **daily**

Halts the one-way delay measurement receiver session at the specified time every day.

Modes

CFM protocol configuration mode

Usage Guidelines

The **no stop** command deletes the stop time.

The one-way delay measurement receiver session should be started before starting the one-way delay measurement Initiator session. Also, the one-way delay measurement Initiator session should be stopped before stopping the one-way delay measurement Receiver session.

Relative time is converted to absolute time. Otherwise, the system would not point to the expected time after a reboot.

Examples

Example of stopping the session after one hour and thirty minutes.

```
device(config-cfm-oneway-dm-receiver-1)#  stop after 01:30:00
```

Example of stopping the session daily at 3:30 pm.

```
device(config-cfm-oneway-dm-receiver-1)#  stop daily 15:30:00
```

History

Release version	Command history
18x.1.00	This command was introduced.

stop (Y1731)

Configure the stop time.

Syntax

stop [**at** *hh:mm:ss* | **after** *hh:mm:ss*]

no stop

Parameters:

at

Spcifies the time to stop at.

hh:mm:ss

Specifies the time in hour, minute, and second format.

after

Specifies the time to stop after.

Command Default

The default value is 01:05:00 (After).

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the stop configuration.

Examples

This example shows how to configure the stop time.

```
device# configure terminal
device (config-cfm)# protocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
```

History

Release version	Command history
18x.1.00	This command was introduced.

storm-control ingress (inteface)

Limits ingress traffic on a specified interface.

Syntax

storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** } { **limit-bps** | **limit-percent** } *rate* }

no storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** }

Parameters

broadcast

Specifies that the command will operate on broadcast traffic only.

unknown-unicast

Specifies that the command will operate on unknown-unicast traffic only.

multicast

Specifies that the command will operate on multicast traffic only.

limit-bps

Specifies that the value given to the *rate* parameter is in bits per second. If the traffic on the interface reaches this rate, no more traffic (for the traffic type specified) is allowed on the interface.

limit-percent

Specifies that the value given to the *rate* parameter is in percentage of capacity of the interface. If the traffic on the interface reaches this percentage of capacity, no more traffic (for the traffic type specified) is allowed on the interface.

rate

Specifies the amount of traffic allowed, either in bits per second or a percentage of the capacity of the interface, depending on which parameter was chosen with the rate.
If you are specifying rate in bps, enter an integer from 0 to 10000000000. Because each application-specific integrated circuit (ASIC) may support different bit granularity, bit rates are rounded up to the next achievable rate.
If you are specifying rate in percent of interface capacity, enter an integer from 0 to 100.

Modes

Interface configuration mode

Usage Guidelines

If you want to modify an active BUM storm control configuration, you must first disable it, then issue the **storm-control ingress** command again with the new parameters.

Enter **no storm-control ingress** to disable BUM storm control for a particular traffic type on an interface.

Examples

To configure storm control on an Ethernet interface, with a rate limited to 1000000 bps:

```
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# storm-control ingress broadcast 1000000
```

History

Release version	Command history
18x.1.00	This command was introduced.

summary-address (OSPFv2)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Syntax

summary-address *A.B.C.D E.F.G.H*

no summary-address

Command Default

Summary addresses are not configured.

Parameters

A.B.C.D E.F.G.H

IP address and mask for the summary route representing all the redistributed routes in dotted decimal format.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.This parameter affects only imported, type 5 external routes.

The no form of the command disables route summarization.

Examples

The following example configures a summary address of 10.1.0.0 with a mask of 10.255.0.0. Summary address 10.1.0.0, includes addresses 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. For all of these networks, only the address 10.1.0.0 is advertised in external LSAs:

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# summary-address 10.1.0.0 10.255.0.0
```

History

Release version	Command history
18x.1.00	This command was introduced.

summary-address (OSPFv3)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Syntax

summary-address *IPv6-addr/mask*

no summary-address

Command Default

Summary addresses are not configured.

Parameters

A:B:C:D/LEN

IPv6 address and mask for the summary route representing all the redistributed routes in dotted decimal format.

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified IPv6 address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.

Examples

The following example configures a summary address of 2001:db8::/24 for routes redistributed into OSPFv3. The summary prefix 2001:db8::/24 includes addresses 2001:db8::/1 through 2001:db8::/24. Only the address 2001:db8::/24 is advertised in an external link-state advertisement.

support autoupload-param

Defines autoupload parameters.

Syntax

support autoupload-param hostip *hostip* | **user** *user_acct* | **password** *password* [**protocol** [**ftp** | **scp** | **sftp**] **directory** *path*

Parameters

hostip *host-ip*
Specifies the IP address of the remote host.

user *user_acct*
Specifies the user name to access the remote host.

password *password*
Specifies the password to access the remote host.

protocol *FTP* | *SCP*| *SFTP*
Specifies the protocol used to access the remote server.

directory *path*
Specifies the path to the directory.

Modes

Global configuration mode

Examples

```
device(config)# support autoupload-param hostip 10.31.2.27 protocol [ftp|scp | sftp]username hegdes
directory /uers/home40/hegdes/autoupload password

(<string>): *****
```

History

Release version	Command history
18x.1.00	This command was introduced.

suppress-arp

Enables Address Resolution Protocol (ARP) suppression on a current VLAN or bridge domain. ARP suppression can lessen ARP-related traffic within an IP Fabric.

Syntax

suppress-arp

no suppress-arp

Command Default

ARP suppression is disabled.

Modes

VLAN configuration mode

Bridge-domain configuration mode

Usage Guidelines

This feature is required, along with ND suppression, if static anycast gateway is supported in an IP Fabric.

To disable ARP suppression, use the **no** form of this command.

Examples

The following example enables ARP suppression on a VLAN.

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# suppress-arp
```

The following example enables ARP suppression on a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 2
device(config-bridge-domain-2)# suppress-arp
```

History

Release version	Command history
18x.1.00	This command was introduced.

suppress-nd

Enables Neighbor Discovery (ND) suppression on a VLAN or bridge domain. ND suppression can lessen the amount of ND control traffic within an IP Fabric.

Syntax

suppress-nd

no suppress-nd

Command Default

ND suppression is disabled.

Modes

VLAN configuration mode

Bridge-domain configuration mode

Usage Guidelines

This feature is required, along with ARP suppression, if static anycast gateway is supported in an IP Fabric.

To disable ND suppression, use the **no** form of this command.

Examples

The following example enables ND suppression on a specified VLAN.

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# suppress-nd
```

The following example enables ND suppression on bridge domain 2.

```
device# configure terminal
device(config)# bridge-domain 2
device(config-bridge-domain-2)# suppress-nd
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport

Puts the interface in Layer 2 mode and sets the switching characteristics of the Layer 2 interface.

Syntax

switchport

no switchport

Command Default

All Layer 2 interfaces are mapped to default VLAN 1 and the interface is set to access mode.

Modes

Interface subtype configuration mode

Usage Guidelines

For changing the interface configuration mode to trunk or changing the default VLAN mapping, use additional **switchport** commands.

To redefine the switch from Layer 2 mode into Layer 3 mode, enter **no switchport**.

Examples

To put a specific Ethernet interface in Layer 2 mode:

```
device# configure terminal
switch(config)# interface ethernet 1/9
switch(conf-if-eth-1/9)# switchport
```

To remove a specific port-channel interface from Layer 2 mode:

```
device# configure terminal
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# no switchport
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport access

Sets the Layer 2 interface as access.

Syntax

switchport access { **vlan** *vlan_id* | **rspan-vlan** *vlan_id* | **mac** *HHHH.HHHH.HHHH* | **mac-group** *mac-group-id* }

no switchport access { **vlan** *vlan_id* | **rspan-vlan** *vlan_id* | **mac** *HHHH.HHHH.HHHH* | **mac-group** *mac-group-id* }

Command Default

All Layer 2 interfaces are in access mode and belong to the VLAN ID 1.

Parameters

vlan *vlan_id*
: Sets the port VLAN (PVID) to the specified *vlan_id*. Range is below 4096 for 802.1Q VLANs, and from 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

rspan-vlan *vlan_id*
: Sets a VLAN ID for RSPAN (Remote Switched Port Analyzer) traffic analysis.

mac *HHHH.HHHH.HHHH*
: Sets a source MAC address for classifying an untagged VLAN specified by the **vlan** keyword.

mac-group *mac-group-id*
: (Optional) Specifies a set of MAC addresses. The group of addresses must be established by the global **mac-group** command.

Modes

Interface subtype configuration mode on edge ports

Usage Guidelines

In access mode, the interface only allows untagged and priority tagged packets.

In a Virtual Fabrics context, use this command also to configure service or transport VFs on an access port. This allows multiple untagged VLANs on the port by means of SRC MAC classifiers.

Enter **no switchport access vlan** to set the PVID to the default VLAN 1.

Examples

To set the Layer 2 interface PVID to 100 on a specific Ethernet interface:

```
device# configure terminal
switch(config)# interface ethernet 1/9
switch(conf-if-eth-1/9)# switchport access vlan 100
```

To set the PVID to the default VLAN 1 on a specific port-channel interface:

```
device# configure terminal
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# no switchport access vlan
```

The following examples illustrate configuration with service or transport VFs in a Virtual Fabrics context.

In global configuration mode, establish a mac-group:

```
device# configure terminal
switch(config)# mac-group 1
switch(config-mac-group 1)# mac 0002.0002.0002
switch(config-mac-group 1)# mac 0005.0005.0005
switch(config-mac-group 1)# mac 0008.0008.0008
```

In interface configuration mode, ensure that the switchport mode is set to access:

```
device# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if-eth-1/1)# switchport mode access
```

Set the default access VLAN (the default is 1) to 5000 (a classified VLAN):

```
device# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if-eth-0/1)# switchport access vlan 5000
```

Classify an 802.1Q VLAN by means of a source MAC address:

```
device# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if-eth-1/1)# switchport access vlan 200 mac 0002.0002.0002
```

Configure a classified VLAN (> 4095) on the same interface with a MAC address. Frames that do not match the source MAC addresses of 0002.0002.0002 or 0004.0004.0004 are classified into VLAN 5000 (the access VLAN for all untagged frames that do not have MAC address classifications.

```
device# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if-eth-1/1)# switchport access vlan 6000 mac 0004.0004.0004
```

The following errors occur because a MAC address can be classified to only one VLAN on the same interface.

```
device# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if-eth-1/1)# switchport access vlan 7000 mac-group 1
switch(config-if-eth-1/1)# %Error: Mac-address/Mac-group is overlapping with another Mac-address/Mac-
group configuration on the same port.
switch(config-if-eth-1/1)# switchport mode access
switch(config-if-eth-1/1)# switchport access vlan 7000 mac-group 1
switch(config-if-eth-1/1)# switchport access vlan mac 8000 0008.0008.0008
switch(config-if-eth-1/1)# %Error: Mac-address/Mac-group is overlapping with another Mac-address/Mac-
group configuration on the same port.
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport mode

Sets the mode of the Layer 2 interface.

Syntax

switchport mode { **access** | **trunk** }

Parameters

access

Sets the Layer 2 interface as access. Access mode assigns the port to a VLAN

trunk

Sets the Layer 2 interface as trunk. Trunk mode makes the port linkable to other switches and routers

Modes

Interface subtype configuration mode

Usage Guidelines

You must configure the same native VLAN on both ends of an 802.1 or classified VLAN trunk link. Failure to do so can cause bridging loops and VLAN leaks.

Examples

To set the mode of a specific Ethernet interface to access:

```
device# configure terminal
switch(config)# interface ethernet 1/9
switch(conf-if-eth-1/9)# switchport mode access
```

To set the mode of a specific port-channel interface to trunk:

```
device# configure terminal
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# switchport mode trunk
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport mode trunk-no-default-native

Configures a port to trunk mode without the native vlan.

Syntax

switchport mode trunk-no-default-native

Modes

Interface configuration mode

Usage Guidelines

By assigning this mode, you can configure an untagged logical interface on the specified port. The device discards any ingress tagged or untagged packet until a switchport classification or native VLAN classification is configured.

To disable this functionality, issue the **no switchport** command, or enter a different switchport mode by using the **switchport mode access** command or the **switchport mode trunk** command.

Before you change the switch port mode from **switchport mode access** with an explicit **switchport access vlan** to **switchport mode trunk-no-default-native**, you must enter the **no switchport** command on the interface level, and then enter the **switchport** command to set the interface as a switchport. Now you can configure the **switchport mode trunk-no-default-native** command.

Port mode change is not allowed when port security is enabled on the interface.

This is the fundamental difference between this command and the **switch mode trunk** command, which implicitly creates VLAN 1 on the port.

The global command **dot1q tag native-vlan** does not affect the ingress or egress tagging behavior of the native VLAN configured in this mode.

The following native VLAN commands that are supported in regular trunk mode are NOT supported in this mode:

- **switchport trunk tag native-vlan**
- **switchport trunk native-vlan**

Examples

The following example configures a trunk port without a default native VLAN, then explicitly configures the native VLAN.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# switchport mode trunk-no-default-native
device(config-if-eth-0/1)# switchport trunk tagged
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport port-security

Enables port security on an interface port.

Syntax

switchport port-security

no switchport port-security

Command Default

Port security is not enabled.

Modes

Interface configuration mode

Usage Guidelines

Port mode change is not allowed when port security is enabled on the interface.

The **no switchport port-security** command disables port security on the interface.

Examples

The following example enables port MAC security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport port-security mac-address

Configures the MAC address option for port security on an interface port.

Syntax

switchport port-security mac-address *address* **vlan** *vlan_id*

Command Default

MAC address is not configured for port security.

Parameters

mac-address *address*

Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

vlan *vlan_id*

Specifies a VLAN.

Modes

Interface configuration mode

Usage Guidelines

Static MAC addresses cannot be configured on a secure port. They must be configured as secure MAC addresses on the secure port.

When static MAC address is configured on an access secure port, the MACs qualify for access VLANs, but on trunk port, VLAN must be specified.

The **no switchport port-security mac-adress** command removes the specified MAC address.

Examples

The following example configures static MAC address for port security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security mac-address 0000.00eb.2d14 vlan 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport port-security max

Configures the maximum number of MAC addresses used for port MAC security on an interface port.

Syntax

switchport port-security max *value*

no switchport port-security max

Parameters

value

The maximum number of secure MAC addresses. Range is from 1 through 8192.

Command Default

The default value is 8192 MAC addresses.

Modes

Interface configuration mode

Usage Guidelines

The maximum MAC address limit for sticky MAC address and static MAC address depends on the device limit. For dynamically learned MAC addresses, the maximum limit is 8192 per port.

The **no switchport port-security max** command restores the default value of maximum number of MAC addresses.

Examples

The following example configures the maximum number of MAC addresses used for port MAC security on an interface port as 10:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security max 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport port-security shutdown-time

Configures the auto recovery time for ports that shuts down following a port security violation on an interface.

Syntax

switchport port-security shutdown-time *time*

Command Default

Auto recovery of ports is not enabled.

Parameters

time

The amount of time in minutes, the port waits before it recovers from forced port shutdown. Range is from 1 through 15.

Modes

Interface configuration mode

Usage Guidelines

The shutdown and no-shutdown processes initiated as part of the port violation action is independent of the shutdown process explicitly initiated by an administrator on the same port on which port MAC security is enabled.

If a port security-based change occurs when a port is shut down, the shutdown timer is not triggered. Consequently, the user must restore the full functionality of the port.

When port security violation causes a port to be shut down and the user manually changes the shutdown time, the shutdown timer is reset and the timer starts with the new shutdown time.

The **no switchport port-security shutdown-time** command disables the auto recovery functionality.

Examples

The following example configures the auto recovery time as 4 minutes for ports that shuts down following a port security violation on an interface.

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security shutdown-time 4
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport port-security sticky

Enables sticky MAC learning on the port to convert the dynamically learned MAC addresses to sticky secure MAC addresses.

Syntax

switchport port-security sticky [**mac-address** *address* **vlan** *vlan_id*]

no switchport port-security sticky [**mac-address** *address* **vlan** *vlan_id*]

Command Default

Sticky MAC learning on the port is not enabled.

Parameters

mac-address *address*

Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

vlan *vlan_id*

Specifies a VLAN.

Modes

Interface configuration mode

Usage Guidelines

When sticky MAC learning is enabled on a secured port, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All the subsequent sets of dynamically learned MAC addresses will also be converted to sticky secure MAC addresses.

The **no switchport port-security sticky** disables sticky MAC learning on a secure port, and all the sticky MAC addresses will be converted back to dynamically learned MAC addresses.

Sticky MAC addresses persist even if the port goes down or if the device reboots.

Examples

The following example enables sticky MAC learning on the port and configures port security with sticky MAC address:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security sticky
device(conf-if-eth-3/2)# switchport port-security sticky mac-address 0000.0018.747C vlan 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport port-security violation

Configures the violation response action for port security on an interface.

Syntax

switchport port-security violation shutdown

Command Default

The port shuts downs if port security violation occurs.

Parameters

shutdown

Puts the interface into the error-disabled state.

Modes

Interface configuration mode

Usage Guidelines

If a MAC address already learned on a secured port ingresses on a non-secured port or through another secured port, it is not considered security violation. In this scenario, MAC movement happens if it is a dynamically learned MAC address. If it is a static MAC address or sticky MAC address, MAC movement does not happen, but the traffic is switched (flooded or forwarded) based on the destination MAC address.

If the port shuts down after security violation, an administrator can explicitly bring up the interface or a shutdown timer can be configured using the **switchport port-security shutdown-time** command. After the configured shutdown time, the interface automatically comes up and the port security configuration remains configured on the port.

When the device reboots after port shutdown due to security violation, the ports come up in the shutdown state.

Examples

The following example configures the violation response action as shutdown for port security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security violation shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport trunk allowed

Adds or removes VLANs on a Layer 2 interface in trunk mode.

Syntax

switchport trunk allowed { **vlan** | **rspan-vlan** } { **add** *vlan_id* { **ctag** { *id* | *ctag* **-** *range* } | **all** | **except** *vlan_id* | **none** | **remove** *vlan_id* }

Parameters

add *vlan_id*
Adds a VLAN to transmit and receive through the Layer 2 interface. The VLAN can be an 802.1Q VLAN, an RSPAN VLAN, or a transport VLAN.

all
Allows only 802.1Q VLANs to transmit and receive through the Layer 2 interface. This keyword does not apply to classified or transport VLANs.

ctag
Specifies an incoming C-TAG or range of C-TAGs for classified or transport VLANs.

id
C-TAG ID.

range
Range of C-TAG IDs, for example, 100-200, or 10,20,100-200, applicable only if the VLAN is a transport VLAN.

except *vlan_id*
Allows only 802.1Q VLANs except the specified VLAN ID to transmit and receive through the Layer 2 interface.

none
Allows only 802.1Q VLANs to transmit and receive through the Layer 2 interface. This keyword does not apply to service or transport VFs.

rspan-vlan *vlan_id*
Selects a VLAN for Remote Switched Port Analyzer (RSPAN) traffic monitoring.

remove *vlan_id*
Removes a VLAN that transmits and receives through the Layer 2 interface.

Modes

Interface subtype configuration mode

Usage Guidelines

A transport VF C-TAG can be any VLAN ID that is not used in other classifications or as a 802.1Q VLAN.

Examples

To add the tagged VLAN 100 to a specific Ethernet interface:

```
device# configure terminal
switch(config)# interface ethernet 0/9
switch(conf-if-eth-0/9)# switchport trunk allowed vlan add 100
```

To remove the tagged VLAN 100 from the interface:

```
device# configure terminal
switch(config)# interface ethernet 0/9
switch(conf-if-eth-0/9)# switchport trunk allowed vlan remove 100
```

Configure a classified VLAN with a C-TAG:

```
device# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if-eth-0/1)# switchport trunk allowed vlan add 5000 ctag 100
switch(config-if-eth-0/1)# switchport trunk allowed vlan add 6000 ctag 200
```

An 802.1Q vlan specified as a user VLAN cannot be used as a C-TAG in a classified VLAN. The following show conflicts.

- Edge C-TAG 100 is already assigned to VLAN 5000 at the same port:

```
device# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if-eth-0/1)# switchport trunk allowed vlan add 8000 ctag 100
switch(config-if-eth-0/1)# %Error: C-tag is already used.
```

- Edge VLAN 888 was already used in 802.1Q configuration.

```
device# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if-eth-0/1)# switchport trunk allowed vlan add 8000 ctag 888
switch(config-if-eth-0/1)# %Error: Ctag is configured in the allowed range on this port.
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport trunk native-vlan-untagged

Configures a port to accept only untagged packets, and specifies that those packets be egress untagged. The untagged packets may be classified to an 802.1Q VLAN, a service VF, or a transport VF.

Syntax

switchport trunk native-vlan-untagged *vlan_id*

no switchport trunk native-vlan-untagged

Parameters

vlan_id

Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface.

Modes

Interface subtype configuration mode on a trunk port

Usage Guidelines

This command is supported when the port is in no-default-vlan trunk mode, as enabled by means of the **switchport mode trunk-no-default-native** command.

Use the **no switchport trunk native-vlan-untagged** command to remove the configuration.

Port mode change is not allowed when port security is enabled on the interface.

Examples

Configure untagged native VLAN 5000, allow VLAN 6000, and make VLAN 7000 the default VLAN.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# switchport mode trunk-no-default-native
device(config-if-eth-0/1)# switchport trunk native-vlan untagged 5000
device(config-if-eth-0/1)# switchport trunk add vlan 6000 ctag 100-200
device(config-if-eth-0/1)# switchport trunk default-vlan 7000
```

Remove the native VLAN 5000.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# no switchport trunk native-vlan-untagged
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport trunk native-vlan-xtagged

Configures a port to accept both tagged and untagged packets, and specifies the egress tagging behavior.

Syntax

switchport trunk native-vlan-xtagged *vlan_id* [**ctag** *cvid*] **egress** { **tagged** | **untagged** | **any** }

no switchport trunk native-vlan-xtagged

Parameters

vlan_id
: Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface.

ctag *cvid*
: Sets an optional C-TAG (802.1Q VLAN ID) for a service or transport VF (VLAN ID > 4095).

egress
: Enables the selection of required tagging options.

  tagged
  : Specifies packets as tagged.

  untagged
  : Specifies packets as untagged.

  any
  : Specifies that packets preserve their ingress encapsulation.

Modes

Interface subtype configuration mode on a trunk port

Usage Guidelines

This command is supported when the port is in no-default-vlan trunk mode, as enabled by means of the **switchport mode trunk-no-default-native** command.

Note the following:

- Ingress packets may be classified to an 802.1Q VLAN, a service VF, or a transport VF.
- The native VLAN must accept tagged frames for the **ctag** keyword to apply.
- If the specified VLAN is an 802.1Q VLAN, the **ctag** option is not required.
- If the specified VLAN is an 802.1Q VLAN or a service VF, the **egress** tagging options are **tagged** or **untagged**.
- If the specified VLAN is a transport VF, then the **egress** tagging option must be **any** to preserve the encapsulation of ingress frames.

Use the **no switchport trunk native-vlan-xtagged** command to remove the configuration.

Port mode change is not allowed when port security is enabled on the interface.

Examples

Configure transport VF 6000 that accepts C-TAG range 100 through 200 and a native VLAN that can be either tagged or untagged.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# switchport mode trunk-no-default-native
device(config-if-eth-0/1)# switchport trunk native-vlan-xtagged 6000 ctag 10 egress any
device(config-if-eth-0/1)# switchport trunk allow vlan 6000 ctag 100-200
```

Remove the native VLAN from the transport VF.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# no switchport trunk native-vlan-xtagged
```

History

Release version	Command history
18x.1.00	This command was introduced.

switchport trunk tag native-vlan

Enables tagging on native VLAN traffic.

Syntax

switchport trunk tag native-vlan

no switchport trunk tag native

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no switchport trunk tag native** to untag native traffic for a specific interface.

Examples

To enable tagging for native traffic on a specific Ethernet interface:

```
device# configure terminal
switch(config)# interface ethernet 0/9
switch(conf-if-eth-0/9)# switchport trunk tag native-vlan
```

History

Release version	Command history
18x.1.00	This command was introduced.

sync-interval

Configures the interval between Precision Time Protocol (PTP) synchronization (Sync) messages on an interface.

Syntax

sync-interval *seconds*

no sync-interval

Command Default

See Parameters.

Parameters

seconds

Interval between PTP Synch messages, in log seconds. Range is -4 through 2. The default is -1 (2 packets/second). See the Usage Guidelines. Range is -4 through 2. The default is -1 (2 packets/second).

Modes

PTP configuration mode

Interface subtype configuration mode

Usage Guidelines

The inputs for **interval** represent base 2 exponents, where the packet rate is $1/(2^{\log \text{seconds}})$.

Configuring this interval on an edge port overrides the switch (global) default.

ATTENTION
Do not configure a rate slower than the default on links between SLX devices.

Use the **no** form of this command to revert to the default.

Examples

To configure a PTP Sync interval of 2 on an Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# protocol ptp
device(conf-if-eth-0/1-ptp)# sync-interval 2
```

To revert to the default PTP Sync interval of -1:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# protocol ptp
device(conf-if-eth-0/1-ptp)# no sync-interval
```

History

Release version	Command history
18x.1.00	This command was introduced.

sysmon fe-acces-check

Configures system error monitoring.

Syntax

sysmon fe-access-check [**action** | **disable** | **poll-interval** | **recovery-threshold** | **threshold**]

Parameters

action
Sets Fe-Access-Check action.

disable
Disables the Fe Access Check.

poll-interval
Sets the Fe-Access-Check poll-interval.

recovery-threshold
Sets the Fe-Access-Check recovery threshold.

threshold
sets the Fe-Access-Check threshold.

Modes

Global configuration mode

Usage Guidelines

By default, the Fe access check is disabled. The default recovery threshold is 1 and the default threshold is 3. The default action is log, which logs the FE acces errors.

Examples

```
device(config)# sysmon fe-access-check ?
Possible completions:
  action               Set Fe-Access-Check action
  disable              Disable Fe Access Check (Default: Enabled)
  poll-interval        Set Fe-Access-Check poll-interval
  recovery-threshold   Set Fe-Access-Check recovery threshold
  threshold            Set Fe-Access-Check threshold
device(config)# sysmon fe-access-check recovery-threshold ?
Possible completions:
  <1-3>   Default: 1
device(config)# sysmon fe-access-check recovery-threshold 2
device(config)# sysmon fe-access-check threshold?
Possible completions:
  threshold   Set Fe-Access-Check threshold
device(config)# sysmon fe-access-check threshold ?
Possible completions:
  <1-10>   Default: 3
device(config)# sysmon fe-access-check threshold 5
device(config)# sysmon fe-access-check action ?
Possible completions:
  log       Log FE access error (Default action)
  recover   Recover FE
device(config)# sysmon fe-access-check action log ?
Possible completions:
  <cr>
device(config)# sysmon fe-access-check action log?
Possible completions:
  log   Log FE access error (Default action)
device(config)# sysmon fe-access-check recover ?
Possible completions:
<1-3>  Default is 1
device(config)# sysmon fe-access-check recover 2
```

History

Release version	Command history
18x.1.00	This command was introduced.

sysmon link-crc-monitoring

Enables link CRC monitoring.

Syntax

sysmon sfm-walk [**auto** | **disable-redundancy-check** | **poll-interval** | **threshold**]

Parameters

action

Sets Link CRC Monitoring actions.

disable

Disables link CRC Monitoring.

poll-interval

Sets link CRC monitoring poll-interval.

threshold

Sets link CRC Monitoring threshold.

Modes

Global configuration mode

Usage Guidelines

By default, link-crc monitoring is disabled. Default threshold is 5 and default poll-interval is 60 seconds.

Examples

```
device(config)# sysmon link-crc-monitoring ?
Possible completions:
  action          Set Link CRC Monitoring action
  disable         Disable Link CRC Monitoring (Default: Enabled)
  poll-interval   Set Link CRC Monitoring poll-interval
  threshold       Set Link CRC Monitoring threshold
device(config)# sysmon link-crc-monitoring threshold ?
Possible completions:
  <1-10>   Default: 5
device(config)# sysmon link-crc-monitoring threshold 9
device(config)# sysmon link-crc-monitoring poll-interval ?
Possible completions:
  <1-300>   Default: 60 Sec
device(config)# sysmon link-crc-monitoring poll-interval 500
```

History

Release version	Command history
18x.1.00	This command was introduced.

sysmon sfm-walk

Enables SFM walk.

Syntax

sysmon sfm-walk [**auto** | **disable-redundancy-check** | **poll-interval** | **threshold**]

Parameters

auto
Enable auto SFM walk.

disable-redundancy-check
Disables SFM Walk redundancy check.

poll-interval
Sets SFM Walk poll-interval.

threshold
Sets SFM Walk reassembly error threshold.

Modes

Global configuration mode

Usage Guidelines

By default, SFM walk and redundancy check are disabled.

Examples

```
device(config)# sysmon sfm-walk ?
Possible completions:
  auto                        Enable Auto SFM Walk (Default: Disabled)
  disable-redundancy-check    Disable SFM Walk redundancy check (Default:
                              Enabled)
  poll-interval               Set SFM Walk poll-interval
  threshold                   Set SFM Walk reassembly error threshold
device(config)# sysmon sfm-walk auto?
Possible completions:
  auto   Enable Auto SFM Walk (Default: Disabled)
device(config)# sysmon sfm-walk auto ?
Possible completions:
  <cr>
device(config)# sysmon sfm-walk disable-redundancy-check?
Possible completions:
  disable-redundancy-check    Disable SFM Walk redundancy check (Default:
                              Enabled)
device(config)# sysmon sfm-walk disable-redundancy-check ?
Possible completions:
  <cr>
device(config)# sysmon sfm-walk poll-interval?
Possible completions:
  poll-interval   Set SFM Walk poll-interval
device(config)# sysmon sfm-walk poll-interval ?
Possible completions:
  <1-600>   Default: 30 Sec
SLX(config)# sysmon sfm-walk poll-interval 500
The Client sysmgr is not Known or Connected
```

History

Release version	Command history
18x.1.00	This command was introduced.

system-description

Sets the global system description specific to LLDP.

Syntax

system-description *line*

no system-description

Parameters

line

Specifies a description for the LLDP system. The string must be between 1 and 50 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no system-description** to clear the global LLDP system description.

Examples

To set the global system description specific to LLDP on the SLX-OS platform, enter the following:

```
device(conf-lldp)# system-description SLXR
```

History

Release version	Command history
18x.1.00	This command was introduced.

system-monitor tm

Accesses system monitor traffic manager (sys-mon TM) configuration mode to configure the monitoring of the traffic manager (TM) device or Virtual Output Queue (VOQ) discarded packets.

Syntax

system-monitor tm

no system-monitor tm

Modes

Global configuration mode

Usage Guidelines

By default, the monitoring of the TM device and VOQ discarded packets is disabled until you configure their threshold.

Use the **no** form of this command to reset the monitoring of the TM device and VOQ discarded packets configurations to their default values and disable the monitoring of the packets.

Examples

The following example enables VOQ discarded packets monitoring and accesses sys-mon TM configuration mode.

```
device# configure terminal
device (config)# system-monitor tm
device (config-sys-mon-tm)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

system-monitor-mail

Configures various email settings as part of system monitoring.

Syntax

system-monitor-mail [**fru** | **interface** | **relay** | **security** |**sfp**]

Parameters

fru

Configure FRU mail settings.

interface

Configure interface mail settings.

relay

Configure relay ip mail settings.

security

Cconfigure security mail settings.

sfp

Configure sfp mail settings.

Modes

Global configuration mode

Examples

```
device(config)# system-monitor-mail ?
Possible completions:
  fru         Configure FRU mail settings
  interface   Configure interface mail settings
  relay       Configure relay ip mail settings
  security    Configure security mail settings
  sfp         Configure sfp mail settings
device(config)# system-monitor-mail fru ?
Possible completions:
  <email:string>  e-mail address for FRU alerts
  enable   Enable FRU email alerts
device(config)# system-monitor-mail fru enable ?
Possible completions:
  <cr>
device(config)# system-monitor-mail fru enable?
Possible completions:
  enable   Enable FRU email alerts
device(config)# system-monitor-mail fruemail ?
                                   ^
% Invalid input detected at '^' marker.
device(config)# system-monitor-mail fru email ?
Possible completions:
  <cr>
device(config)# system-monitor-mail fru ncp@extreme.com
device(config)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

system-monitoring power alert state removed action raslog

Monitors the power supply component and generates RASLog when the component changes from the configured state.

Syntax

system-monitoring power alert state removed action raslog

Parameters

Alert

Configures alerts for the POWER SUPPLY component.

State

Specifies the supported states for component (power supply) that may be monitored.

action

Specifies the action that may be taken when component (power supply) changes from the configured state.

Modes

Global configuration mode

Examples

```
device(config)# system-monitor power ?
Possible completions:
  alert       Configure alerts for component:POWER SUPPLY
  threshold   Configure threshold for component:POWER SUPPLY
device(config)# system-monitor power alert ?
Possible completions:
  action   Action that may be taken when component:POWER SUPPLY changes
           configured state
  state    Supported states for component: POWER-SUPPLY that may be monitored
device(config)# system-monitor power alert state ?
Possible completions:
  [removed]  all  faulty  inserted  none  on  removed
device(config)# system-monitor power alert state removed ?
Possible completions:
  action   Action that may be taken when component:POWER SUPPLY changes
           configured state
  <cr>
device(config)# system-monitor power alert state removed action ?
Possible completions:
  [raslog]  all  email  none  raslog
device(config)# system-monitor power alert state removed action raslog ?
Possible completions:
  <cr>
device(config)# system-monitor power alert state removed action raslog
```

History

Release version	Command history
18x.1.00	This command was introduced.

system power-cycle-db-shutdown

Shuts down the chassis configuration database gracefully without restarting the device for a planned power-cycle.

Syntax

system power-cycle-db-shutdown

Command Default

The chassis configuration database is running normally.

Modes

Global configuration mode

Usage Guidelines

When devices encounter abrupt power cycles, there have been rare cases of device configuration database corruption. This database corruption causes the device to reboot and reverts the device to the startup configuration.

In the case of scheduled power-cycles, it is recommended to use the **system power-cycle-db-shutdown** command before actual restarting the device.

This command shuts down the chassis configuration database, without rebooting the device. All commands (except for the **reload** command) are blocked on this node until the node is restarted. The node also informs its HA-peer to shut-down its database gracefully and not handle any database requests henceforth.

NOTE

Suppose the configuration database on a switch gets corrupted due to an abrupt power cycle, run the **firmware install** or the **write erase** commands to clean up the corrupted files and/or to reinstall the firmware.

The node is not fully functional until it restarts. This command should be run as part of any planned power outages.

Examples

```
device# configure terminal
device(config)# system power-cycle-db-shutdown
Are you sure you want to shutdown database for power-cycle? [y/n]: y
2017/02/09-13:02:42, [DCM-1015], 51,, INFO, SLX9140, Switch is prepared for power-cycle. No clis will
work henceforth. Need power-cycle or reload to make switch fully functional.
Operation Successful.
```

History

Release version	Command history
18x.1.00	This command was introduced.

system-name

Sets the global system name specific to LLDP.

Syntax

system-name *name*

no system-name

Command Default

The host name from the device is used.

Parameters

name

Specifies a system name for the LLDP. The string must be between 1 and 32 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no system-name** to delete the name.

Examples

To specify a system name for the LLDP:

```
device(conf-lldp)# system-name System10
```

History

Release version	Command history
18x.1.00	This command was introduced.

table-map

Maps external entry attributes into the BGP routing table, ensuring that those attributes are preserved after being redistributed into OSPF.

Syntax

table-map *string*

no table-map *string*

Command Default

This option is disabled.

Parameters

string

Specifies a route map to be whose attributes are to be preserved. Range is from 1 through 63 ASCII characters.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to remove the table map.

Use this command only to set the tag values. Normally, a route map is applied on routes (and therefore the routes are updated) before it is stored in the BGP routing table. Use the **table-map** command to begin the update before the routes are stored in the IP routing table.

Configurations made by this command apply to all peers.

Route maps that contain **set** statements change values in routes when the routes are accepted by the route map. For inbound route maps (route maps that filter routes received from neighbors), the routes are changed before they enter the BGP routing table. For tag values, if you do not want the value to change until a route enters the IP routing table, you can use a table map to change the value. A table map is a route map that you have associated with the IP routing table. The device applies the **set** statements for tag values in the table map to routes before adding them to the routing table. To configure a table map, you first configure the route map, then identify it as a table map. The table map does not require separate configuration. You can have only one table map.

NOTE

Use table maps only for setting the tag value. Do not use table maps to set other attributes. To set other route attributes, use route maps or filters. To create a route map and identify it as a table map, enter commands such those shown in the first example below. These commands create a route map that uses an address filter. For routes that match the IP prefix list filter, the route map changes the tag value to 100 and is then considered as a table map. This route map is applied only to routes that the device places in the IP routing table. The route map is not applied to all routes. The first example below assumes that IP prefix list p11 has already been configured.

Examples

This example illustrates the execution of the **table-map** command.

```
device# configure terminal
device(config)# route-map tag_ip permit 1
device(config-route-map/tag_ip/permit/1)# match ip address prefix-list p11
device(config-route-map/tag_ip/permit/1)# set tag 100
device(config-route-map/tag_ip/permit/1)# exit
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# table-map tag_ip
```

This example removes the table map for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# no table-map tag_ip
```

This example removes the table map for VRF “red”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# no table-map tag_ip
```

History

Release version	Command history
18x.1.00	This command was introduced.

tacacs-server

Configures a Terminal Access Controller Access-Control System plus (TACACS+) server.

Syntax

tacacs-server { **host** *hostname* [**use-vrf** *vrf-name*]

tacacs-server { **source-ip** [*chassis-ip* | *mm-ip*] }

[**port** *portnum*]

[**protocol** { **chap** | **pap** }]

[**key** *shared_secret*]

[**encryption-level** *value_level*]

[**timeout** *secs*]

[**retries** *num*]

no tacacs-server { **host** *hostname* | **source-ip** [*chassis-ip* | *mm-ip*] } [**use-vrf** *vrf-name*]

Command Default

Refer to the Parameters section for specific defaults.

Parameters

host hostname
Specifies the IP address or domain name of the TACACS+ server. IPv4 and IPv6 addresses are supported.

use-vrf *vrf-name*
Specifies a VRF though which to communicate with the TACACS+ server. See the Usage Guidelines.

tacacs-server source-ip [**chassis-ip** | **mm-ip**]
Specifies the chassis IP address or MM IP address as the source IP address for TACACS+ authentication and accounting.

port *portnum*
Specifies the authentication port. Valid values range from 0 through 65535. The default is 49.

protocol { *chap* | *pap* }
Specifies the authentication protocol. Options include CHAP and PAP. The default is CHAP.

key *shared_secret*
Specifies the text string that is used as the shared secret between the device and the TACACS+ server to make the message exchange secure. The key must be between 1 and 40 characters in length. The default key is **sharedsecret** . The exclamation mark (!) is supported both in RADIUS and TACACS+ servers, and you can specify the password in either double quotes or the escape character (\), for example **"secret!key"** or **secret\!key**. The only other valid characters are alphanumeric characters (such as a-z and 0-9) and underscores. No other special characters are allowed.

encryption-level *value_level*

Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The valid values are 0 and 7, with 0 being clear text and 7 being the most heavily encrypted. The default value is 7.

timeout *secs*

Specifies the time to wait for the TACACS+ server to respond. The default is 5 seconds.

retries *num*

Specifies the number of attempts allowed to connect to a TACACS+ server. The default is 5 attempts.

Modes

Global configuration mode

Usage Guidelines

If a TACACS+ server with the specified IP address or host name does not exist, it is added to the server list. If the TACACS+ server already exists, this command modifies the configuration. The **key** parameter does not support an empty string.

Executing the **no** form of the **tacacs-server** command attributes resets the specified attributes to their default values.

NOTE

Before downgrading to a software version that does not support the **encryption-level** keyword, set the value of this keyword to **0**. Otherwise, the firmware download will throw an error that requests this value be set to **0**.

Before downgrading to a version that doesn't support **tacacs-server source-ip**, you must remove the source-ip configuration using **no tacacs-server source-ip**. Otherwise, the firmware download process throws an error requesting to reset the cipher.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

To configure an IPv4 TACACS+ server:

```
device# configure terminal
device(config)# tacacs-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# tacacs-server source-ip chassis-ip
device(config-host-10.24.65.6/mgmt-vrf)# protocol chap retries 100
device(config-host-10.24.65.6/mgmt-vrf)#
```

To modify an existing TACACS+ server configuration:

```
device# configure terminal
device(config)# tacacs-server host 10.24.65.6
device(config-tacacs-server-10.24.65.6/mgmt-vrf))# key "changedsec"
```

To delete a TACACS+ server:

```
device# configure terminal
device(config)# no tacacs-server host 10.24.65.6
```

To configure an IPv6 TACACS+ server:

```
device# configure terminal
device(config)# tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)# protocol chap key "mysecret"
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)#  tacacs-server source-ip
chassis-ip
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

tag-type

Configures TPID for the specified interface.

Syntax

tag-type *tp-id*

no tag-type *tp-id*

Parameter:

tp-id

Specifies the TPID. A test profile name can be can be a maximum of 32 characters .

Command Default

The default TPID value is 0x8100.

Modes

Interface configuration mode

Usage Guidelines

The interface can be a port or a port-channel (LAG).

Use the **no** form of the command to revert to the default TPID value.

The TPID feature has the following limitations:

- **AVT profile limitation**: Because of the limited number of AVT profiles (ingress and egress), the support for TPID configuration is available for the outer TPID of the packet without reducing the number of AVT profiles. When a packet is dual tagged, the inner TPID that is supported and recognized is TPID 0x8100.
- **System maximum TPID**: Hardware allows up to only four TPID configurations. The TPID can be any user-defined value. However, the inner TPID for a dual-tagged packet must be 0x8100, which means you can configure only three additional TPIDs in a system. TPID 0x8100 is the default value for all interfaces until you change it by means of the **tag-type** command.

  ATTENTION
  When the tag type is changed on interface, the interface is brought down first, causing all learned MAC addresses to be flushed.

Examples

This example shows how to configure a nondefault TPID on an Ethernet interface.

```
device# configure terminal
device(config)# inteface ethernet 1/1
device(conf-if-eth-1/1)# tag-type 0x9100
```

This example shows how to revert to the default TPID value.

```
device# configure terminal
device(config)# inteface ethernet 1/1
device(conf-if-eth-1/1)# no tag-type
```

This example shows how to configure a nondefault TPID on a port-channel interface.

```
device# configure terminal
device(config)# inteface port-channel 10
device(config-Port-channel-10)# tag-type 0x88a8
```

History

Release version	Command history
18x.1.00	This command was introduced.

telemetry client-cert

Generates the SSL certificate used by Telemetry server and client for a secure connection.

Syntax

telemetry client-cert { **generate** | **delete** }

Command Default

There is no SSL certificate.

Parameters

generate

Generates the certificate

delete

Deletes the certificate.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **telemetry client-cert delete** to delete the SSL certificate for Telemetry server and clients.

Examples

Typical command execution example.

```
device# telemetry client-cert generate
```

History

Release version	Command history
18x.1.00	This command was introduced.

telemetry collector

Activates Telemetry collector configuration mode.

Syntax

telemetry collector { *telemetry-collector-name* }

Command Default

Telemetry collector configuration mode is deactivated.

Parameters

telemetry-collector-name

A unique name for a Telemetry collector. The name can be a string of up to 32 characters, consisting of letters, digits, and the underscore.

Modes

Global configuration mode

Usage Guidelines

Update operations are allowed only when telemetry collector is in deactivated ("no activate") state.

Examples

Typical command example for activating Telemetry collector configuration mode.

```
device# configure terminal
device(config)# telemetry collector collector_1
device(config-telemetry-collector_collector_1)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

telemetry profile

Enters telemetry-profile configuration mode.

Syntax

telemetry profile interface default_interface_statistics

telemetry profile system-utilization default_system_utilization_statistics

Command Default

The Telemetry profile configuration mode is deactivated.

Parameters

interface default_interface_statistics
Accesses configuration mode for profile **default_interface_statistics** of the **interface** profile type.

system-utilization default_system_utilization_statistics
Accesses configuration mode for profile **default_system_utilization_statistics** of the **system-utilization** profile type.

Modes

Global configuration mode

Usage Guidelines

If a telemetry profile has no attributes, no information is streamed to the collector.

The **no** option is not supported for this command.

The interface statistics gathered by the default_interface_statistics profile are:

- In/Out packets
- In/Out unicast packets
- In/Out broadcast packets
- In/Out multicast packets
- In/Out packets per second
- In/Out octets
- In/Out errors
- In/Out CRC errors
- In/Out discards

The system utilization statistics gathered by the default_system_utilization_statistics profile are:

- Total system memory
- Total used memory
- Total free memory

- Cached memory
- Buffers
- User free memory
- Kernel free memory
- Total swap memory
- Total free swap memory
- Total used swap memory
- User process
- System process
- Niced process
- Io wait
- Hw interrupt
- Sw interrupt
- Idle state
- Steal time
- Uptime

Examples

Example of entering telemetry profile configuration mode.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

telemetry server

Activates Telemetry server configuration mode.

Syntax

telemetry server

Command Default

Telemetry server configuration mode is deactivated.

Modes

Global configuration mode

Usage Guidelines

Update and No operations are allowed only when telemetry server is in deactivated ("no activate") state.

Examples

Typical command example for activating Telemetry server configuration mode.

```
device# configure terminal
device(config)# telemetry server
device(config-server-mgmt-vrf)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

telnet

Establishes a Telnet session to a remote networking device.

Syntax

telnet *IP_address* [**port-number** *port_number*] [**vrf** *name*]

telnet *hostname* } [**port-number** *port_number*] [**interface** { **ethernet** *slot/port* } | **management** | {**ve** *number* }] [**vrf** *name*]

Command Default

The default port is 23.

Parameters

IP_address
The server IP address in either IPv4 or IPv6 format.

port-number *port*
Specifies the port number in the remote device to connect to. Range is from 0 through 65535. For the connection to succeed, a TCP server must be listening for client connections at the specified port.

vrf *vrf-name*
Specifies a VRF instance. See the Usage Guidelines.

hostname
Specifies the host name which is a string between 1 and 63 ASCII characters in length.

port-number *port*
Specifies the port number in the remote device to connect to. Range is from 0 through 65535. For the connection to succeed, a TCP server must be listening for client connections at the specified port.

interface
Specifies an interface.

ethernet *slot/port*
Specified the Ethernet interface slot and port number.

management
Specifies a management interface.

ve *VE-id*
Specifies the VE interface number.

Modes

Privileged EXEC mode

Usage Guidelines

You can override the default port. However, the device must be listening on this port for the connection to succeed.

The following features are not supported:

- Display Telnet sessions
- Ability to terminate hung Telnet sessions

Examples

The following example establishes a Telnet connection to a remote device.

```
device# telnet 10.20.51.68 vrf mgmt-vrf
```

History

Release version	Command history
18x.1.00	This command was introduced.

telnet server

Configures the Telnet server on the device.

Syntax

telnet server [**use-vrf** *name*] **shutdown**

no telnet server { [**use-vrf** *name*] **shutdown**}

Command Default

The Telnet service is enabled by default.

Parameters

standby enable
Enables the Telnet server on the standby management module (MM).

use-vrf *name*
Specifies a user-defined VRF.

shutdown
Disables the Telnet server.

Modes

Global configuration mode

Usage Guidelines

Shutting down the Telnet service forcibly disconnects all Telnet sessions running on a device.

When you use the **telnet server shutdown** command without a user-defined VRF, the service is shut down on mgmt-vrf only.

Telnet services are associated and started on mgmt-vrf and default-vrf.

Telnet server can be enabled on a maximum number of six VRFs.

Examples

The following example shuts down the Telnet server on the device.

```
device# configure terminal
device(config)# telnet server shutdown
```

History

Release version	Command history
18x.1.00	This command was introduced.

terminal

Sets terminal parameters for the current session.

Syntax

terminal length *lines*

terminal monitor

terminal no length

terminal timeout *seconds*

no terminal { **monitor** | **timeout** }

Command Default

The terminal length is 24 lines.

The terminal timeout is 600 seconds (10 minutes).

Parameters

length *number_of_lines*
Specifies the number of lines to be displayed. Valid values range from 1 through 512. Specify 0 for infinite length.

monitor
Enables terminal monitoring.

timeout *seconds*
Specifies the timeout value in minutes. Enter an integer from 1 to 8192. Specify 0 to disable the timeout.

Modes

Privileged EXEC mode

Usage Guidelines

The **timeout** overrides the timeout configuration set by the **line vty exec-timeout** command, but only for the duration of the current session. When the current session ends, the configured values apply for any subsequent sessions.

Even if other keys are pressed during the timeout period, the only keystroke that prevents logout is **Enter**.

This command is not available on the standby management module.

To reset the default timeout, use the **no terminal timeout** command.

To disable monitoring, use the **no terminal monitor** command.

To reset the default number of displayed lines, use the **terminal no length** command.

Examples

The following example sets the display length to 30 lines.

```
device# terminal length 30
```

The following example sets timeout length to 3600 seconds (60 minutes).

```
device# terminal timeout 3600
```

The following example restores the session timeout setting its default value of 600 seconds (10 minutes).

```
device# no terminal timeout
```

History

Release version	Command history
18x.1.00	This command was introduced.

test-profile

Creates a test profile.

Syntax

test-profile *test-profile-name*

no test-profile

Parameter:

test-profile-name

Specifies the test profile name. A test profile name can be can be a maximum of 32 characters .

Command Default

This feature is disabled.

Modes

Y.1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the corresponding configured test profile and also its associations with Source and Target MEP pair.

Examples

This example shows how to create a test profile .

```
device# configure terminal
device(config)# protocol cfm
device((protocol-cfm)# test-profile my_test_profile
```

History

Release version	Command history
18x.1.00	This command was introduced.

threshold

Specifies if the measurement exceeds the configured average or max threshold value.

Syntax

threshold { **forward** | **backward** } | { **average** *value* | **max** *value* }

no threshold

Command Default

Parameters

forward
Defines the forward direction.

backward
Defines the backward direction.

average *value*
Defines the average value.

max *value*
Defines the maximum value.

Modes

Y.1731 configuration mode

Usage Guidelines

The **threshold** command specifies if the measurement exceeds the configured average or max threshold value in the backward or forward direction, then Syslogs or SNMP traps need to generated..

The **average-threshold** parameter specifies that when the average-threshold value in the applied profile is exceeded, take actions as configured in the action profile for this event.

The **max-threshold** parameter specifies that when the max-threshold value in the applied profile is exceeded, take actions as configured in the action profile for this event.

Examples

Example of setting the direction and average threshold.

```
device# configure terminal
device(config)# protocol cfm
device(protocol-cfm)# y1731
device(protocol-cfm-y1731)# test-profile my_test_profile
device(protocol-cfm-y1731-my_test_profile)# threshold backward
device(protocol-cfm-y1731-my_test_profile)# threshold average 25
device(protocol-cfm-y1731-my_test_profile)# exit
```

History

Release version	Command history
18x.1.00	This command was introduced.

threshold (ETH-DM)

Configures the ETH-DM threshold.

Syntax

threshold [**average** *average-threshold* | **maximum** *maximum-threshold*]

no threshold [**average** *average-threshold* | **maximum** *maximum-threshold*]

Parameters:

average *average-threshold*
Specifies the average threshold. The valid value is from 1 to 4294967295.

maximum *maximum-thershold*
Specifies the maximum threshold. The valid value is from 1 to 4294967295.

Command Default

The default value for average threshold is 4294967295 uSec. The default value for maximum threshold is 4294967295 uSec.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the threshold configuration.

Examples

This example shows how to configure the threshold value.

```
device# configure terminal
device (config-cfm)# protocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
device(config-cfm-y1731-test-profile-my_test_profile)# threshold maximum 3294967295
```

History

Release version	Command history
18x.1.00	This command was introduced.

threshold (ETH-SLM)

Configures the ETH-SLM threshold.

Syntax

threshold { **backward** [**avarage** *average-value* | **maximum** *maximum-value*] | **forward** [**avarage** *average-value* | **maximum** *maximum-value*] }

no threshold { **backward** [**avarage***average-value* | **maximum** *maximum-value*] | **forward** [**avarage** *average-value* | **maximum** *maximum-value*] }

Parameters:

backward
Specifies ETH-SLM backward threshold.

average *average-value*
Specifies the ETH-SLM backward average threshold value. The average value range is from 1 to 4294967295.

maximum*maximum value*
Specifies the ETH-SLM backward maximum threshold value. The average value range is from 1 to 4294967295.

forward
Specifies ETH-SLM forward threshold.

Command Default

The default value for average threshold is 4294967295 uSec. The default value for maximum threshold is 4294967295 uSec.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the threshold configuration.

Examples

This example shows how to configure the threshold value.

```
device# configure terminal
device (config-cfm)# protocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
device(config-cfm-y1731-test-profile-my_test_profile)# threshold forward maximum 3294967295
```

History

Release version	Command history
18x.1.00	This command was introduced.

threshold-monitor cpu

Configures monitoring of CPU usage of the system and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor cpu { [**actions** [**none** | **raslog** [{ **limit** *limit_when_reached* | **poll** *polling_interval* | **retry** *number_of_retries*]] }

no threshold-monitor cpu

Parameters

actions

Specifies the action to be taken when a threshold is exceeded.

none

No action is taken.

raslog

Specifies RASLog messaging.

limit

Specifies the baseline CPU usage limit as a percentage of available resources.

limit_when_reached

When the limit set by this parameter is exceeded, a RASLog WARNING message is sent. When the usage returns below the limit, a RASLog INFO message is sent. Valid values range from 0 through 80 percent. The default is 70 percent.

poll

Specifies the polling interval in seconds.

polling_interval

The range is from 0 through 3600. The default is 120

retry

Specifies the number of polling retries before desired action is taken.

number_of_retries

Range is from 1 through 100. The default is 3.

Modes

Global configuration mode

Usage Guidelines

This command sends a RASLog WARNING message when configured thresholds are exceeded.

Examples

```
device(config)# threshold-monitor cpu actions rasloglimit 50 poll10
```

History

Release version	Command history
18x.1.00	This command was introduced.

threshold-monitor memory

Configures monitoring of the memory usage of the system and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor memory { [**actions** [**none** | **raslog** { **high-limit** *percent* | **limit** *percent* | **low-limit** *percent* | **poll** *polling_interval* | **retry** *number_of_retries* } | **high-limit** *percent* | **limit** *percent* | **low-limit** *percent* | **poll** *polling_interval* | **retry** *number_of_retries* }] }

no threshold-monitor memory

Parameters

actions

Specifies the action to be taken when a threshold is exceeded.

none

No action is taken. This is the default.

raslog

Specifies RASLog messaging.

high-limit

Specifies an upper limit for memory usage as a percentage of available memory.

percent

This value must be greater than the value set by **limit** . When memory usage exceeds this limit, a RASLog CRITICAL message is sent. Values range from 0 through 80 percent. The default is 70 percent.

limit

Specifies the baseline memory usage limit as a percentage of available resources.

percent

When this value is exceeded, a RASLog WARNING message is sent. When the usage returns below the value set by **limit** , a RASLog INFO message is sent. Values range from 0 through 80 percent. The default is 60 percent.

low-limit

Specifies a lower limit for memory usage as percentage of available memory.

percent

This value must be smaller than the value set by **limit** . When memory usage exceeds or falls below this limit, a RASLog INFO message is sent. The default is 40 percent.

poll

Specifies the polling interval in seconds.

polling_interval

The range is from 0 through 3600. The default is 120

retry

Specifies the number of polling retries before desired action is taken.

number_of_retries
Range is from 1 through 100. The default is 3.

Modes

Global configuration mode

Examples

```
device(config)# threshold-monitor memory actions none high-limit 80 low-limit 50 limit 70 retry 2 poll
30
```

History

Release version	Command history
18x.1.00	This command was introduced.

threshold-monitor sfp

Configures monitoring of SFP parameters.

Syntax

threshold-monitor sfp { [**apply** *policy_name* | **pause** | **policy** *policy_name*] **type** *SFP_type* **area** *parameters* **alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **none** | **raslog**] | **lowthresh-action** [**all** | **email none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **none raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]] }

no threshold-monitor sfp

Command Default

By default, SFP is not monitored.

Parameters

apply *policy_name*

Applies a custom policy that has been created by the **policy** operand.

pause

Pause monitoring.

policy

Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.

policy_name

Name of a custom policy configuration that can be saved and applied by means of the **apply** operand.

type

Specifies the SFP type. Possible completions are as follows:

1GLR

— SFP Type 1GLR

1GSR

— SFP Type 1GSR

10GLR

— SFP Type 10GLR

10GSR

— SFP Type 10GSR

10GUSR

— SFP Type 10GUSR

100GSR

— SFP Type 100GSR

QSFP

— SFP type QSFP

area

Specifies one of the following SFP parameters to be monitored. See Defaults, below.

Current

Measures the current supplied to the SFP transceiver.

RXP

Measures the incoming laser power, in microWatts (µW).

TXP

Measures the outgoing laser power, in µW).

Temperature

Measures the temperature of the SFP, in degrees Celsius.

Voltage

Measures the voltage supplied to the SFP.

alert

Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

above

Enables setting a value for **highthresh-action**, which specifies the action to be taken when a high threshold is exceeded.

below

Enables setting a value for **highthresh-action** and **lowthresh-action**, which specifies the action to be taken when a low threshold is exceeded.

all

Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of **highthresh-action** only.

all

Specifies that email and RASLog messaging are used.

email

Specifies that an email message is sent.

none

Specifies that no alert is sent.

raslog

Specifies RASLog messaging.

limit

Specifies the percent of threshold usage, from 0 through 80. The default is 75.

poll

Specifies the polling interval in seconds, from 0 through 3600. The default is 120.

retry

Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.

threshold

Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.

buffer
An integer value.

high-threshold
An integer value.

low-threshold
An integer value.

timebase
Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.

day
Calculates the difference between a current data value and that value a day ago.

hour
Calculates the difference between a current data value and that value an hour ago.

minute
Calculates the difference between a current data value and that value a minute ago.

none
Compares a data value to a threshold boundary level.

Modes

Global configuration mode

Examples

A typical command might look like this:

```
device(config)# threshold-monitor sfp custom type QSFP area rxp threshold high-threshold 2000 low-
threshold 1000
```

History

Release version	Command history
18x.1.00	This command was introduced.

timeout (link-oam)

Allows you to configure timeout value, which corresponds to hold time before the Discovery process restarts.

Syntax

timeout *sec*

no timeout

Command Default

The default wait time is 5 seconds.

Parameters

sec

Specifies the hold time (in seconds) before the discovery process restarts. The range is from 1 through 10. The default value is 5.

Modes

Link OAM configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure a wait time of 10 seconds.

```
device(config-link-oam)# timeout 4
```

History

Release version	Command history
18x.1.00	This command was introduced.

timeout (RADIUS)

Species the wait time allowed for a Remote Authentication Dial-In User Service (RADIUS) server response.

Syntax

timeout *sec*

no timeout

Command Default

The default wait time is 5 seconds.

Parameters

sec

Specifies the wait time (in seconds) allowed for a RADIUS server response. The range is from 1 through 60. The default value is 5.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure a wait time of 10 seconds.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# timeout 10
```

History

Release version	Command history
18x.1.00	This command was introduced.

timeout (Y1731)

Configures timeout in seconds.

Syntax

timeout *timeout-value*

no timeout *timeout-value*

Parameters:

timeout-value

Spcifies the timeout value. The range is from 1 to 4 seconds.

Command Default

The default value for timeout is 1 second.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the timeout configuration.

Examples

This example shows how to configure the timeout value.

```
device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
device(config-cfm-y1731-test-profile-my_test_profile)# threshold maximum 3294967295
device(config-cfm-y1731-test-profile-my_test_profile)# timeout 1
```

History

Release version	Command history
18x.1.00	This command was introduced.

timers (BGP)

Adjusts the interval at which BGP KEEPALIVE and HOLDTIME messages are sent.

Syntax

timers { **keep-alive** *keepalive_interval* **hold-time** *holdtime_interval* }

no timers

Parameters

keep-alive *keepalive_interval*
: Frequency in seconds with which a device sends keepalive messages to a peer. Range is from 0 through 65535 seconds. The default is 60.

hold-time *holdtime_interval*
: Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Range is from 0 through 65535 seconds. The default is 180.

Modes

BGP configuration mode

Usage Guidelines

The KEEPALIVE and HOLDTIME message interval is overwritten when the **fast-external-failover** command takes effect on a down link to a peer.

You must enter a value for **keep-alive** before you can enter a value for **hold-time**. Both values must be entered. If you only want to adjust the value of one parameter, enter the default value of the parameter that you do not want to adjust.

The **no** form of the command clears the timers.

Examples

The following example sets the keepalive timer for a device to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# timers keep-alive 120 hold-time 360
```

The following example sets the keepalive timer for a device to 0 seconds and the hold-timer to 0 seconds so that the device waits indefinitely for messages from a neighbor without tearing down the session.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# timers keep-alive 0 hold-time 0
```

History

Release version	Command history
18x.1.00	This command was introduced.

timers (OSPFv2)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) throttle timers.

Syntax

timers { **lsa-group-pacing** *interval* | **throttle spf** *start hold max* }

Command Default

See the parameters section for specific defaults.

Parameters

lsa-group-pacing *interval*

Specifies the interval at which OSPF LSAs are collected into a group and refreshed, check-summed, or aged by the OSPF process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

throttle spf

Specifies start, hold and maximum wait intervals for throttling SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 60000 milliseconds. The default is 0.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 0.

max

Maximum wait time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 0.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

The **no timers lsa-group-pacing** command restores the pacing interval to its default value.

The **no timers throttle spf** command sets the SPF timers back to their defaults.

Examples

The following example sets the LSA group pacing interval to 30 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# timers lsa-group-pacing 30
```

The following example sets the SPF delay to 10000 milliseconds, the hold time to 15000 milliseconds, and the maximum wait time to 30000 milliseconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# timers throttle spf 10000 15000 30000
```

timers (OSPFv3)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) timers.

Syntax

timers { **lsa-group-pacing** *interval* | **spf** *start hold* }

Command Default

Enabled.

Parameters

lsa-group-pacing *interval*

Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check-summed, or aged by the OSPFv3 process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

spf

Specifies start and hold intervals for SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 65535 seconds.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 65535 seconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

The **no timers lsa-group-pacing** command restores the pacing interval to its default value.

The **no timers spf** command sets the SPF timers back to their defaults.

Examples

The following example sets the LSA group pacing interval to 30 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# timers lsa-group-pacing 30
```

The following example sets the SPF delay time to 10 and the hold time to 20.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# timers spf 10 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

tlv-type

Enables the Port Status type-length-value (TLV) metric for the specified Maintenance End Points (MEP).

Syntax

tlv-type { **port-status-tlv** }

no tlv-type port-status-tlv

Command Default

The Port Status TLV is not enabled.

Parameters

port-status-tlv

Enables the Port Status TLV metric.

Modes

CFM protocol configuration mode .

Usage Guidelines

The **no tlv-type port-status-tlv** command disables the Port Status TLV metric for the specified MEP.

Examples

Command example to enable the Port Status TLV metric.

```
device# configure terminal
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
device(config-cfm-md-ma-ma1)# mep 1 down ethernet 1/2
device(config-cfm-md-ma-mep-1)# tlv-type port-status-tlv
```

History

Release version	Command history
18x.1.00	This command was introduced.

topology-group

Configures the topology group.

Syntax

topology-group *group-id*

no topology-group *group-id*

Command Default

A topology group is not configured.

Parameters

group-id

Specifies the topology group ID. The ID ranges from 1 through 256.

Modes

Global configuration mode

Usage Guidelines

Each topology group contains a master VLAN and can contain one or more member VLANs and VLAN groups. You must configure the master VLAN and member VLANs or member VLAN groups before you configure the topology group.

You can configure up to 30 topology groups. Each group can control up to 4096 VLANs. A VLAN cannot be controlled by more than one topology group. The topology group must contain a master VLAN and can also contain individual member VLANs, VLAN groups, or a combination of individual member VLANs and VLAN groups.

The **no** form of the command removes the topology group.

Examples

The following example configures the topology group with ID 2 and adds master VLAN and member VLANs.

```
device# configure terminal
device(config)# topology-group 2
device(config-topo-group-2)# master-vlan 2
device(config-topo-group-2)# member-vlan 3
device(config-topo-group-2)# member-vlan 4
device(config-topo-group-2)# member-vlan 5
```

History

Release version	Command history
18x.1.00	This command was introduced.

traceroute

Traces the network path of packets as they are forwarded to a destination address.

Syntax

traceroute { *IPv4_address* | *host-name* | **ipv6** [*dest-ipv6-addr* | *host-name*] } [**interface**] [**maxttl** *value*] [**minttl** *value*] [**src-addr** *src-addr*] [**timeout** *seconds*] [**vrf** *vrf-name*]

Parameters

IPv4_address
Specifies the IPv4 address of the destination device.

host-name
Specifies the hostname of the destination device.

ipv6 *dest-ipv6-addr*
Specifies the IPv6 address of the destination device.

interface
Selects the output interface.

maxttl *value*
Maximum Time To Live value in a number of hops.

minttl *value*
Minimum Time To Live value in a number of hops.

src-addr *address*
Specifies the IPv4 or IPv6 address of the source device.

timeout *seconds*
The traceroute timeout value.

vrf *vrf-name*
Name of the VRF. If no VRF is specified, the default-vrf is used.

Modes

Privileged EXEC mode

Usage Guidelines

To use the **traceroute** command on the management VRF, enter **mgmt-vrf**. You must enter the name of the management VRF manually.

Examples

The following example executes an IPv6 traceroute, with minimum and maximum TTL values.

```
device# traceroute ipv6 fec0:60:69bc:92:218:8bff:fe40:1470 maxttl 128 minttl 30 src-addr fec0:60:69bc:
92:205:33ff:fe9e:3f20 timeout 3

traceroute to fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470), 128 hops max, 80
byte packets
30  fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470)  2.145 ms  2.118 ms  2.085
ms
```

History

Release version	Command history
18x.1.00	This command was introduced.

track (VRRP)

Enables VRRP tracking for a specified interface. VRRP Extended (VRRP-E) sessions can track a specified interface or a network.

Syntax

track { **ethernet** *slot*/*port*| **port-channel** *number* } [**priority** *value*]

track network { *ip-addressmask* | *ipv6-address*/*mask* } [**priority** *value*]

no track { **ethernet** *slot*/*port*| **port-channel** *number* } [**priority** *value*]

no track network { *ip-address*/*mask* | *ipv6-address*/*mask* } [**priority** *value*]

Command Default

The default priority value is 2.

Parameters

ethernet *slot port*
Specifies a valid, physical Ethernet subtype with appropriate slot and port number.

port-channel *number*
Specifies the port-channel number. Valid values range from 1 through 6144.

priority *value*
The track priority is a number from 1 through 254, and is used when a tracked interface or network up or down event is detected. For VRRP, if the tracked interface goes offline, the specified priority value is subtracted from the priority of the current device. For VRRP-E, if the tracked interface or network goes offline, the current device priority is reduced by the configured priority value. If the tracked interface or network comes online, the specified priority value is added to the priority of the current device.

network
Enables tracking of a specified network. Network tracking is supported only on VRRP-E sessions.

ip-address
Specifies an IPv4 network address.

ipv6-address
Specifies an IPv6 network address.

mask
Specifies a mask for the associated IP or IPv6 subnet.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This command can be used to track interfaces for VRRP or VRRP-E. Only VRRP-E sessions support network tracking.

For VRRP, the tracked interface can be any Ethernet or port-channel interface other than the one on which this command is issued.

The networks to be tracked can be either present or absent from the Routing Information Base (RIB).

The maximum number of interfaces or networks you can track per virtual router is 16.

Enter **no track** with the specified interface or network to remove the tracked port or tracked network configuration.

Examples

To set the track port to 2/4 and the track priority to 60:

```
device# configure terminal
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# vrrp-group 1
device(config-vrrp-group-1)# track ethernet 2/4 priority 60
```

The following example shows how to configure network 10.1.1.0/24 to be tracked, and if the network goes down, the VRRP-E device priority is lowered by a value of 20. The lower priority may trigger a switchover and a backup device with a higher priority becomes the new master for VRRP-E group 1.

```
device# configure terminal
device(config)# protocol vrrp-extended
device(config)# interface ve 100
device(conf-if-Ve-100)# vrrp-extended-group 1
device(config-vrrp-extended-group-1)# track network 10.1.1.0/24 priority 20
```

History

Release version	Command history
18x.1.00	This command was introduced.

trigger

Defines event-handler triggers. When the trigger-condition occurs, a Python script is run.

Syntax

trigger *trigger-id* **raslog** *raslog-id* [**pattern** *posix-ext-regex*]

no trigger [*trigger-id*]

Command Default

No trigger is defined.

Parameters

trigger-id
Specifies an ID number for the trigger. Valid values are 1 through 100, and must be unique per event-handler profile.

raslog *raslog-id*
Specifies a RASlog message ID as the trigger.

pattern *posix-ext-regex*
Specifies a POSIX extended regular expression to search within the specified RASlog message ID.

Modes

Event-handler configuration mode

Usage Guidelines

You can create from 1 through 100 triggers per profile.

You can also define one trigger as part of the **event-handler** command.

To delete one or all triggers, use the **no** form of this command, as follows:

- To delete all triggers, enter **no trigger**.
- To delete a specific trigger, enter **no trigger** *trigger-id*

NOTE
You cannot delete the last remaining trigger from an activated event-handler profile.

You can modify an existing trigger without deleting it and then re-creating it.

If the event-handler for which you are modifying triggers is active on the device, the changes take effect with no need to de-activate and re-activate the event-handler.

A Python event-handler script runs only if all of the following occur:

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.

- In configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.
  - Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

Examples

The following example defines triggers in two event handlers.

```
device# configure terminal
device(config)# event-handler eventHandler2
device(config-event-handler-eventHandler2)# trigger 1 raslog NSM-1001
device(config-event-handler-eventHandler2)# trigger 2 raslog NSM-1003
```

The following example defines a trigger that uses POSIX extended REGEX to search for a match within a specified RASlog message ID.

```
device# configure terminal
device(config-event-handler-eventHandler1)# event-handler eventHandler2
device(config-event-handler-eventHandler2)# trigger 1 raslog NSM-1003 pattern Interface Ethernet 0/
[1-9] is link down
```

RASlog message NSM-1003 includes "**interface** *interface-name* is link down", indicating that an interface is offline because the link is down. The REGEX searches within such a message for an interface from 0/1 through 0/9.

trigger-function

For an implementation of an event-handler profile, if multiple triggers are defined for an event-handler action, specifies if the action runs only if all of the triggers occur; or if one is sufficient.

Syntax

trigger-function { **OR** | **AND** { **time-window** *seconds* } }

no trigger-function

Command Default

The event-handler action runs if any of the triggers occur (**OR**).

Parameters

OR

The event-handler action runs if any of the triggers occur.

AND

The event-handler action runs only if all of the triggers occur.

time-window *seconds*

In seconds, specify the time window within which all of the triggers must occur in order that the event-handler action runs.

Following an initial triggering of an event-handler action, any subsequent trigger launches the action an additional time if the following conditions are true:

- The **trigger-mode** parameter is set to the default **each-instance**.
- The subsequent trigger occurs within the specified **time-window**.

Modes

Event-handler activation mode

Usage Guidelines

The **no** form of this command sets the **trigger-function** setting to the default **OR** option.

Examples

The following example determines that the event-handler action runs only if all of the triggers occur within 120 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# trigger-function AND time-window 120
```

The following example resets **trigger-function** to the default **OR** option.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no trigger-function
```

trigger-mode

For an implementation of an event-handler profile, specifies if recurring trigger conditions can launch an event-handler action more than once.

Syntax

trigger-mode *mode*

no trigger-mode

Command Default

Each time the trigger condition occurs, the event-handler action is launched.

Parameters

mode

Specifies if an event-handler action can be triggered only once or more than once.

each-instance

The event-handler action is launched on each trigger instance received.

on-first-instance

As long as the device is running, the event-handler action is launched only once. Following a device restart, the event-handler action can be triggered again.

only-once

For the duration of a device configuration, the event-handler action is launched only once.

Modes

Event-handler activation mode

Usage Guidelines

The **no** form of this command resets the **trigger-mode** setting to the default **each-instance** option.

Examples

The following example sets the trigger mode to **on-first-instance**.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# trigger-mode on-first-instance
```

The following example resets **trigger-mode** to the default value of **each-instance**.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no trigger-mode
```

ttl

Configures the time to live (TTL) value for a tunnel interface.

Syntax

ttl *ttl-value*

no ttl

Parameters

ttl-value

Specifies the TTL value. The range is from 1 to 255.

Command Default

The default TTL value is 255.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no** form of this command to revert to the default value.

Examples

This example configures the TTL value for the tunnel interface.

```
device# configure terminal
device (config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
device(config-intf-tunnel-5)# ttl 64
```

History

Release version	Command history
18x.1.00	This command was introduced.

tunable-optics

This command assigns channels to tunable optic interfaces (T-SFP+) for specific wavelengths.

Syntax

tunable-optics sfpp channel *channel_number*

Command Default

The T-SFP+ optic defaults to a "no wavelength" state before being activated.

Modes

Interface configuration mode

Usage Guidelines

Tunable SFP+ optics are optional hardware that can be installed in the linecards with optical SFPs.

If you are installing a T-SFP+ in a 144S port, the T-SFP+ optic needs to be installed in both ends of the cable. The T-SFP+ at each end of the cable link must be configured at the same wavelength by setting them to the same channel on each device.

Failure to duplicate the channel setting may allow the link to come online, but the link behavior may be erratic.

If the firmware determines an error is exceeding a specified limit, a RASLOG message event occurs and the port is taken offline.

The T-SFP+ interface defaults to a "no wavelength" state. When a supported Extreme device boots, the firmware sets the desired wavelength of the T-SFP+ optic.

When a T-SFP+ interface is installed it is very important that the interface is configured to the same channel (wavelength) at both ends. Use the **show media tunable-optic-sfpp** command to determine the currently configured channel.

T-SFP+ interfaces are tuned to specific wavelengths and frequencies using pre-defined channels.

Refer to the *Extreme SLX-OS Monitoring Configuration Guide* for complete information on tunable optics.

The following tables lists the frequency and wavelength assigned to channels for tunable SFP+ optic interfaces.

TABLE 6 Supported wavelengths and channel numbers

Channel	Frequency (THz)	Wavelength (nm)
1	191.10	1568.77
2	191.15	1568.36
3	191.20	1567.95
4	191.25	1567.54
5	191.30	1567.13
6	191.35	1566.72
7	191.40	1566.31
8	191.45	1565.90
9	191.50	1565.50
10	191.55	1565.09

TABLE 6 Supported wavelengths and channel numbers (continued)

Channel	Frequency (THz)	Wavelength (nm)
11	191.60	1564.68
12	191.65	1564.27
13	191.70	1563.86
14	191.75	1563.45
15	191.80	1563.05
16	191.85	1562.64
17	191.90	1562.23
18	191.95	1561.83
19	192.00	1561.42
20	192.05	1561.01
21	192.10	1560.61
22	192.15	1560.20
23	192.20	1559.79
24	192.25	1559.39
25	192.30	1558.98
26	192.35	1558.58
27	192.40	1558.17
28	192.45	1557.77
29	192.50	1557.36
30	192.55	1556.96
31	192.60	1556.55
32	192.65	1556.15
33	192.70	1555.75
34	192.75	1555.34
35	192.80	1554.94
36	192.85	1554.54
37	192.90	1554.13
38	192.95	1553.73
39	193.00	1553.33
40	193.05	1552.93
41	193.10	1552.52
42	193.15	1552.12
43	193.20	1551.71
44	193.25	1551.32
45	193.30	1550.92
46	193.35	1550.52
47	193.40	1550.12
48	193.45	1549.72
49	193.50	1549.32
50	193.55	1548.91
51	193.60	1548.51

TABLE 6 Supported wavelengths and channel numbers (continued)

Channel	Frequency (THz)	Wavelength (nm)
52	193.65	1548.11
53	193.70	1547.72
54	193.75	1547.32
55	193.80	1546.92
56	193.85	1546.52
57	193.90	1546.12
58	193.95	1545.72
59	194.00	1545.32
60	194.05	1544.92
61	194.10	1544.53
62	194.15	1544.13
63	194.20	1543.73
64	194.25	1543.33
65	194.30	1542.94
66	194.35	1542.54
67	194.40	1542.14
68	194.45	1541.75
69	194.50	1541.35
70	194.55	1540.95
71	194.60	1540.56
72	194.65	1540.16
73	194.70	1539.77
74	194.75	1539.37
75	194.80	1538.98
76	194.85	1538.58
77	194.90	1538.19
78	194.95	1537.79
79	195.00	1537.40
80	195.05	1537.00
81	195.10	1536.61
82	195.15	1536.22
83	195.20	1535.82
84	195.25	1535.43
85	195.30	1535.04
86	195.35	1534.64
87	195.40	1534.25
88	195.45	1533.86
89	195.50	1533.47
90	195.55	1533.07
91	195.60	1532.68
92	195.65	1532.29

TABLE 6 Supported wavelengths and channel numbers (continued)

Channel	Frequency (THz)	Wavelength (nm)
93	195.70	1531.90
94	195.75	1531.51
95	195.80	1531.12
96	195.85	1530.72
97	195.90	1530.33
98	195.95	1529.94
99	196.00	1529.55
100	196.05	1529.16
101	196.10	1528.77
102	196.15	1528.38

Examples

Typical command example.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# tunable-optics sfpp channel 5
device(conf-if-eth-0/1)# do show media optical-monitoring
N/A - Not Available.
N/S - Optical-monitoring Not Supported.
Port            Module      Supply       Channel      Frequency Wavelength Bias         Channel
                Temperature Voltage      TX Power     Error     Error      Current      RX Power
                ( C )       ( mVolts )   ( uWatts )   ( GHz )   ( nm )     ( mAmps )    ( uWatts )
=============== =========== ============ ============ ========= ========== ============ ============
Eth 0/1         36          3291.6       694.4        0.0       0.000      38.550       748.8

Eth 0/24                                 N/S

Eth 0/32        33          3317.1       685.1        0.0       0.000      37.132       914.5

Eth 0/48                                 N/S
```

History

Release version	Command history
18x.1.00	This command was introduced.

tx-frame-count

Configures the transmission frame count.

Syntax

tx-frame-count *frame-count*

no tx-frame-count

Parameters:

frame-count

Specifies the transmission frame count. The range is from 1 to 1000.

Command Default

The default value for tx-frame-count is 10 .

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the transmission frame count configuration.

Examples

This example shows how to configure the transmission frame count.

```
device# configure terminal
device (config-cfm)# protocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
device(config-cfm-y1731-test-profile-my_test_profile)# threshold maximum 3294967295
device(config-cfm-y1731-test-profile-my_test_profile)# tx-frame-count 300
```

History

Release version	Command history
18x.1.00	This command was introduced.

tx-interval

Configures the transmission interval.

Syntax

tx-interval *tx-interval*

no tx-interval

Parameters:

tx-interval

Specifies the transmission interval in seconds. Valid values can be 1, 10, 60, or 600 seconds.

Command Default

The default value for tx interval is 1 second.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the transmission interval configuration.

Examples

This example shows how to configure the transmission interval.

```
configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
```

History

Release version	Command history
18x.1.00	This command was introduced.

type

Configure a profile type as ETH-DM or ETH-SLM.

Syntax

type [**delay-measurement** | **synthetic-loss-measurement**]

Parameters:

delay-measurement

Specifies the profile type as delay management.

synthetic-loss-measurement

Specifies the profile type as synthetic loss measurement.

Modes

Y.1731 configuration mode

Examples

This example shows how to configure the profile type as delay measurement or as synthetic loss measurement .

```
device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement

device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type synthetic-loss-measurement
```

History

Release version	Command history
18x.1.00	This command was introduced.

type layer2-extension

Specifies that a VXLAN overlay gateway uses the Layer 2 extension.

Syntax

type layer2-extension

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

There is no **no** form of this command.

Examples

The following example specifies the Layer 2 extension:

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# type layer2-extension
```

History

Release version	Command history
18x.1.00	This command was introduced.

unlock username

Unlocks a locked user account.

Syntax

unlock username *name*

Parameters

name

Specifies the name of the user account.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to unlock a user who has been locked out because of unsuccessful login attempts. A user account is locked by the system when the configured threshold for login retries has been reached.

Examples

The following example unlocks a user account.

```
device# unlock username testUser
Result: Unlocking the user account is successful
```

History

Release version	Command history
18x.1.00	This command was introduced.

update-time

Configures the interval at which BGP next-hop tables are modified. BGP next-hop tables should always have IGP (non-BGP) routes.

Syntax

update-time *sec*

no update-time *sec*

Command Default

This option is disabled.

Parameters

sec

Update time in seconds. Range is from 0 through 30. Default is 5 seconds.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to restore the defaults.

The update time determines how often the device computes the routes (next-hops). Lowering the value set by the **update-time** command increases the convergence rate.

By default, the device updates the BGP4 next-hop tables and affected BGP4 routes five seconds following IGP route changes. Setting the update time value to 0 permits fast BGP4 convergence for situations such as a link failure or IGP route changes, starting the BGP4 route calculation in subsecond time.

NOTE

Use the **advertisement-interval** command to determine how often to advertise IGP routes to the BGP neighbor.

Examples

This example sets the BGP4+ update-time interval to 30.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# update-time 30
```

History

Release version	Command history
18x.1.00	This command was introduced.

usb

Enables or disables an attached USB device. The device is inaccessible until it is enabled.

Syntax

usb { **on** | **off** }

Parameters

on

Turns the USB device on.

off

Turns the USB device off.

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local device. A device reload automatically turns the USB device off.

This command is supported only on the local device.

Examples

To enable a USB device attached to the local device:

```
device# usb on
USB storage enabled
```

To disable a USB device attached to the local device:

```
device# usb off
USB storage disabled
```

History

Release version	Command history
18x.1.00	This command was introduced.

usb dir

Lists the contents of an attached USB device.

Syntax

usb dir

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local device. The USB device must be enabled before this function is available.

This command is supported only on the local device.

Examples

To list the contents of the USB device attached to the local device:

```
device# usb dir
firmwarekey\ 0B 2016 Aug 15 15:13
support\ 106MB 2016 Aug 24 05:36
support1034\ 105MB 2016 Aug 23 06:11
config\ 0B 2016 Aug 15 15:13
firmware\ 380MB 2016 Aug 15 15:13
Available space on usbstorage 74%
```

History

Release version	Command history
18x.1.00	This command was introduced.

usb remove

Removes a file from an attached USB device.

Syntax

usb remove directory *directory* **file** *file*

Parameters

directory *directory*

Specifies one the name of the directory where the file you want to remove is located. Valid USBstorage directories are /firmware, /firmwarekey, /support, and /config.

file *file*

Specifies the name of the file to be removed.

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local device. The USB device must be enabled before this function is available.

This command is supported only on the local device.

Examples

To remove a configuration file from a USB device attached to the local device:

```
device# usb remove directory config file startup-config.backup
```

History

Release version	Command history
18x.1.00	This command was introduced.

use-v2-checksum

Enables the v2 checksum computation method for a VRRPv3 IPv4 session.

Syntax

use-v2-checksum

no use-v2-checksum

Command Default

VRRPv3 uses the v3 checksum computation method.

Modes

Virtual-router-group configuration mode

Usage Guidelines

Some non-Extreme devices only use the v2 checksum computation method in VRRPv3. This command enables v2 checksum computation method in VRRPv3 and provides interoperability with these non-Extreme devices.

The **no** form of this command enables the default v3 checksum computation method in VRRPv3 sessions.

Examples

The following example shows the v2 checksum computation method enabled for an VRRPv3 IPv4 session on an Extreme device.

History

Release version	Command history
18x.1.00	This command was introduced.

user (alias configuration)

Launches the user-level alias configuration mode, in which you can manage user aliases.

Syntax

user *username*

no user *username*

Parameters

username

Specifies the account login name.

Modes

Alias configuration mode

Usage Guidelines

To delete all aliases defined for a specified user, enter the **no** form of this command.

Examples

The following example accesses user-alias configuration mode for the user jdoe, and defines a user-level alias named "sv" for the **show version** command.

```
device# configure terminal
device(config)# alias-config
device(config-alias-config)# user jdoe
device(config-user-jdoe)# alias sv "show version"
```

History

Release version	Command history
18x.1.00	This command was introduced.

username

Creates and configures a user account.

Syntax

username *username* **password** *password* **role** *role_name* [**access-time** *HHMM* **to** *HHMM*] [**desc** *description*] [**enable** { **true** | **false** }] [**encryption-level** { **0** | **7** }] [**expire** { **never** | *YYYY-MM-DD* }]

no username *name*

Parameters

username
Specifies the account login name.

access-time *HHMM* **to** *HHMM*
Restricts the hours during the day that the user may be logged in. Valid values range from 0000 through 2400. By default, users are granted 24 hour access. Use 24-hour format. For example, to restrict access to the daily work schedule, use **access-time 0800 to 1800**. By default, there is no access-time limitation. To change access time, include both the new "from" time and "to" time. To restore default access time, specify **access-time** *0000* **to** *2400*.

desc *description*
Specifies a description of the account (optional). The description can be up to 64 characters long, and can include any printable ASCII character, except for the following characters: single quotation marks (‘), double quotation marks (“), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces, enclose the text in double quotation marks.

enable
Enables or disables the account.

true
(Default) Enables the account.

false
Disables the account. A user whose account is disabled cannot log in.

expire
Specifies the password expiration setting.

never
(Default) Does not specify a password expiration date.

YYYY-MM-DD
Specifies a password expiration date.

password *password*
Specifies the account password. To use the exclamation mark (!) character, either precede it with the escape character (\)—**secret\!password**—or enclose the password within double quotes—**"secret!password"**.

role *role_name*
Specifies the role assigned to the username account.

encryption-level { 0 | 7 }

Specifies the password encryption level. The values are 0 (clear text) and 7 (encrypted). Clear text (0) is the default. If service password-encryption is enabled, it overrides a user-level setting.

Modes

Global configuration mode

Usage Guidelines

The *username* must be from 1 through 40 characters. It must begin with a letter or underscore and be comprised of only letters, numbers, underscore and period. A username is case sensitive. It cannot be the same as that of an existing role.

When creating a username, you must specify a password and a role. When modifying a username, it is sufficient to enter **username** *username*, followed by the new values.

The maximum number of user accounts on a device is 64.

If a user's password, access time, or role is changed, any login sessions for that user are terminated.

To specify **access-time**, use the system time defined for the SLX-OS operating system. For the current system time, enter **show clock**.

To delete a user, enter the **no username** *username* command.

Examples

The following example configures a user account.

```
device# configure terminal
device(config)# username testUser password ******** role user desc
```

The following example modifies an existing user account.

```
device# configure terminal
device(config)# username testUser desc "add op test user"
```

The following example modifies an existing user account, restricting the hours that an existing user may be logged in from 08:00 AM through 18:00 PM.

```
device# configure terminal
device(config)# username testUser access-time 0800 to 1800
```

History

Release version	Command history
18x.1.00	This command was introduced.

vc-mode

Configures the virtual connection (VC) mode for a pseudowire (PW) profile.

Syntax

vc-mode { **raw** | **tag** }

no vc-mode

Command Default

The default VC mode is **raw** .

Parameters

raw

Specifies using raw mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the VLAN tag is removed before it is sent out on the wire. When an untagged packet is received on an untagged AC endpoint it is encapsulated as is and sent out on the wire.

tag

Specifies using tag mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the packet is encapsulated as is and sent out on the wire. When an untagged packet is received on an untagged AC endpoint, a dummy tag is added and it is sent out on the wire.

Modes

Pseudowire-profile configuration mode.

Usage Guidelines

The **no** form of the command restores the default value.

NOTE

When a pseudowire profile is attached to a bridge domain, on which routing is enabled (by using the **router-interface** command), you are not allowed to change the pseudowire profile **vc-mode** configuration to **raw**.

Examples

The following example shows how to set the VC mode to **tag** for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# vc-mode tag
```

History

Release version	Command history
18x.1.00	This command was introduced.

virtual-ip

Configures a virtual IPv4 address or IPv6 address for the virtual router.

Syntax

virtual-ip { *ipv4-address* | *ipv6-address* }

no virtual-ip { *ipv4-address* | *ipv6-address* }

Parameters

ipv4-address
Virtual IPv4 address of the virtual router.

ipv6-address
Virtual IPv6 address of the virtual router.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The virtual IPv4 address or IPv6 address is the IP address that an end-host sets as its default gateway. The virtual IP address must belong to the same subnet as the underlying interface. A maximum of 16 virtual IP addresses can be configured for VRRP; only one virtual IP address can be configured for VRRP-E. The session is enabled as soon as the first virtual IP address is configured.

You can perform this command for VRRP or VRRP-E. VRRPv3 introduced the ability to use an IPv6 address when an IPv6 VRRPv3 group is configured.

This command accepts both fe80/10 link local addresses or fe80/64 addresses as virtual-IP.

Enter the **no virtual-ip** command with a specified virtual IP address to delete the specified virtual IP address

Examples

To assign a virtual IP address of 192.53.5.1 to the VRRP virtual group 1:

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# vrrp-group 1
device(config-vrrp-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IP address of 192.53.5.1 to the VRRP-E virtual group 1:

```
device(config)# protocol vrrp
device(config)# interface ve 20
device(config-ve-20)# vrrp-group-extended 1
device(config-vrrp-extended-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IPv6 address of 2001:2019:8192::1 to the VRRP-Ev3 virtual group 19:

```
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 2019
device(config-ve-2019)# ipv6 address 2001:2019:8192::122/64
device(config-ve-2019)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-19)# virtual-ip 2001:2019:8192::1
```

History

Release version	Command history
18x.1.00	This command was introduced.

virtual-mac

Enables generation of a virtual MAC with 0 IP hash.

Syntax

virtual-mac *virtual_mac_address*

Parameters

virtual_mac_address
Specifies a virtual MAC address.

Modes

VRRP-Extended group configuration mode

Usage Guidelines

The distributed VXLAN gateway functionality depends on VRRP-E for multi-homing. By default, the VRRP-E virtual MAC is derived as 02:e0:52:*<2-byte-ip-hash>*:*<1-byte-vrid>*. The VXLAN gateway requires that the virtual MAC be a function of only VRID. The two-byte hash of the virtual IP should be set to zeros, for example, 02e0.5200.00xx:100.

Examples

To enable the generation of a virtual MAC:

```
device# configure terminal
device(config)# interface ve 10
device(config-Ve-10)# vrrp-extended-group 100
device(config-vrrp-extended-group-100)# virtual-mac 02e0.5200.00xx:100
```

History

Release version	Command history
18x.1.00	This command was introduced.

vlan

Specifies a VLAN and enters VLAN configuration mode.

Syntax

vlan *vlan_id*

no vlan *vlan_id*

Command Default

No VLAN is configured.

Parameters

vlan_id

Specifies a VLAN ID. Range is from 1 through 4090.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to delete a VLAN.

Examples

To configure VLAN 10:

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

vlan (EVPN)

Specifies a VLAN, or adds or removes a range of VLANs, for an Ethernet Virtual Private Network (EVPN) instance.

Syntax

vlan *VLAN-ID*

no vlan *VLAN-ID*

vlan { **add** | **remove** } {*VLAN-range* }

Command Default

Disabled

Parameters

VLAN-ID
Specifies a VLAN.

add
Adds a range of VLANs to the default EVPN instance.

remove
Removes a range of VLANs from the default EVPN instance.

VLAN-range
Specifies a hyphen-delimited VLAN range.

Modes

EVPN configuration mode

Usage Guidelines

Each VLAN/BD added to an EVPN configuration is considered as an EVPN instance and is assigned a unique EVPN instance ID (EVI) internally. The EVI is calculated as shown in the following table.

TABLE 7 Calculating EVI values from VLAN/BD values

VLAN/BD	EVI value
VLAN: 1–4096	VLAN ID
BD: 1–4096	BD ID + 4096

ATTENTION
To interoperate with third-party vendors, the RTs across the interoperating devices must be the same. If third-party devices do not support automatic RT assigment, or the EVIs are not calculated as shown in the above table, the VLAN/BD instances must be configured manually to ensure that RTs across the devices are compatible.

Examples

The following example specifies a VLAN and enter VLAN configuration mode.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# vlan 100
device(evpn-vlan-100)#
```

The following example adds VLANs 100 through 200 to the default EVPN instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# vlan add 100-200
```

The following example removes VLANs 150 through 180 from the default EVPN instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# vlan remove 150-180
```

History

Release version	Command history
18x.1.00	This command was introduced.

vpn-statistics

Enables VPN statistics for a VRF.

Syntax

vpn-statistics

no vpn-statistics

Command Default

No RD is assigned to the VRF.

Parameters

as-num

Composed of the local ASN number followed by a colon ":" and a unique arbitrary number. For example 3:6.

ip-num:id

Composed of the local IP address followed by a colon ":" and a unique arbitrary number.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of the command returns to the default setting.

Examples

The following example shows how to enable VPN statistics for a VRF.

```
device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd 1:2
device#(config-vrf-vpn1)# vpn-statistics
```

History

Release version	Command history
18x.1.00	This command was introduced.

vrf

Creates a Virtual Routing and Forwarding (VRF) instance and enters VRF configuration mode.

Syntax

vrf *name*

Parameters

name

Character string for the name of the VRF. The string can be up 24 characters long, but should not contain punctuation or special characters.

Modes

Global configuration mode

Examples

To create the VRF instance "myvrf" and enter VRF configuration mode:

```
device# configure terminal
device(config)# vrf myvrf
device(config-vrf-myvrf)#
```

History

Release version	Command history
18x.1.00	This command was introduced.

vrrp-acceptmode-disable

Disables accept mode for the backup Virtual Router Redundancy Protocol (VRRP) virtual IP (VIP).

Syntax

vrrp-acceptmode-disable

no vrrp-acceptmode-disable

Command Default

When configured, accept mode is enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command enables accept mode for the backup VRRP VIP.

When enabled, accept mode allows a backup VRRP master device to respond to ping, traceroute, and Telnet packets if it becomes the master VRRP device.

Examples

The following example shows how to disable accept mode for the backup VRRP VIP.

```
device# configure terminal
device(config)# vrrp-acceptmode-disable
```

History

Release version	Command history
18x.1.00	This command was introduced.

vrrp-extended-group

Configures a virtual-router-extended group and enters into the virtual router configuration mode..

Syntax

vrrp-extended-group *group-ID*

no vrrp-extended-group *group-ID*

Parameters

group-ID

A user-assigned number from 1 through 255 that you assign to the virtual router group.

Modes

Virtual Ethernet (ve) interface configuration mode

Usage Guidelines

This configuration is for virtual Ethernet (VE) interfaces only.

Enter **no vrrp-extended-group** *group-ID* to remove the specific VRRP Extended group.

If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

Examples

The following example shows how to assign the VE interface with a VLAN number of 20 to the virtual router extended group with the ID of 1. (First you must enable VRRP-E on the switch.)

vrrp-group

Configures a virtual router group (VRRP) and enters into the virtual router configuration mode.

Syntax

vrrp-group *group-ID* [**version** { **2** | **3** }]

no vrrp-group *group-ID* [**version** { **2** | **3** }]

Command Default

VRRP version 2 is the default.

Parameters

group-ID

A value from 1 through 255 that you assign to the virtual router group.

version

Specifies in which version of VRRP the IPv4 VRRP group is to be configured.

2 | **3**

Version 2 or version 3 of VRRP.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no vrrp-group** *group-ID* to remove a specific VRRP group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

You can specify in which version of VRRP the VRRP group is configured using the **version** keyword and either 2 or 3 as the version number. VRRPv3 supports both IPv4 and IPv6 addresses.

Examples

The following example shows how to assign an Ethernet interface to the virtual router group with the ID of 1. (First you must enable VRRP on the switch.)

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(config-if-eth-1/6)# vrrp-group 1
```

The following example shows how to assign an Ethernet interface to the virtual router group with the ID of 1 for VRRPv3. (First you must enable VRRP on the switch.)

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# vrrp-group 1 version 3
```

History

Release version	Command history
18x.1.00	This command was introduced.

vtep-discovery

Enables automatic VXLAN tunnel endpoint (VTEP) discovery by BGP.

Syntax

vtep-discovery

no vtep-discovery

Command Default

Enabled.

Modes

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of this command disables automatic VTEP discovery and creation of VXLAN tunnels.

Examples

The following example disables automatic VTEP discovery by BGP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# no vtep-discovery
```

The following example re-enables automatic VTEP discovery and creation of VXLAN tunnels by BGP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# vtep-discovery
```

History

Release version	Command history
18x.1.00	This command was introduced.

write erase

Returns the switch to factory default state.

Syntax

write erase

Modes

Privileged EXEC mode

Usage Guidelines

This command can be used for device recovery or device configuration reset to the factory default state. Due to its disruptive nature, this command prompts the user about the consequence of losing all current user configuration and resetting the switch to the factory default state. It waits for the user's confirmation before proceeding.

Examples

The following command shows executing the **write erase** command.

```
device# write erase
This command will erase all the configuration on the Compact Flash.
The specified VCS parameters will be set appropriately while
preserving the licenses and management ip-address.

System will go through disruptive reboots during the process.
Please upload all configurations if they need to be saved before
continuing with this command.

Do you want to continue? [y/n]:
```

History

Release version	Command history
18x.1.00	This command was introduced.

y1731

Enters the Y.1731 configuration mode.

Syntax

y1731

no y1731

Command Default

This feature is disabled.

Modes

Protocol CFM configuration mode

Usage Guidelines

Use the **no** form of the command to delete all test and action profiles configured under Y.1731 mode and the corresponding associations with source and target MEP pair.

Examples

This example shows how to enters the Y1731 configuration mode.

```
device# configure terminal
device(config)# protocol cfm
device((protocol-cfm)# y1731
```

History

Release version	Command history
18x.1.00	This command was introduced.