9920 v21.2.2.0 Command References

CLI for Network Packet Brokering and Traffic Management

9039081-00 Rev AA
October 2024

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

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

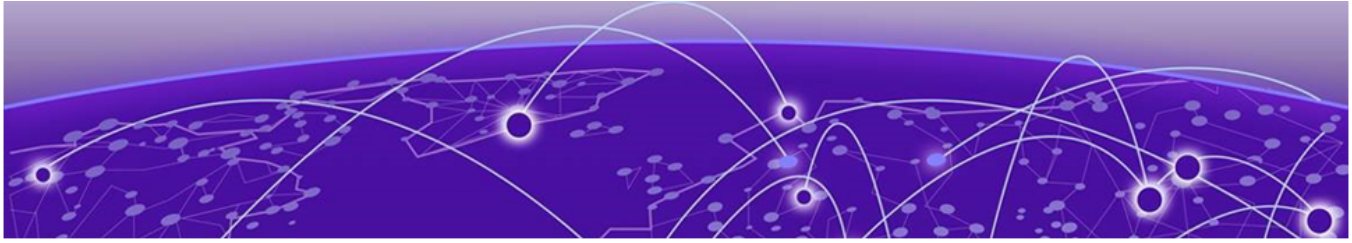
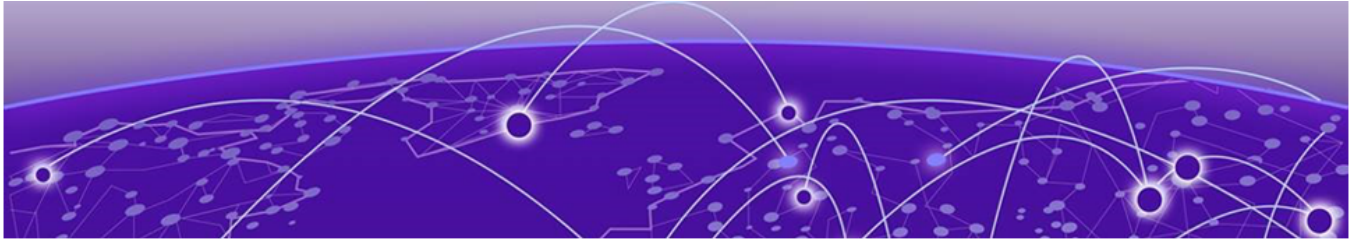


Table of Contents



Abstract

The Command References for version 21.2.2.0 of the 9920 appliance provides a comprehensive guide to managing the 9920 platform via the command-line interface (CLI). It includes detailed command syntax, parameters, and usage for network packet brokering (NPB) and traffic management. Key areas covered include user authentication, authorization, and accounting (AAA), configuration of network interfaces, access control lists (ACLs), and advanced debugging processes. Commands for packet capture, link aggregation (LAG), and traffic filtering based on IP, MAC, and protocol-based rules are also featured. This document is designed for network administrators and engineers responsible for traffic monitoring, resource management, and system diagnostics in high-performance, scalable network environments.

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

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

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	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, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

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

Extreme Portal

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

The Hub

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

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

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

Subscribe to Product Announcements

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

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

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

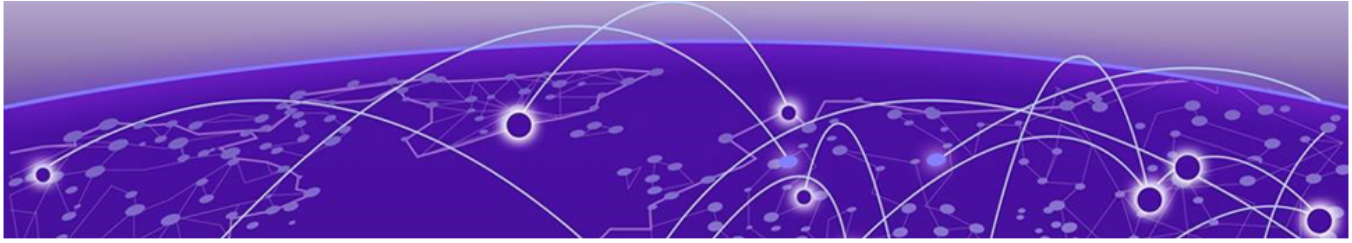
Send Feedback

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

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

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



What's New in this Document

There are new and modified commands for the Extreme 9920 software, release 21.2.2.0.

New Commands

The following command is new in this release.

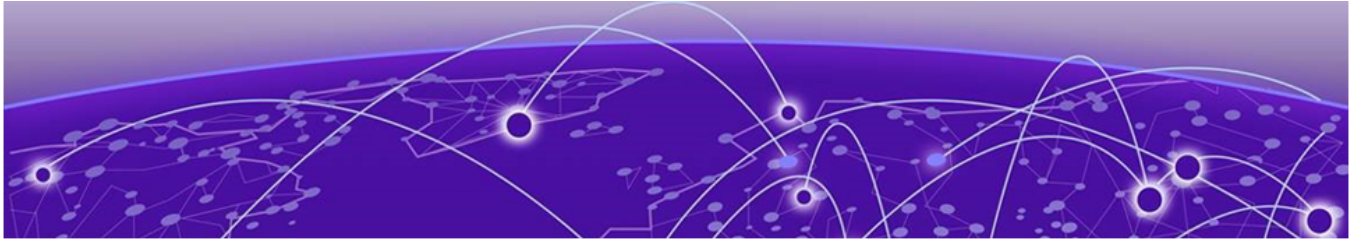
- capture start time on page 50

Modified Commands

The following commands are modified in this release.

- load-balance on page 133
- traffic-type vxlan on page 332
- traffic-type mpls on page 328

For more information about this release, refer to the Extreme 9920 Software Release Notes.



Using the NPB Application CLI

The command line provides a powerful means for configuring, managing, and monitoring packet traffic through the Extreme 9920 device.

The following topics describe accessing and using the NPB application command-line interface (CLI), including syntax, command completion, shortcuts, and other helpful subjects.

User Accounts

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

The NPB application 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 an admin or user role can be assigned.

For more information about user accounts and roles, see *Extreme 9920 Software Security Configuration Guide, 21.2.2.0*.

Default Account Credentials

The NPB application ships with two default user accounts.

When you install the NPB application on Extreme 9920, two default user accounts are provided—**admin** and **user**—with the following case-sensitive default passwords:

- admin account password: **rocks**
- user account password: **password**

As a best practice, log on as the administrator and change the default passwords immediately after the NPB application is installed.

Predefined Accounts and Roles

The NPB application ships with two predefined accounts—**admin** and **user**. The maximum number of user accounts that you can configure is 64, including the predefined accounts.

- **admin**—Accounts with admin role access can execute all commands supported on the device.
- **user**—Accounts with user-level access have read-only permissions. User-level accounts can run the following operational CLI commands.

Table 4: User-level operational commands

Command	Action
dir	List flash files
end	End current mode and change to enable mode
exit	Exit current mode and revert to previous mode
list	Print command list
ping	Ping
quit	Exit current mode and revert to previous mode
show	Show values
terminal	Set terminal timeout parameters
traceroute	Run traceroute
The **ping** and **traceroute** commands are also supported on gNOI and accept both IPv4 and IPv6 addresses.	

Accessing the CLI

After an IP address is assigned to the device, you can access the CLI through a serial console connection to the Ethernet management port or SSH session using the device management IP address.

For information on a session connection, see the *Extreme 9920 Software Configuration Guide, 21.2.2.0*.

The procedure to access the CLI is same for both console interface and SSH session. 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 application CLI uses an industry-standard hierarchical shell familiar to networking administrators.

Exec Mode

Log into the device to access Exec mode. Exec mode supports all clear, show, and debug commands. In addition, some configuration commands that do not make changes to the system configuration are also supported. The following example shows the command prompt in Exec mode:

```
device#
```

Use the `disable`, `exit`, or `logout` command to exit Exec mode.

Config Mode

Config mode supports commands that change the device configuration. All NPB application configurations are auto-persistent. Config mode provides access to sub-configuration modes for individual interfaces and other configuration areas. The following example shows how to access the Config mode:

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

All configuration commands require admin privilege.

do Command

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

For example, if you are configuring an Ethernet interface and you want to run an Exec mode command, such as the **dir** command, you 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-1/2)# 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)
```

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# ?
```

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

```
device# e?
Possible completions:
  event-handler    Event Handler Commands
  execute-script   Run user-level BASH scripts
  exit             Exit the management session
```

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

```
device# terminal ?
Possible completions:
 length    Sets Terminal Length 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 d?
Possible completions:
  debug      Display the udld debug configuration
  defaults   Display default configuration
  dot1x      Show dot1x
```

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
```

CLI Keyboard Shortcuts

The following table lists CLI keyboard shortcuts.

Table 5: 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 stops 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	Deletes all characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word you typed.

Table 5: CLI keyboard shortcuts (continued)

Keystroke	Description
Ctrl+Z	Returns to privileged EXEC mode. Using **Ctrl+Z** in privileged EXEC mode runs partial commands.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.

Show Command Output Modifiers

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

Table 6: CLI command output modifiers

Output Modifier	Description
append *filename*	Appends the output to a file.
save *filename*	Redirects the command output to the specified file.
include *string* or *expression*	Displays the command output that includes the specified expression.
exclude *string* or *expression*	Displays the command output that excludes the specified expression.
begin *string* or *expression*	Displays the command output that begins with the specified expression.
last *number*	Displays only the specified number of last lines of 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.

Unsupported Input Characters

If unsupported input characters are used for user-defined objects, an error message is displayed.

However, characters dependent on combinations of the **AltGr** key and another key are not supported.

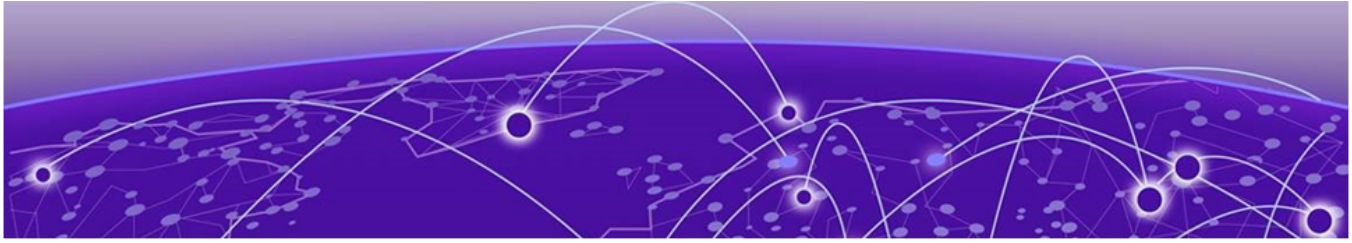
Note
The **AltGr** key is the **Alt** key to the right of the space bar.

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 running such commands and interpreting their results.

Note
Not all diagnostic commands are documented.



NPB Application Commands

The following topics describe NPB application commands and include details about parameters and usage.

aaa accounting

Enables or disables sending accounting logs for commands or login information to the TACACS+ server.

Syntax

aaa accounting { **commands** | **exec** | **all** } **default start-stop** { **tacacs+** | **none** }

no aaa accounting commands default start-stop tacacs+

Command Default

Accounting is disabled.

Parameters

accounting

Configures command accounting.

commands

Enables or disables command accounting.

exec

Enables or disables login accounting.

all

Enables or disables command and login accounting.

default

Enables sending of logged information to the default server.

start-stop

Enables 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.

tacacs+

Configures TACACS+ server for accounting.

none

Disables accounting services.

Modes

Config mode

Usage Guidelines

This command is allowed in Config mode only.

This command is available only to users with the admin role.

You can modify or enable only one accounting configuration.

Examples

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

```
device# configure terminal
device(config)# aaa accounting all default start-stop tacacs+

device# show running-config aaa
aaa authentication login tacacs+ local-auth-fallback
aaa accounting commands default start-stop tacacs+
aaa accounting exec default start-stop tacacs+
```

The following example disables login accounting; command accounting (when also configured) remains active.

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

aaa authentication

Configures the Authentication, Accounting, and Authorization (AAA) login sequence with TACACS+ primary and local auth secondary.

Syntax

aaa authentication login tacacs+ local-auth-fallback

no aaa authentication login tacacs+ local-authfallback

Command Default

Authenticates with the local database if this command is not run.

Parameters

login

Specifies the order of login authentication sources for login

tacacs+

Specifies the use of TACACS+ servers

local-auth-fallback

Specifies the use of a local switch database if authentication methods are not active or authentication fails.

Modes

Config mode

Usage Guidelines

This command is allowed only in configuration mode.

This command is available only to users with the admin role.

Examples

The following example configures the authentication sequence to first use a TACACS+ server, then to use the fallback database if TACACS+ authentication is not active or fails.

```
device# configure terminal
device(config)# aaa authentication login tacacs+ local-auth-fallback
```

The following example removes the authentication sequence from the TACACS+ server and defaults to local database authentication.

```
device(config)# no aaa authentication login tacacs+ local-auth-fallback
```

acl-config

Changes the CLI mode to `acl-config` to configure functions common to all types of ACL.

Syntax

`acl-config`

Parameters

`acl-config`

Specifies ACL common configurations.

Modes

Config mode

Examples

The following example changes the CLI mode to `acl-config`.

```
device(config)# acl-config
device(config-acl-config)#
```

address

Configures the IP address of the remote syslog server.

Syntax

address [*A.B.C.D* | *A:B::C:D*]

Parameters

A.B.C.D

Specifies the IPv4 address.

A:B::C:D

Specifies the IPv6 address.

Modes

Host configuration mode

Usage Guidelines

Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

Examples

The following example shows how to configure the IP address of the remote syslog server.

```
device(config-logging-host-H1)# address 1.1.1.1
Warning: Existing Host configuration changed
```

banner login

Configures the login banner message for displaying before the authentication prompt.

Syntax

banner login *STRING*

no banner login

Parameters

login *STRING*

Specifies the login message string. Valid range is 1-1024.

Modes

Config mode

Examples

The following example configures the banner login message.

```
device(config)# banner login “This is sample login message”

device# show running-config banner
banner login "This is sample login message"
```

banner motd

Configures the message of the day (MOTD) banner for displaying after authenticating the user.

Syntax

banner motd *STRING*

no banner motd

Parameters

motd *STRING*

Specifies the motd message string. Valid range is 1-1024.

Modes

Config mode

Examples

The following example configures the motd banner message.

```
device(config)# banner motd “This is sample motd message”

device# show running-config banner
banner login "This is sample motd message"
```

base command | append

Appends output of the base command to a text file.

Syntax

base command | **append** *FILENAME*

Parameters

base command

Specifies the base command for filtering the output.

append *FILENAME*

Specifies the file name for filtering the output of the base command. File format is `flash://cli/<name>`.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example appends the base command output to a flash file.

```
device# show running-config | append flash://cli/file1
```

base command | begin

Starts displaying the base command output for the matching token or expression.

Syntax

base command | **begin** *REGEX*

Parameters

base command

Specifies the base command for filtering the output.

begin *REGEX*

Specifies the token or expression to match to start displaying the base command output.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example starts displaying the output of the **show running-config** command after matching the expression, `interface ethernet 0/18`.

```
device# show running-config | begin "interface ethernet 0/18"

interface ethernet 0/18
  shutdown
interface ethernet 0/19
  shutdown
interface management 0
  ip address dhcp
  no ipv6 address dhcp
  no shutdown
```

base command | count

Counts the number of lines in the output of the base command.

Syntax

base command | **count**

Parameters

base command

Specifies the base command for filtering the output.

count

Specifies the number of lines in the base command output.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example counts the number of lines in the base command output.

```
device# show running-config | count
Count: 50 lines
```

base command | exclude

Hides the base command output lines that match the specific token or expression.

Syntax

base command | **exclude** *REGEX*

Parameters

base command

Specifies the base command for filtering the output.

exclude *REGEX*

Specifies the token or expression to match for hiding the base command output lines.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example hides the base command output lines that match the expression.

```
device# show running-config | exclude "ethernet 0" | exclude shutdown

ntp enable
ntp server 1.in.pool.ntp.org
ntp server 2.2.2.2
ntp server 2.1.1.1
ntp server 3.2.2.2
ntp server 3.2.2.1
interface management 0
  ip address dhcp
  no ipv6 address dhcp
```

base command | include

Displays only the base command output lines that match the specific token or expression.

Syntax

base command | **include** *REGEX*

Parameters

base command

Specifies the base command for filtering the output.

include *REGEX*

Specifies the token or expression to match for displaying the base command output lines.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example includes the base command output lines that match the specific expression.

```
device# show running-config | include interface | exclude "ethernet 0/"

interface management 0
```

base command | last

Displays only the specified number of last lines from the base command output.

Syntax

base command | **last** *NUMBER*

Parameters

base command

Specifies the base command for filtering the output.

last *NUMBER*

Specifies the number of last lines from the base command output for displaying.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example displays last four lines of the base command output.

```
device# ngnpb# show running-config | last 4

interface management 0
  ip address dhcp
  no ipv6 address dhcp
  no shutdown
```

base command | linenum

Numbers the base command output lines.

Syntax

base command | **linenum**

Parameters

base command

Specifies the base command for filtering the output.

linenum

Numbers the base command output lines.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example numbers the base command output lines.

```
device# show running-config | linnum | last 4

47:interface management 0
48:  ip address dhcp
49:  no ipv6 address dhcp
50:  no shutdown
```

base command | more

Paginates the base command output.

Syntax

base command | **more**

Parameters

base command

Specifies the base command for filtering the output.

more

Paginates the base command output.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example paginates the base command output.

```
device# show running-config | more

ntp enable
ntp server 3.2.2.1
ntp server 1.in.pool.ntp.org
ntp server 2.2.2.2
ntp server 2.1.1.1
ntp server 3.2.2.2
--More--
```

base command | nomore

Suppresses default pagination for the base command output.

Syntax

base command | **nomore**

Parameters

base command

Specifies the base command for filtering the output.

nomore

Suppresses default pagination for the base command output.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example suppresses default pagination for the base command output.

```
device# show running-config | nomore

ntp enable
ntp server 3.2.2.1
ntp server 1.in.pool.ntp.org
ntp server 2.2.2.2
ntp server 2.1.1.1
ntp server 3.2.2.2
interface ethernet 0/1
  shutdown
interface ethernet 0/2
  shutdown
interface ethernet 0/3
  shutdown
interface ethernet 0/4
  shutdown
interface ethernet 0/5
  shutdown
interface ethernet 0/6
  shutdown  .........
```

base command | save

Saves the base command output to a text file.

Syntax

base command | **save** *FILENAME*

Parameters

base command

Specifies the base command for filtering the output.

exclude *FILENAME*

Specifies the file name for writing the base command output. File format is `flash://cli/<name>`.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example writes the base command output to the specified file.

```
device# show running-config | save flash://cli/file2
```

base command | until

Stops displaying the base command output until a match is found for the specific token or expression.

Syntax

base command | **until** *REGEX*

Parameters

base command

Specifies the base command for filtering the output.

until *REGEX*

Specifies the token or expression to match from the base command output.

Modes

Filter mode

Usage Guidelines

The "|" symbol in this command does not act as a separator, but instead provides access to the filter command.

Examples

The following example stops displaying the base command output until a match is found.

```
device# show running-config | until "interface ethernet 0/2"

ntp enable
ntp server 2.1.1.1
ntp server 3.2.2.2
ntp server 3.2.2.1
ntp server 1.in.pool.ntp.org
ntp server 2.2.2.2
interface ethernet 0/1
  shutdown
interface ethernet 0/2
```

breakout

Configures breakout mode on the supported connectors.

Syntax

breakout [*4x10g* | *4x25g*]

no breakout

Parameters

4x10g

Configures the 4 x 10 G breakout mode.

4x25g

Configures the 4 x 25 G breakout mode.

Modes

Connector config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is supported only on even numbered ports. Example: 1/8

The port must not be part of a port channel.

The port must be in shutdown state.

The current and the previous port are deleted and four new ports with the breakout speed are created.

Examples

The following examples shows how to configure and verify breakout ports.

```
device(config-connector-1/8)# breakout 4x10g
WARN: Enabling breakout on a interface is a disruptive action and will result port 1/7 to
be unavailable for use along with defaulting all the configs on port 1/8.

device(config-connector-1/8)# breakout 4x10g
Port is already in breakout mode.
```

capture packet interface

Configures onboard packet capture on the interface.

Syntax

capture packet interface ethernet *IFNAME* { **direction** [*both* | *rx* | *tx*] [**packet-count** *number*] }

no capture packet interface ethernet *IFNAME*

Parameters

interface ethernet *IFNAME*

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

direction

Specifies the type of packet capture.

both

Specifies both ingress and egress packet capture.

rx

Specifies ingress packet capture.

tx

Specifies egress packet capture.

packet-count *number*

Specifies the number of packets to be captured on the interface. Valid packet capture values range from 1 to 8000.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Only one mirror session is allowed per port.

You must configure the interface before configuring packet capture.

A maximum of 10 mirror sessions per device are allowed.

Packet capture is not allowed if maximum PCAP files are already created.

When packet-count parameter is specified, the packet capture automatically stops on the interface after the specified number of packets are captured.

The maximum number of existing PCAP files cannot exceed 25.

Onboard packet capture is not persistent across reboot.

Examples

The following example configures both ingress and egress packet capture, up to 100, on ethernet interface 1/1.

```
device# capture packet interface ethernet 1/1 direction both packet-count 100
device# show capture packet config
```

The following example removes packet capture configuration on the specified ethernet slot/port.

```
device# no capture packet interface ethernet 1/1
```

capture start

Starts onboard packet capture in the active running PCAP file.

Syntax

capture start

Parameters

start

Starts packet capture.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

You must configure the interface before configuring packet capture.

Only one mirror session is allowed per port.

A maximum of 10 mirror sessions per device are allowed.

Packet capture is not allowed if maximum PCAP files are already created.

When packet-count parameter is specified, the packet capture automatically stops on the interface after the specified number of packets are captured.

The maximum number of existing PCAP files cannot exceed 25.

The **start** command does not clear hardware entries.

Onboard packet capture is not persistent across reboot.

Examples

The following example starts packet capture.

```
device# capture start
```

capture start time

Starts onboard packet capture at the configured time.

Syntax

capture start time *value*

Parameters

time *value*

Specifies the PCAP capture start time in format `YYYY-MM-DD HH:MM`. The Time must be inline with the system time in `UTC` format.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Only one mirror session is allowed per port.

You must configure the interface before configuring packet capture.

A maximum of 10 mirror sessions per device are allowed.

Packet capture is not allowed if maximum PCAP files are already created.

When packet-count parameter is specified, the packet capture automatically stops on the interface after the specified number of packets are captured.

The maximum number of existing PCAP files cannot exceed 25.

The **start** and **stop** commands do not clear hardware entries.

Onboard packet capture is not persistent across reboot.

Examples

The following example starts, verifies, and stops packet capture.

```
device# capture start time 2024-07-23 13:00
device# show capture packet config
capture start 2024-07-23 13:00 (UTC)
```

capture stop

Stops writing the packet capture to the PCAP file and moves the active file to the next available inactive PCAP file.

Syntax

capture stop

Parameters

stop

Stops packet capture.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Only one mirror session is allowed per port.

You must configure the interface before configuring packet capture.

A maximum of 10 mirror sessions per device are allowed.

Packet capture is not allowed if maximum PCAP files are already created.

When packet-count parameter is specified, the packet capture automatically stops on the interface after the specified number of packets are captured.

The maximum number of existing PCAP files cannot exceed 25.

The **start** and **stop** commands do not clear hardware entries.

Onboard packet capture is not persistent across reboot.

Examples

The following example stops packet capture.

```
device# capture stop
```

channel-group

Assigns and configures a physical interface to a link aggregation group (LAG).

Syntax

channel-group *number* **mode** { **on** | **active** | **passive** }

no channel-group

Parameters

number

Specifies the number of the channel groups. Valid range is from 1 through 255.

mode

Specifies the LAG mode of the interface.

on

Specifies that all LAGs that are not running LACP remain in this mode. This is the default mode.

active

Enables LACP on the specified interface.

passive

Enables LACP only if an LACP device is detected.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

The LAG in the `on` channel mode is a pure LAG (static-lag), and can aggregate a maximum of 64 ports.

Validations for the command are as follows:

- The channel-group must be already present.
- MTU must not be configured.
- A port must be mapped with only one channel-group.
- The speed of the member ports must be same as the current port.
- The ingress-group or egress object configured on an interface cannot be configured as a member port of the port- channel.

The `no channel-group` command removes the interface from the channel-group.

Examples

The following examples configure a physical interface to the channel-group.

```
device# configure terminal
device# interface ethernet 1/1
device#(config-if-eth-1/1)# channel-group 1 mode on
device#(config-if-eth-1/1)# no shutdown
device#(config-if-eth-1/1)# end

device# show running-config
interface ethernet 1/1
  channel-group 1 mode on
  no shutdown

device# configure terminal
device(config)# interface port-channel 100
device(config-if-po-100)# no shutdown
device(config-if-po-100)# exi
device(config)#
device(config)# interface ethernet 1/8:1
device(config-if-eth-1/8:1)# channel-group 100 mode active

device# show running-config
protocol lacp
hardware
 connector 1/8
  breakout 4x10g
 connector 2/8
  breakout 4x10g
interface port-channel 100
 no shutdown
interface ethernet 1/8:1
 channel-group 100 mode active
 no shutdown
interface ethernet 1/8:2
```

clear counters access-list

Clears all or specified counters for all configured MAC, IPv4, and IPv6 access lists.

Syntax

clear counters access-list all

clear counters ip access-list [*ACL_NAME* | **all**]

clear counters ipv6 access-list [*ACL_NAME* | **all**]

clear counters mac access-list [*ACL_NAME* | **all**]

Parameters

ACL_NAME

Specifies the name of the access-list.

all

Specifies all configured access-lists.

ip

Specifies the IPv4 access-list.

ipv6

Specifies the IPv6 access-list.

mac

Specifies the MAC access-list.

Modes

Exec mode

Examples

The following examples clear counters for access-lists.

```
device# clear counter ip access-list all
device# clear counter ip access-list v4-acl
device# clear counter ipv6 access-list v6-acl
device# clear counter mac access-list l2-acl
```

The following example displays all MAC access-lists and their counters.

```
device# show mac access-list all

mac access-list L2
  seq 10 permit 02:02:02:02:02:02 02:02:02:02:02:02 02:02:02:02:02:03 02:02:02:02:02:03
( 0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )
```

The following example displays all IP access-lists and their counters.

```
device# show ip access-list all
ip access-list grp_a_deny_1
  seq 10 deny ip 2.2.4.0 255.255.255.0 1.1.1.3 255.255.255.255 ( 5000000 Packets,
1940000000 Bytes, 0 Packets/sec, 0 Bits/sec )
  seq 20 deny ip 2.2.5.0 255.255.255.0 1.1.1.4 255.255.255.255 ( 5000000 Packets,
1940000000 Bytes, 0 Packets/sec, 0 Bits/sec )
ip access-list grp_a_deny_2
  seq 10 deny ip 2.2.6.0 255.255.255.0 1.1.1.5 255.255.255.255 ( 5000000 Packets,
1940000000 Bytes, 0 Packets/sec, 0 Bits/sec )
  seq 20 deny ip 2.2.7.0 255.255.255.0 1.1.1.6 255.255.255.255 ( 5000000 Packets,
1940000000 Bytes, 0 Packets/sec, 0 Bits/sec )
```

The following example verifies that all access-list counters were cleared.

```
device# show ip access-list all
ip access-list grp_a_deny_0
  seq 10 deny ip 2.2.2.0 255.255.255.0 1.1.1.1 255.255.255.255 ( 0 Packets, 0 Bytes, 0
Packets/sec, 0 Bits/sec )
  seq 20 deny ip 2.2.3.0 255.255.255.0 1.1.1.2 255.255.255.255 ( 0 Packets, 0 Bytes, 0
Packets/sec, 0 Bits/sec )
ip access-list grp_a_deny_1
  seq 10 deny ip 2.2.4.0 255.255.255.0 1.1.1.3 255.255.255.255 ( 0 Packets, 0 Bytes, 0
Packets/sec, 0 Bits/sec )
  seq 20 deny ip 2.2.5.0 255.255.255.0 1.1.1.4 255.255.255.255 ( 0 Packets, 0 Bytes, 0
Packets/sec, 0 Bits/sec )
```

clear counters egress

Clears all egress counters.

Syntax

clear counters egress all

Parameters

all

Specifies deletion of all counters for configured egresses.

Modes

Exec mode

Usage Guidelines

This command is ignored silently if an entry is not present.

Examples

The following example clears counters for all egresses.

```
device# clear counters egress all
```

clear counters egress-group

Clears counters for all egress-groups.

Syntax

clear counters egress-group all

Parameters

all

Specifies deletion of counters for all egress groups.

Modes

Exec mode

Usage Guidelines

This command is ignored silently if an entry is not present.

Examples

The following example clears counters for all egress groups.

```
device# clear counters egress-group all
```

clear counters encap

Clears current statistics available on encap.

Syntax

clear counters encap { *name* | **all** }

Parameters

name

Specifies the encap counter name.

all

Specifies all encap counters.

Modes

Encap config mode

Usage Guidelines

Valid encap name must be provided.

Examples

The following example clears `encap_1` counters.

```
device(config-encap)# clear counters encap encap_1

Show running:
device# show encap counters encap_1

Tunnel Encapsulation Statistics(GRE)
    Egress port : ethernet 1/2
      RX Frames : 0
       RX Bytes : 0
```

The following example clears all `encap` counters.

```
device# clear counters encap all
```

The following example shows `encap` counters.

```
device# show counters encap encap-1

Tunnel Encapsulation Statistics(GRE)
    Egress port : ethernet 10/2
      RX Frames : 0
       RX Bytes : 0
mac access-list L2
```

clear counters ingress-group

Clears all or specified counters for all ingress-groups.

Syntax

clear counters ingress-group { *name* | **all** }

Parameters

name

Specifies the name of the ingress-group counter. Supports 1-64 characters.

all

Specifies all ingress-group counters.

Modes

Exec mode

Usage Guidelines

If the ingress group has only the associated ports, the **clear ingress-group counters** command does not clear statistics as it fetches the interface statistics. Interface clear clears the statistics for the ingress group as well.

Examples

The following example clears ingress-group counters.

```
device# clear counters ingress-group ig1

device# clear counters ingress-group all
```

The following example displays all ingress-group counters information.

```
# show counters ingress-group all
Number of ingress-groups: 2
Ingress-group Packet Statistics (Vxlan Tunnel)
        Name : IgVxlanVni100
   RX Frames : 0
    RX Bytes : 0
```

The following example clears counters on all ingress groups and verifies it with the show command.

```
device# clear counters ingress-group all

device# show counters ingress-group all
Number of ingress-groups: 2
        Name : ig_01
No ingress-group stats found
```

```
         Name : ig_02
No ingress-group stats found
```

clear counters interface

Clears counters of the specified interface.

Syntax

clear counters interface ethernet [*IFNAME* | **all**]

clear counters interface management *number*

clear counters interface port-channel [*PORANGE* |**all**]

Parameters

ethernet

Specifies the counters of Ethernet interfaces.

IFNAME

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

all

Clears all Ethernet interface counters.

management *number*

Specifies the management interface.

port-channel

PORANGE

Specifies the channel number or range of channel numbers. Valid range is 1 to 255.

all

Specifies all port-channel interfaces.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example clears counters of the Ethernet interface on slot/port 1/1.

```
device# clear counters interface ethernet 1/1
```

The following example clears counters on management interface 0.

```
device# clear counters interface management 0
```

The following example clears port-channel 1 counters.

```
device# clear counters interface port-channel 1

device# clear counters interface port-channel 1-3,5,7-9
```

The following example clears counters for all Ethernet interfaces.

```
device# clear counters interface ethernet all
```

clear counters lacp

Clears all LACP counters.

Syntax

clear counters lacp

Parameters

counters lacp

Specifies the LACP counters.

Modes

Exec mode

Examples

The following example clears LACP counters.

```
device# clear counters lacp
```

clear counters lacp interface

Clears all LACP port-channel counters.

Syntax

clear counters lacp interface port-channel *PORANGE*

Parameters

port-channel *PORANGE*

Specifies the channel number or range of channel numbers assigned to the Ether Channel logical interface. Valid range is 1-255. Example: 1,1-3,5,7-9.

Modes

Config mode

Examples

The following example clears the LACP port channel counters.

```
device# configure terminal

device(config)# clear counters lacp interface port-channel 100,200
```

clear counters listener-policy

Clears the counters of the specified or all configured listener-policies.

Syntax

clear counters listener-policy [*POLICY_NAME* | **all**]

clear counters ip access-list [*ACL_NAME* | **all**] **listener-policy** [*POLICY_NAME* | **all**]

clear counters ipv6 access-list [*ACL_NAME* | **all**] **listener-policy** [*POLICY_NAME* | **all**]

clear counters mac access-list [*ACL_NAME* | **all**] **listener-policy** [*POLICY_NAME* | **all**]

Parameters

ACL_NAME

Specifies the name of the access-list.

POLICY_NAME

Specifies the name of the listener policy.

all

Specifies counters information for all access-lists or listener policies.

ip

Specifies the IPv4 access-list.

ipv6

Specifies the IPv6 access-list.

mac

Specifies the MAC access-list.

Modes

Exec mode

Examples

The following example clears counters for listener-policies.

```
device# clear counters listener-policy lp1

device# clear counters listener-policy lp1 ipv6 access-list all

device# clear counters listener-policy lp1 mac access-list macAcl

device# clear counters mac access-list l2-acl listener-policy lp1
```

clear counters lldp all

Clears all LLDP counters.

Syntax

clear counters lldp all

Parameters

all

Specifies all interfaces.

Modes

This command is supported in all modes.

Examples

The following examples clears LLDP counters information.

```
device# clear counters lldp all
```

clear counters lldp interface ethernet

Clears LLDP counters information.

Syntax

clear counters lldp

clear counters lldp interface ethernet [*IFNAME* | **all**]

Parameters

interface ethernet

Specifies the interface name.

IFNAME

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

all

Specifies all interfaces.

Modes

This command is supported in all modes.

Examples

The following examples clear LLDP counters information.

```
device# clear counters lldp all

device# clear counters lldp interface ethernet 1/1
```

clear counters route-map

Clears the counters of the specified or all configured route-maps.

Syntax

clear counters route-map [*ROUTE_MAP_NAME* | **all**]

clear counters ip access-list [*ACL_NAME* | **all**] **route-map** [*ROUTE_MAP_NAME* | **all**]

clear counters ipv6 access-list [*ACL_NAME* | **all**] **route-map** [*ROUTE_MAP_NAME* | **all**]

clear counters mac access-list [*ACL_NAME* | **all**] **route-map** [*ROUTE_MAP_NAME* | **all**]

Parameters

ACL_NAME

Specifies the name of the access-list.

ROUTE_MAP_NAME

Specifies the name of the route-map.

all

Specifies counters information for all access-lists or route-maps.

ip

Specifies the IPv4 access-list.

ipv6

Specifies the IPv6 access-list.

mac

Specifies the MAC access-list.

Modes

Exec mode

Examples

The following examples clears counters for route-maps.

```
device# clear counters route-map all

device# clear counters route-map all ip access-list ipv4Acl

device# clear counters ip access-list v4-acl route-map r1

device# clear counters ipv6 access-list v4-acl route-map all
```

clear counters transport-tunnel

Clears the specified or all counters for transport tunnels.

Syntax

clear counters transport-tunnel [**all** | *name*]

Parameters

all

Specifies all transport-tunnels.

name

Specifies the name of the transport-tunnel.

Modes

Exec mode

Usage Guidelines

You must have the admin role to run this command.

Examples

The following example clears counters for all transport tunnels.

```
device# clear counters transport-tunnel all
```

clock set

Sets the clock date and time.

Syntax

clock set *date - time*

Parameters

set *date - time*

Sets the clock date and time.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example configures clock date and time.

```
device# clock set
TIME dateTime (CCYY-MM-DDTHH:MM:SS)

device# clock set 23423423-23-21T23:00:00
Failed to parse time specification: 23423423-23-21 23:00:00
```

clock timezone

Configures the system time zone.

Syntax

clock timezone *region / city*

no clock timezone *region / city*

Parameters

timezone *region / city*

Specifies the supported time zone.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

The `no clock timezone` resets the system clock to default UTC.

Examples

The following example configures the time zone for Los Angeles.

```
device(config)# clock timezone America/Los_Angeles
```

connector

Configures the connector.

Syntax

connector *slot/port*

Parameters

slot/port

Specifies the name of the connector in slot/port format.

Modes

Hardware configuration mode

Examples

The following example shows how to configure the connector.

```
device(config)# hardware
device(config-hardware)# connector 1/2
device(config-connector-1/2)
```

copy default-config

Clears the running configuration.

Syntax

copy default-config running-config

Parameters

default-config

Specifies the default configuration.

running-config

Specifies the current running configuration.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

After running this command, the system reboots with the management interface configuration.

Examples

The following example replaces the running configuration with the default configuration.

```
device# copy default-config running-config

This operation will modify your running configuration.
WARN: system will be rebooted to have configuration changes to take effect!

Do you want to continue? [y/n]:
Reloading.... please wait
```

copy FILE

Copies contents of a configuration file from the specified location to the running configuration.

Syntax

copy FLASH-FILE running-config

copy REMOTE-FILE running config

copy USB-FILE running-config

Parameters

running-config

Specifies the current running configuration.

FLASH-FILE

Specifies the flash file path in format `flash://flash-type/file-name`.

REMOTE-FILE

Specifies the remote server file path in format `scp://username:password@host[:port]/filepath`.

Domain name, IPv4 address, and IPv6 address are supported as host. Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

USB-FILE

Specifies the USB file path in format `usb://file-name`.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Valid user credentials must be provided for accessing the remote server.

Input config file path must be valid.

Examples

The following examples are some valid **copy** commands.

```
device# copy flash://config-file/testfile running-config

device# scp://test:test@1.1.1.1:22/home/test/config-file/testfile running-config

device# copy usb://testfile running-config
```

copy FILE1 FILE2

Copies a flash or USB file to a remote server and vice versa.

Syntax

copy FLASH-FILE FLASH-FILE

copy FLASH-FILE USB-FILE

copy FLASH-FILE REMOTE-FILE

copy USB-FILE FLASH-FILE

copy USB-FILE USB-FILE

copy USB-FILE REMOTE-FILE

copy REMOTE-FILE FLASH-FILE

copy REMOTE-FILE USB-FILE

Parameters

FLASH-FILE

Specifies the flash file path in format `flash://flash-type/file-name`.

REMOTE-FILE

Specifies the remote server file path in format `scp://username:password@host[:port]/filepath`.

Domain name, IPv4 address, and IPv6 address are supported as host. Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

USB-FILE

Specifies the USB file path in format `usb://file-name`.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Valid user credentials must be provided for accessing the remote server.

Input file path must be valid.

Target destination must be reachable.

Copying a file from one remote server to another remote server is not supported.

Examples

The following example copies a file from the USB to a remote location.

```
device# copy usb://testfile  scp://testuser:testpassword@1.1.1.1:22/home/testuser/test123
```

copy running-config

Copies the running configuration to the specified file to create a backup.

Syntax

copy running-config FLASH-FILE

copy running-config REMOTE-FILE

copy running-config USB-FILE

Parameters

running-config

Specifies current running configuration.

FLASH-FILE

Specifies the flash file path in format `flash://flash-type/file-name`.

REMOTE-FILE

Specifies the remote server file path in format `scp://username:password@host[:port]/filepath`.

Domain name, IPv4 address, and IPv6 address are supported as host. Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

USB-FILE

Specifies the USB file path in format `usb://file-name`.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Valid user credentials must be provided for accessing the remote server.

The file path must be valid.

The target destination file must be reachable.

Examples

The following example copies the running configuration to the specified file.

```
device# copy running-config flash://config-file/testfile

device# copy running-config scp://test:test@1.1.1.1:22/home/test/testfile

device# copy running-config usb://testfile
```

crypto export

Exports the default CA certificate from the device to the remote host in PEM format.

Syntax

crypto export [**ca-certificate default**] [**protocol** [**scp** | **sftp**]]
[**remote-server** *ADDRESS*] [**remote-file** *FILE*] [**user** *NAME*]
[**password** *NAME*]

Parameters

ca-certificate default

Specifies the default CA certificate.

protocol [**scp** | **sftp**]

Specifies the protocol used for sending the CA certificate.

remote-server *ADDRESS*

Specifies the IPv4 or IPv6 unicast address of the remote server.

remote-file *FILE*

Specifies the remote file name to copy the CA certificate. Supports 1-512 characters.

user *NAME*

Specifies the remote user to copy the CA certificate. Supports 1-64 characters.

password *NAME*

Specifies the remote user password. Supports 1-64 characters.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example exports the default CA certificate from the switch to the remote-server.

```
device# crypto export ca-certificate default protocol scp remote-server 10.37.16.211
remote-file /root/temp/test.txt user root password root123
Exporting switch 'default' CA certificate...
Exported switch 'default' CA certificate successfully.
```

crypto import-pkcs

Imports a TLS server certificate and a private key in PKCS12 format.

Syntax

crypto import-pkcs type [**https**] **protocol** [**scp** | **sftp**] [**host** *ip-address*] [**file** *cert-file*] [**passphrase** *passphrase*] [**user** *remote-user*] [**password** *password*]

no crypto import type [**https**]

Parameters

protocol

scp

Specifies use of SCP for accessing the certificate file.

sftp

Specifies use of SFTP for accessing the certificate file.

type https

Indicates that the certificate is used for HTTPS server authentication.

host *remote-ip*

Specifies the IPv4 or IPv6 unicast address of the remote server where the file is located.

user *remote-user*

Specifies the remote user with access to the file. Supports 1-64 characters.

password *remote-user-password*

Specifies the password for the remote user.

Note
As a best practice, do not list the password in the command line for security purposes. The user is prompted for the password.

file *certificate-and-key-file*

Specifies the PKCS file to retrieve. Supports 1-512 characters.

pkcspassphrase *passphrase*

Specifies the passphrase to unlock the file. Supports 1-64 characters.

Modes

Exec mode

Usage Guidelines

Use this command to import a TLS server certificate and private key (in PKCS12 format) to a device and establish a secure connection.

The `no` form of the command removes the installed PKCS-format files.

Examples

The following example specifies HTTPS authentication and SCP for the certificate file `ngnpb.pkcs`.

```
device# crypto import-pkcs protocol scp type https host 10.24.12.111 user testuser
password password file ngnpb.pkcs pkcspassphrase passphrase

HTTPS server certificate imported.

Installing https certificate will result in a momentary delay and may affect active CLI
connections - please be patient.
Successfully imported file: ngnpb.pkcs
```

The following example removes the installed PKCS-format files.

```
device# no crypto import-pkcs type https
```

crypto import type

Imports the authentication certificate for security configuration.

Syntax

crypto import type [**https** | **syslogca**] **protocol** [**scp** | **sftp**] [**host** *ip-address*] [**certificate** *cert-file*] [**key** *key-file*] [**user** *remote-user*] [**password** *remote-password*]

no crypto import type [**https** | **syslogca**]

Parameters

type

https

Specifies an HTTPS certificate.

syslogca

Specifies a Syslogca certificate

host *ip-address*

Specifies the IPv4 or IPv6 unicast address of the remote server where the file is located.

protocol

scp

Specifies the use of SCP for accessing the certificate file.

sftp

Specifies the use of SFTP for accessing the certificate file.

certificate *file-name*

Defines the name of the certificate file.

key *key-file*

Specifies the key file to retrieve.

username

Specifies the name of the remote user that has access to the file.

password *user-password*

Defines the password for the user name on the host server. The password for a remote user can be up to 64 characters.

Note
As a best practice, do not list the password in the command line for security purposes.

Modes

Exec mode

Usage Guidelines

The `no` form of the command removes the authentication certificate.

When the `no` form of the command is used with **`https`** type, a new certificate or key pair is regenerated and used with the ingress controller.

This command is available only to users with the admin role.

Examples

The following example imports the certificate key pair using SCP.

```
device# crypto import type https protocol scp host
10.37.16.211 certificate /root/certMgmt/certificates/ngnpbTestCA_Cert.pem key /root/
certMgmt/certificates/ngnpbTestCA.key user root password root123
Installing https certificate will result in a momentary delay and may affect active CLI
connections - please be patient.
```

The following example deletes an HTTPS certificate.

```
device# no crypto import type https
device#
```

decap

Decapsulates the current tunnel of the received packet.

Syntax

decap

no decap

Modes

Route-map config mode

Listener-policy config mode

Usage Guidelines

Enabled in route-map mode: Decapsulates a particular encapsulation header in the packet and process remaining packet in further processing blocks. The scope of the headers is shifted to inner headers automatically.

Enabled in listener-policy mode: Terminates the incoming tunneled packets and strips the tunneled header. The payload of the tunneled packet is forwarded to the egress.

The **no decap** command removes the decapsulation action from the route map.

Examples

The following example enables the decap function in route-map configuration mode and then uses the show command to verify the setting.

```
device# configure terminal
device(config)# route-map rmap1 10
device(config-route-map)# decap

device# show route-map all
route-map rmap1 10
forward-action deny
decap

Policy matches: 0 packets, 0 bytes, 0 Packets/secRate, 0 Bits/sec
```

The following example enables the decap function in listener-policy configuration mode.

```
device# configure terminal
device(config)# listener-policy lp1 100
device(config-listener-policy)# decap
```

The following example removes the decap function from a route-map for `rmap1 10`.

```
device# configure terminal
device(config)# route-map rmap1 10
device(config-route-map)# no decap
```

delete

Deletes a flash or USB file.

Syntax

delete FLASH-FILE

delete USB-FILE

Parameters

FLASH-FILE

Specifies the flash file path in format `flash://flash-type/file-name`.

USB-FILE

Specifies the USB file path in format `usb://file-name`.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Valid input file path must be provided.

The active PCAP file cannot be deleted.

Examples

The following examples show how to delete configuration files.

```
device# delete flash://config-file test.txt
Warning: File flash://config-file/test.txt will be deleted (from flash).
Do you want to continue? [y/n]:

device# delete usb://test
Warning: File usb://test will be deleted (from usb).
Do you want to continue? [y/n]:
```

The following example deletes a PCAP file.

```
device# delete flash://pcap-file/test.pcap
```

The following example deletes a system-created file.

```
device# delete flash://config-file/
Warning: File flash://config-file/ will be deleted (from flash).
Do you want to continue? [y/n]: y
```

description

Sets the description for a route map, listener policy, interface, mirror object, or a Quality of Service (QoS) forwarding group.

Syntax

description *description-string*

no description

Parameters

description-string

Specifies the description of the route map, listener policy, interface, mirror object, or forwarding group.

Maximum length of the description is 63 characters. Special characters are allowed.

Modes

Route-map config mode

Listener-policy config mode

Interface config mode

Mirror config mode

QoS config mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following examples show how to configure a description for an interface.

```
device# configure terminal
device(config)# route
device(config-if-eth 1/10)# description Ethernet Interface 1/10 (100G)

device# show running interface ethernet 1/10
interface ethernet 1/10
description Ethernet Interface 1/10 (100G)
shutdown
```

The following examples show how to configure a description for a listener policy.

```
device# configure terminal
device(config)# listener-policy lp-12
device(config-listener-policy)# description listener policy 12
```

```
device# show listener-policy lp-12
interface ethernet 1/10
description listener-policy 12
shutdown
```

The following example shows how to configure a description for a route map.

```
device# configure terminal
device(config)# route-map rmap10
device(config-route-map)# description rmap10 configured Month Date, Year
```

The following example displays the specified route-map.

```
device# show route-map rmap10
interface ethernet 1/10
description rmap10 configured Month Date, Year
no shutdown
```

The following examples show how to configure a description for a mirror object, then display the mirror object.

```
device(config)# mirror mirr_1
device(config-mirror)# description mirror-1

device# show mirror mirr_1

                  Name : mirr_1
           Description : mirror-1
             Interface : none
```

The following example shows how to create a description of a QoS forwarding group.

```
device#(config-qos-group)# description group-for-site-A-to-B
```

deny ipv4-dest

Drops packets that match the configured destination IPv4 address and mask.

Syntax

deny [**ipv4-dest** *addr mask*]

no deny [**ipv4-dest** *addr mask*]

Parameters

ipv4-dest *addr mask*

Specifies the IPv4 address and mask configured in dotted decimal notation. Example: 196.168.0.1.

Modes

Transport tunnel config mode

Usage Guidelines

This command is available only to users with the admin role.

A valid IP address and mask must be provided.

The configured destination IP address must be removed before you configure a new destination IP address.

If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.

Examples

The following example configures the IPv4 address and mask to match and deny further packet processing for transport tunnel tt1 and verifies the configuration with the show command.

```
device(config)# transport-tunnel tt1
device(config-transport-tunnel)# deny ipv4-dest 192.168.4.20 255.255.255.0

device# show running-config transport-tunnel tt1
transport-tunnel tt1
  deny ipv4-dest 192.168.4.20 255.255.255.0
```

deny ipv6-dest

Drops packets that match the configured destination IPv6 address and mask.

Syntax

deny [**ipv6-dest** *addr mask*]

no deny [**ipv6-dest** *addr mask*]

Parameters

ipv6-dest *addr mask*

Specifies the source IPv6 address and mask configured in hexadecimal between 0 and FFFF. Example: 202:304:606:708:90a:b0c:d0e:f11.

The upper 4 bytes and lower 8 bytes of the mask must be zero because only 32 bits out of 128 bits of IPv6 are supported. Example: 0000:0000:FFFF:FFFF:0000:0000:0000:0000.

Modes

Transport tunnel config mode

Usage Guidelines

This command is available only to users with the admin role.

A valid IP address and mask must be provided.

The configured destination IP address must be removed before you configure a new destination IP address.

If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.

Examples

The following example configures the IPv6 address and mask to match and deny further packet processing for transport tunnel tt1 and verifies the configuration with the show command.

```
device(config)# transport-tunnel tt1

device(config-transport-tunnel)#
deny ipv6-dest 1145:456:234:2345:1123:1145:456:234 0000:0000:FFFF:FFFF:0000:0000:0000:000

device# show transport-tunnel tt1
                  Name : tt1
      Source-Ipv6-Addr : 2233:304:606:708:90a:b0c:d0e:f11
      Source-Ipv6-Mask : 0000:0000:FFFF:FFFF:0000:0000:0000:000
Destination-Ipv6-Addr : 1145:456:234:2345:1123:1145:456:234
Destination-Ipv6-Mask : 0000:0000:FFFF:FFFF:0000:0000:0000:000
```

```
           Tunnel-Type : GRE
         Ingress-Group : none

device# show running-config transport-tunnel
transport-tunnel tt1
  tunnel-type gre ipv6-src
2233:304:606:708:90a:b0c:d0e:f11 0000:0000:FFFF:FFFF:0000:0000:0000:000
  deny ipv6-dest
1145:456:234:2345:1123:1145:456:234 0000:0000:FFFF:FFFF:0000:0000:0000:000
```

destination-ipv4-addr

Configures the destination IPv4 address for the encapsulation of outgoing packets.

Syntax

destination-ipv4-addr *ip-addr*

no destination-ipv4-addr *ip-addr*

Parameters

ip-addr

Specifies the IPv4 address to be configured as the destination IP address.

Modes

Encap config mode

Usage Guidelines

Validations for the command are as follows:

- Valid IP addresses must be provided. The following addresses are considered invalid IP addresses:
  - Unspecified IP address (0.0.0.0)
  - Broadcast IP address (255.255.255.255)
  - Multicast IP addresses (224.x.x.x to 240.x.x.x)
- One IP address per encapsulation is allowed. The configured IP address must be removed before you configure a new IP address.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures the destination IP address.

```
device(config-encap-1)# destination-ipv4-addr 20.20.20.1

Show running:
device# show running-configuration

encap encap-1
destination-ipv4-addr 20.20.20.1
```

destination-mac-addr

Configures the destination MAC address for the encapsulation of outgoing packets.

Syntax

destination-mac-addr *mac-addr*

no destination-mac-addr *mac-addr*

Parameters

mac-addr

Specifies the MAC address to be configured as the destination MAC.

Modes

Encap config mode

Usage Guidelines

Validations for the command are as follows:

- A valid MAC address must be provided.
- One MAC address per encapsulation is allowed. The configured MAC address must be removed before you configure a new MAC address.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures the destination MAC address.

```
device(config-encap-1)# destination-mac-addr 00:01:02:03:04:05
device(config-encap-1)#

Show running:
device# show running-configuration

encap encap-1
destination-mac-addr 00:01:02:03:04:05
```

dir

Lists flash and USB directory information.

Syntax

dir [**flash://**[**api-gw** | **chassis-mgr** | **cli** | **config-file** | **coredumps** | **firmware** | **interface-mgr** | **lacp** | **lldp** | **ms-images** | **pcap-file** | **snmp** | **tech-support**]] | [**usb://***filename*]

Parameters

dir

Lists flash directory information.

flash://api-gw

Lists API gateway files.

flash://chassis-mgr

Lists chassis files.

flash://cli

Lists CLI files.

flash://config-file

Lists configuration files.

flash://coredumps

Lists coredump files.

flash://firmware

Lists firmware files.

flash://interface-mgr

Lists interface manager files.

flash://lacp

Lists LACP files.

flash://lldp

Lists LLDP files.

flash://ms-images

Lists ms images files.

flash://pcap-file

Lists PCAP files.

flash://snmp

Lists SNMP files.

flash://tech-support

Lists tech support files.

usb://*filename*

Lists USB files.

Modes

Exec mode

Examples

The following example lists flash directory information.

```
device# dir
config-file :
-rw-r--r-- 790 2021-04-22 05:50:40 comm9.conf
-rw-r--r-- 1047 2021-04-17 09:03:27 temp.conf
-rw-r--r-- 117 2021-04-12 05:54:09 temp2.conf
-rw-r--r-- 73 2021-04-13 06:14:34 temp3.conf
-rw-r--r-- 48 2021-04-13 06:18:08 temp4.conf
-rw-r--r-- 1047 2021-04-17 10:16:18 temp_1618654577.conf
-rw-r--r-- 1047 2021-04-19 11:47:49 temp_1618832866.conf
pcap-file :
-rw-r--r-- 0 2021-06-01 08:03:44 README.md
tech-support :
firmware :
ms-images  :

drwxr-xr-x  4096  2021-12-16 21:13:24  api-gw
drwxr-xr-x  4096  2021-12-16 21:13:24  chassis-mgr
drwxr-xr-x  4096  2021-12-16 21:13:24  cli
drwxr-xr-x  4096  2021-12-16 21:13:24  config-db
drwxr-xr-x  4096  2021-12-16 21:13:24  interface-agent
drwxr-xr-x  4096  2021-12-16 21:13:24  interface-mgr
drwxr-xr-x  4096  2021-12-16 21:13:24  lacp
drwxr-xr-x  4096  2021-12-16 21:13:24  lldp
drwxr-xr-x  4096  2021-12-16 21:13:24  msg-bus
drwxr-xr-x  4096  2021-12-16 21:13:24  nexthop-agent
drwxr-xr-x  4096  2021-12-16 21:13:24  packet-mgr
drwxr-xr-x  4096  2021-12-16 21:13:24  pbd-agent
drwxr-xr-x  4096  2021-12-16 21:13:24  pcap-agent
drwxr-xr-x  4096  2021-12-16 21:13:24  persistent-state-db
drwxr-xr-x  4096  2021-12-16 21:13:24  pipeline-agent
drwxr-xr-x  4096  2021-12-16 21:13:24  security
drwxr-xr-x  4096  2021-12-16 21:13:24  sfcs-agent
drwxr-xr-x  4096  2021-12-16 21:13:24  snmp
drwxr-xr-x  4096  2021-12-16 21:13:24  state-db
drwxr-xr-x  4096  2021-12-16 21:13:24  stratum
drwxr-xr-x  4096  2021-12-16 21:13:24  svcplane-agent
drwxr-xr-x  4096  2021-12-16 21:13:24  target-proxy-agent

chassis-mgr:
interface-mgr:
lacp:
lldp:
cli:
api-gw:
snmp:
coredumps:
-rw------- 273702912 2021-05-28 10:08:07 core.npbcli.PID_13825.SIG_6.16
22196487

USB:
```

```
-rw-r--r-- 734 2021-05-11 04:49:58 test
-rw-r--r-- 734 2021-05-06 18:33:36 test1
-rw-r--r-- 734 2021-05-14 04:04:07 test123
-rw-r--r-- 734 2021-05-06 18:24:01 testfile

device# dir usb://
USB:
-rw-r--r-- 734 2021-05-11 04:49:58 test
-rw-r--r-- 734 2021-05-06 18:33:36 test1
-rw-r--r-- 734 2021-05-14 04:04:07 test123
-rw-r--r-- 734 2021-05-06 18:24:01 testfile
```

egress

Creates or deletes an egress.

Syntax

egress *name*

no egress *name*

Parameters

name

Specifies the name of the configured egress object.

Supports 1-32 characters. Characters allowed are alpha-numeric, underscore and dot. Underscore is not allowed as the first character.

Modes

Config mode

Egress config mode

Usage Guidelines

This command is available only to users with the admin role.

A valid egress name must be provided. The reserved name, **all**, cannot be used for configuration.

An egress name must be unique. An error is returned if you try to use the same name for an egress as for an egress group.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

The **no** form of the command deletes the specified egress name.

Examples

The following example creates egress-123.

```
device(config)# egress egress-100
device(config-egress)# precedence 10 interface ethernet 1/10
device(config-egress)# set encap-100
device(config-egress)# set listener-policy lp-100

device# show running-config egress
Egress egress-100
Precedence 10 interface ethernet 1/10
```

```
encap-100
lp-100
```

egress-group

Creates or removes an egress-group.

Syntax

egress-group *name*

no egress-group *name*

Parameters

name

Specifies the name of the egress-group. Supports 1-32 characters.

Characters allowed are alpha-numeric, underscore, and dot. Underscore is not allowed as the first character.

Modes

Config mode

Usage Guidelines

A maximum of 64 egress objects can be added to an egress-group.

A valid egress name must be provided.

An egress-group name must be unique. An error is returned if you try to use the same name for an egress-group as for an egress.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

The **no** form of the command deletes the specified egress-group.

Examples

The following example creates an egress group named MyEgressGroup.

```
device(config)# egress-group MyEgressGroup
```

enable acl-counter

Enables or disables ACL counters globally.

Syntax

enable acl-counter

no enable acl-counter

Modes

ACL config mode

Usage Guidelines

The **enable acl-counter** command is enabled by default.

When this command is enabled, ACLs update their count to the extreme-policy-statistics module in the Extreme YANG tree.

The **show running configuration** command does not show the **enable acl-counter** command because it is the default value.

When the **enable acl-counter** command is disabled, the `count` option in ACL rules comes into effect. The count is published to the extreme-policy-statistics module and other control plane applications for ACL rules that explicitly specify the count option.

The **no** form of the command disables ACL counters globally.

Examples

The following examples shows how to configure ACL counters.

```
device(conf)# acl-config
device(conf-acl-config)# enable acl-counter
device(config)# ip access-list acl-ipv4-1
device(config-ip-acl)# seq 10 permit tcp any any count
     <- This ACL clause will display count.
device(config-ip-acl)# seq 20 deny ip any any
     <- This ACL clause also will display count.

device(conf)# acl-config
device(conf-acl-config)# no enable acl-counter
device(config)# ip access-list acl-ipv4-1
device(config-ip-acl)# seq 10 permit tcp any any count
    <- This ACL clause will display count.

device(config-ip-acl)# seq 20 deny ip any any
    <- This ACL clause will not display count.

device# show running-config acl-config

acl-config
no enable acl-counter
```

encap

Configures encapsulation parameters for the outgoing packets.

Syntax

encap *name*

no encap *name*

Parameters

name

Specifies the name of the encap object. Supports 1-64 characters.

The name must start with an alphabet character or an underscore.

Modes

Config mode

Encap config mode

Usage Guidelines

Validations for the command are as follows:

- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.
- If the **no** form of the command is run with the configuration, all sub-mode configurations are removed along with the encap object.
- The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Examples

The following example configures encapsulation parameters for encap-1.

```
device(config)# encap encap-1
device(config-encap-1)#
```

encap-type

Configures encapsulation type for outgoing packets.

Syntax

encap-type gre

no encap-type gre

Parameters

gre

Sets encapsulation type to GRE.

Modes

Encap config mode

Usage Guidelines

Validations for the command are as follows:

- The `encap-type` cannot be modified or deleted when the encap is associated with the egress object.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following examples show GRE encapsulation.

```
device# configure terminal
device(config)# encap encap-1
device(config-encap)# encap-type gre

Show running:
device# show running-config encap
encap encap-1
  encap-type gre
```

fec

Configures Forward Error Correction (FEC) mode.

Syntax

fec [**fc-fec** | **rs-fec** | **auto-negotiation** | **disabled**]

Parameters

fc-fec

Configures FC-FEC in manual mode.

rs-fec

Configures RS-FEC in manual mode.

auto-negotiation

Configures FEC auto negotiation.

disabled

Disables FEC.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is supported only on ports with 100G or 25G speed.

The interface must be disabled before changing the FEC configuration.

Speed configuration is not allowed when FEC is configured.

Examples

The following examples show FEC configuration.

```
device(config)# int e 4/16
device(config-if-eth-4/16)# fec fc-fec

device(config)# int e 4/16
device(config-if-eth-4/16)# channel-group 111 mode on
device(config-if-eth-4/16)# fec rs-fec

device# show int e 4/16
ethernet 4/16 Admin state DOWN    Operational state DOWN
 Interface index is 268435744 (0x10000120)
 MTU 0 bytes
 Hardware is Ethernet  mac address 40:88:2f:c1:02:43
Current Speed  100G
FEC Mode: RS-FEC
```

```
Statistics
 Carrier Transitions: 0
           LastClear: 0s
Input:
          Broadcast Pkts: 0
            Discard Pkts: 0
             Errors Pkts: 0
              FCS Errors: 0
              MCast Pkts: 0
                  Octets: 0
              UCast Pkts: 0
       Unknown Protocols: 0
Out:
          Broadcast Pkts: 0
            Discard Pkts: 0
             Errors Pkts: 0
              MCast Pkts: 0
                  Octets: 0
              UCast Pkts: 0
```

forward-action

Determines the actions performed on a packet for the current route map or listener-policy.

Syntax

forward-action { **permit** | **deny** }

Command Default

Default is **permit**.

Parameters

permit

Modifies outgoing packets according to specified matching actions. Otherwise, it tries to match the condition in the next instance of the same listener-policy. If a match is not found, the packet is forwarded without applying any actions.

deny

Skips the matching listener policy instance and drops traffic.

Modes

Route-map config mode

Listener-policy config mode

Examples

The following example allows packet forwarding based on the ACL for the current route map.

```
device# configure terminal
device# config-route-map
device(config-route-map)# forward-action permit
```

The following example allows packet forwarding based on the ACL for the current listener policy.

```
device# configure terminal
device(config)# listener-policy lp1 <sId>
device(config-listener-policy)# forward-action permit

device# show listener-policy rt 45
  forward-action permit
```

The following example blocks packet forwarding and drops packets for the current route map.

```
device# config-route-map
device(config-route-map)# forward-action deny
```

hardware

Enters the hardware mode.

Syntax

hardware

Parameters

hardware

Allows hardware configuration.

Modes

Config mode

Examples

The following example shows how to enter the hardware mode.

```
device(config)# hardware
device(config-hardware)#
```

ingress-group

Configures or removes an ingress group for classifying the packets received on the interface.

Syntax

ingress-group *name*

no ingress-group {*name* | **all** }

Parameters

name

Specifies the name of the ingress group to be used for packets received on the interface.

all

Deletes all configured ingress groups. Use of this parameter deletes interface binding also.

Modes

Config mode

Usage Guidelines

The **no** form of the command deletes a specified ingress group or all configured ingress groups.

Removal of an ingress-group fails silently if the group is not present.

Examples

The following example configures the ingress group, binds route-map rm1 to this ingress group, and then verifies the configuration.

```
device# configure terminal
device(config)# ingress-group group-1
device(config-ingress-group)#  set route-map rm1

device# show running-config ingress-group
ingress-group ingress-group-1
  set route-map rm1
```

interface ethernet

Changes the configuration mode to interface or range of interfaces.

Syntax

Interface ethernet *IFNAME*

Parameters

IFNAME

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following examples change the config mode to interface configuration mode.

```
device# configure terminal
device(config)# interface ethernet 1/10-14
device(config-if-eth 1/10-14)#

device(config)# int e 1/1-16,2/1-16
device(config-if-eth-1/1-16,2/1-16)#

device(config-hardware)# int e 1/2:1-4,2/1-16
device(config-if-eth-1/2:1-4,2/1-16)#
```

interface port-channel

Creates a port-channel or changes the configuration mode to an already created port-channel or a range of port-channels.

Syntax

interface port-channel *PORANGE*

no interface port-channel *PORANGE*

Parameters

PORANGE

Specifies the channel number or range of multiple channel numbers. The valid range is 1 through 255.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

The packets are load balanced on member port-channel ports when a port-channel is added as part of the egress.

The `no interface port-channel PORANGE` command deletes the LAG group.

Examples

The following example configures the link aggregation group.

```
device# configure terminal
device(config)# interface port-channel 1
device(config-if-po-1)# no shutdown

device# configure terminal
device(config)# interface port-channel 1-3,5,7-9
device(config-if-po-1-3,5,7-9)# no shutdown
```

ip access-list

Creates an IP access control list (ACL). ACLs contain rules that permit or deny traffic based on packet fields belonging to the IPv4 family of protocols.

Syntax

ip access-list *name*

no ip access-list *name*

Parameters

name

Specifies the name of the IP access list.

Modes

Config mode

Usage Guidelines

Command-line mode changes from `(config)` to `(config-ip-acl)` after new IP ACL is created.

Names cannot exceed 64 characters and must start with an alphabetic character or an underscore, followed by alphabetic or numeric characters or dots.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Examples

The following example creates an ACL named P4. On successful creation the mode changes to `config-ip-acl`.

```
device# configure terminal
device(config)# ip access-list P4
device(config-ip-acl)#

device# show running-config ip access-list P4
ip access-list P4

device# show running-config ip access-list all
ip access-list P4
```

The following example deletes the ACL named P4.

```
device# configure terminal
device(config)# no ip access-list P4
```

ip address

Configures the IPv4 address for the interfaces.

Syntax

ip address *A.B.C.D/M*

ip address *dhcp*

no ip address *A.B.C.D/M*

no ip address *dhcp*

Parameters

A.B.C.D/M

Specifies the valid IPv4 unicast address.

dhcp

Specifies the DHCP IPv4 address.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is supported on management interfaces.

The **no ip address** command removes the IPv4 address configured on the interface.

The **no ip address dhcp** command removes the DHCP IPv4 address configured on the interface.

Examples

The following example configures the IPv4 address.

```
device# configure terminal
device(config)# interface management 0
device(config-if-mgmt-0)# ip address 192.168.122.10/24

device# show running interface management 0
interface management 0
no ip address dhcp
ip address 192.168.122.10/24
shutdown
```

The following example configures the DHCP IPv4 address.

```
device# configure terminal
device(config)# interface management 0
device(config-if-mgmt-0)# ip address dhcp

device# show running interface management 0
interface management 0
ip address dhcp
shutdown
```

ip dns

Configures the DNS IP address.

Syntax

ip dns domain-name *NAME*

ip dns name-server [*A.B.C.D* | *XX:XX::XX*]

no ip dns domain-name *NAME*

no ip dns name-server [*A.B.C.D* | *XX:XX::XX*]

Parameters

domain-name *NAME*

Specifies the DNS domain name.

name-server *A.B.C.D* | *XX:XX::XX*

Specifies the IPv4 or IPv6 address of the DNS name server.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

A maximum of six DNS domain names is supported.

A maximum of three DNS name servers is supported.

The `no ip dns domain-name` command removes the specified DNS domain name.

The `no ip dns name-server` command removes the specified DNS name server.

Examples

The following example configures IP DNS domain name.

```
device(config)# ip dns domain-name extreme.com

device(config)# ip dns domain-name corp.extreme.com

device(config)# do sh running-config ip dns
ip dns domain-name corp.extremenetworks.com
ip dns domain-name extremenetworks.com
ip dns name-server 10.6.16.32
ip dns name-server 10.6.24.30
ip dns name-server 1111:2222::1
```

The following example configures IP DNS name server.

```
device(config)# ip dns name-server 10.6.16.32

device(config)# ip dns name-server 1111:2222::1

device# sh running-config ip dns
ip dns name-server 10.6.16.32
ip dns name-server 1111:2222::1
```

ip gateway

Configures an IPv4 gateway for the interfaces.

Syntax

ip gateway *A.B.C.D*

no ip gateway *A.B.C.D*

Parameters

A.B.C.D

Specifies the IPv4 address of the gateway.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is supported on management interfaces.

Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

The **no** form of the command removes the IP address configured on the interface.

Examples

The following example configures an IPv4 gateway.

```
device# configure terminal
device(config)# interface management 0
device(config-if-mgmt-0)# ip gateway 192.168.122.1

device# show running interface management 0
interface management 0
no ip address dhcp
ip address 192.168.122.10/24
ip gateway 192.168.122.1
shutdown
```

ipv6 access-list

Creates an IPv6 access list that contains rules that permit or deny traffic based on packet fields of the IPv6 family of protocols.

Syntax

ipv6 access-list *name*

no ipv6 access-list *name*

Parameters

name

Specifies the name of the IPv6 access list.

Modes

Config mode

Usage Guidelines

Names cannot exceed 64 characters and must start with an alphabetic character or an underscore, followed by alphabetic or numeric characters or dots.

On successful completion, the CLI mode changes from `config` to `ipv6-acl`.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Examples

The following example creates an IPv6 access list, P6.

```
device# configure terminal
device(config)#ipv6 access-list P6
device(config-ipv6-acl)#

device# show running-config ipv6 access-list ip6-acl
ipv6 access-list ip6-acl

device# show running-config ipv6 access-list all
ipv6 access-list ip6-acl
```

ipv6 address

Configures the IPv6 address for the interfaces.

Syntax

ipv6 address *A:B::C:D/M*

no ipv6 address *A:B::C:D/M*

ipv6 address *dhcp*

no ipv6 address *dhcp*

Parameters

A:B::C:D/M

Specifies the IPv6 address configuration.

dhcp

Specifies the DHCP IPv6 address.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is supported on management interfaces.

Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

The command `no ipv6 address` removes the IPv6 address configured on the interface.

The command `no ipv6 address dhcp` removes the DHCP IPv6 address configured on the interface.

Examples

The following example configures the IPv6 address.

```
device# configure terminal
device(config)# interface management 0
device(config-if-mgmt-0)# ipv6 address 2001:db8:fe::100/120

device# show running interface management 0
interface management 0
ipv6 address 2001:db8:fe::100/120
shutdown
```

The following example configures the DHCP IPv6 address.

```
device# configure terminal
device(config)# interface management 0
device(config-if-mgmt-0)# ipv6 address dhcp

device# show running interface management 0
interface management 0
ipv6 address dhcp
shutdown
```

ipv6 gateway

Configures an IPv6 gateway for the interfaces.

Syntax

ipv6 gateway *A:B::C:D*

no ipv6 gateway *A:B::C:D*

Parameters

A:B::C:D

Specifies the IPv6 address for the gateway.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is supported on management interfaces.

Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

The **no** form of the command removes the IP gateway on the interface.

Examples

The following example configures an IPv6 gateway.

```
device# configure terminal
device(config)# interface management 0
device(config-if-mgmt-0)# ipv6 gateway 2001:db8:fe::2

device# show running interface management 0
interface management 0
ipv6 gateway 2001:db8:fe::2
shutdown
```

lacp min-links

Configures or resets the minimum number of active member links required for the port-channel to be operationally UP.

Syntax

lacp min-links *min-link-number*

no lacp min-links *min-link-number*

Parameters

min-links *min-link-number*

Specifies the minimum number of active member links required for the port-channel to be operationally UP. The range is 1 through 64. The default value is 1.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

The **no** form of the command resets the minimum LACP threshold to the default value 1.

Examples

The following example configures the minimum LACP threshold.

```
device# configure terminal
device(config)# interface port-channel 1
device(config-if-po-1)# lacp min-links 3
device(config-if-po-1)# end

device# show running-configuration
interface port-channel 1
lacp  min-links 3
no shutdown
```

lacp port-priority

Configures or resets the port priority for use with LACP.

Syntax

lacp port-priority *NUM*

no lacp port-priority *NUM*

Parameters

port-priority *NUM*

Specifies the port priority. Valid values are from 1 through 65535 and higher numbers have a lower priority. The default value is 32768.

Modes

Interface config mode

Usage Guidelines

The `no lacp port-priority` command resets LACP system priority to the default value, 32768.

Examples

The following example configures LACP port priority.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config)# lacp port-priority 40000

device# show running-configuration
protocol lacp
hardware
 connector 1/8
  breakout 4x10g
interface port-channel 1
 no shutdown
interface ethernet 1/8:1
 channel-group 1 mode active
 lacp port-priority 1234
 no shutdown
```

lacp rate

Configures or resets the fast rate at which LACP control packets are received on the LACP supported interface.

Syntax

lacp rate { **fast** | **normal** }

no lacp rate fast

Parameters

rate

Specifies LACP reception interval.

fast

Specifies that the LACP packets are sent at a 1 second interval and 3 second timeout.

normal

Specifies that the LACP packets are sent at 30 second intervals with a 90 second timeout. Default rate is 30 seconds.

Modes

Interface config mode

Usage Guidelines

The **no** form of the command resets the LACP rate interval to the default value, 30 seconds.

Timeout is calculated on the LACP rate. For fast rate, timeout is 3 x 1 = 3 seconds and for normal rate, timeout is 30 x 3 = 90 seconds.

Examples

The following example configures the LACP rate.

```
device# configure terminal
device(config)# interface ethernet 1/8:1
device(config-if-eth-1/8:1)# lacp rate fast

device# show running-config
protocol lacp
 lacp system-priority 1234
hardware
 connector 1/8
  breakout 4x10g
 connector 2/8
  breakout 4x10g
interface port-channel 100
```

```
 no shutdown
interface ethernet 1/1
 shutdown
interface ethernet 1/2
 shutdown
interface ethernet 1/3
 shutdown
interface ethernet 1/4
 shutdown
interface ethernet 1/5
 shutdown
interface ethernet 1/6
 shutdown
interface ethernet 1/8:1
 channel-group 100 mode active
 lacp rate fast
 no shutdown
interface ethernet 1/8:2
```

lacp system-mac

Configures or resets the MAC address to be used for the LACP exchanges.

Syntax

lacp system-mac *mac-address*

no lacp system-mac

Parameters

system-mac *mac-address*

Specifies the MAC address for configuring LACP protocol exchanges. The MAC address format is XXXX.XXXX.XXXX.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

The `no lacp system-mac` command resets LACP system MAC to the default MAC address.

Examples

The following example configures LACP system-mac.

```
device# configure terminal
device(config)#  interface port-channel 100
device(config-if-po-100)# lacp system-mac aabb.ccdd.eeff
device(config-if-po-100)# end

device# show running-config
protocol lacp
 lacp system-priority 1234
hardware
 connector 1/8
  breakout 4x10g
 connector 2/8
  breakout 4x10g
interface port-channel 100
 lacp system-mac aabb.ccdd.eeff
 lacp system-priority 1234
 no shutdown
```

lacp system-priority

Configures or resets the system priority for use with LACP.

Syntax

lacp system-priority *priority*

no lacp system-priority

Parameters

system-priority *priority*

Configures system priority. Valid values are from 1 through 65535, and higher numbers have a lower priority. The default value is 32768.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

The `no lacp system-priority` command resets LACP system priority to the default value, 32768.

Examples

The following example configures LACP system priority.

```
device# configure terminal
device(config)# interface port-channel 100
device(config-if-po-100)# lacp system-priority 1234
device(config-if-po-100)# end

device# show running-config
protocol lacp
 lacp system-priority 1222
hardware
 connector 1/8
  breakout 4x10g
 connector 2/8
  breakout 4x10g
interface port-channel 1
interface port-channel 100
 lacp system-priority 1234
 no shutdown
```

linecard

Configures the specified slot for a line card of a given type.

Syntax

linecard *slot linecard-type*

no linecard *slot*

Parameters

slot

Specifies the line card slot number to be configured. Valid slot range is 1 through 8.

linecard-type

Specifies the type of line card. Valid values are LC4x400G and LC16x100G.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

Run this command before physically inserting the line card in the slot.

If the configured line card type does not match the inserted line card type, the card goes into the faulty state.

If the line card is in the faulty state, reconfigure the slot before powering it on.

Power off the line card before removing the slot configuration.

The [no] form of the command removes the slot configuration and powers off the line card.

Examples

The following examples show how to configure a slot for the line card and verify the configuration:

```
device# configure t
device(config)# linecard 1 LC16x100G

device(config)# no linecard

device# show running-config
linecard 1 LC16x100G
linecard 2 LC4x400G
```

link-fault-signaling

Enables or disables Link Fault Signaling (LFS).

Syntax

link-fault-signaling

no link-fault-signaling

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is not allowed on management interface.

The **no** form of the command disables LFS.

Examples

The following example enables LFS.

```
device(config-if-eth-1/8)# link-fault-signaling

device# show int e 1/8:2
ethernet 1/8:2 Admin state UP      Operational state DOWN
 Interface index is 268435873 (0x100001a1)
 MTU 9216 bytes
 Hardware is Ethernet  mac address 40:88:2f:c1:02:0d
 Current Speed  10G
 FEC Mode: disabled
 Link Fault Signaling: ON
 Link Fault Status: Remote fault
```

The following example disables LFS.

```
device(config-if-eth-1/8)# no link-fault-signaling
```

listener-policy

Creates or removes a listener policy.

Syntax

listener-policy { *name sequence-id* }

no listener-policy { [*name sequence-id*]| *sequence-id* | **all** }

Parameters

name

Specifies the listener policy name. Supports 1 through 64 characters. Allowed Characters are alpha-numeric, underscore, and dot.

Underscore is not allowed as the first character.

sequence-id

Specifies the sequence ID. The valid range is 1 through 65535.

all

Specifies that all listener policies are to be deleted with the `no` form of the command.

Modes

Config mode

Usage Guidelines

Valid listener policy name must be provided.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Attempts to remove any listener policy that is not configured are ignored.

Examples

The following examples show how to configure a listener policy.

```
device# configure terminal
device(config)# listener-policy lp1 4 13

device(config)# listener-policy lp2 5

device(config)# no listener-policy lp1 4 13
device(config)# no listener-policy lp2 5
```

The following example removes the configured listener policy.

```
device# configure terminal
device(config)# no listener-policy lp1 4 243
```

lldp enable

Enables LLDP on the interface.

Syntax

lldp enable

no lldp enable

Parameters

enable

Enables LLDP on the interface.

Modes

Interface config mode

Usage Guidelines

The `no lldp enable` command disables LLDP on the interface.

Examples

The following example enables LLDP protocol.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if)# lldp enable
device(config-if)# no lldp enable

device# show running-configuration
interface ethernet 1/1
no lldp enable
end
```

lldp hello-timer

Configures the global LLDP transmit interval.

Syntax

lldp hello-timer *seconds*

no lldp hello-timer

Parameters

hello-timer *seconds*

Specifies the global LLDP transmit interval in seconds. Range is 1 to 65535. Default is 30 seconds.

Modes

Config mode

Usage Guidelines

The `no lldp hello-timer` command resets the hello-timer to the default value of 30 seconds.

Examples

The following example configures the `no lldp hello-timer` to 10 seconds.

```
device# configure terminal
device(config)# lldp hello-timer 10

device# show running-configuration
lldp hello-timer 10
```

lldp holdtime

Configures the LLDP holdtime to hold the information received by the neighbor device before discarding it.

Syntax

lldp holdtime *seconds*

no lldp holdtime

Parameters

holdtime *seconds*

Specifies the amount of time in seconds. Valid range is 10 through 65535. Default value is 120 seconds.

Modes

Config mode

Usage Guidelines

The `no lldp holdtime` command resets the holdtime to the default holdtime of 120 seconds.

Examples

The following example configures the `lldp holdtime` to 10 seconds.

```
device# configure terminal
device(config)# lldp holdtime 10
device(config)#

Show running:
device# show running-configuration
lldp holdtime 10
```

lldp receive

Enables global or interface LLDP packet receive mode.

Syntax

lldp receive

no lldp receive

Parameters

receive

Specifies the global or interface LLDP packet receive mode (true or false). Default mode is true.

Modes

Config mode

Interface config mode

Usage Guidelines

The `no lldp receive` command sets the LLDP receive mode to false.

Examples

The following example configures global LLDP packet receive mode.

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

device# show running-configuration
lldp receive
```

The following example configures LLDP packet receive mode on the interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if)# lldp receive

device# show running-configuration
interface ethernet 1/1
lldp receive
```

lldp transmit

Enables global or interface LLDP transmit mode.

Syntax

lldp transmit

no lldp transmit

Parameters

transmit

Specifies the global or interface LLDP packet transmit mode (true or false). Default mode is true.

Modes

Config mode

Interface config mode

Usage Guidelines

The `no lldp transmit` command sets the transmit mode to false.

You cannot disable both `lldp transmit` and `lldp receive` together. Use the global command, `no protocol lldp` to disable both transmit and receive.

Examples

The following example configures LLDP transmit mode globally.

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

device# show running-configuration
lldp transmit
```

The following example configures LLDP transmit mode on the interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if)# lldp transmit
device(config-if)#

device# show running-configuration
interface ethernet 1/1
lldp transmit
```

load-balance

Enables or disables masking of different load balancing options while computing hashing per LAG basis.

Syntax

load-balance dst-ip

load-balance dst-l4-port

load-balance protocol

load-balance src-dst-ip-l4port

load-balance src-dst-ip-l4port-tid

load-balance src-ip

load-balance src-l4-port

load-balance tun-id

no load-balance

Parameters

dst-ip

Specifies the destination IP.

dst-l4-port

Specifies the destination TCP/UDP port.

protocol

Specifies the IP protocol.

src-dst-ip-l4port

Specifies source IP, destination IP, l4port, and protocol-based load balancing (default) method.

src-dst-ip-l4port-tid

Specifies source IP, destination IP, l4 port, protocol, and specific GTP tunnel ID-based load-balancing.

src-ip

Specifies the source IP.

src-l4-port

Specifies the source TCP/UDP port.

tun-id

Specifies the tunnel ID.

Modes

Port-channel config mode

Usage Guidelines

This command is available only to users with the admin role.

The **no load-balance** command sets the default value to LAG hash.

The port-channel must be created first.

The load-balance method configured in other egress-objects that co-exist in the same egress-group must match the new load-balance setting.

If there is a conflict in load-balance setting with other egress objects:

1. Remove the port-channels from other egress objects co-existing in egress-groups.
2. Configure the new load-balance method in all port-channels that co-exist in egress-groups with the current port-channel.
3. Add the port-channels back to egress objects with the original configuration.

Examples

The following examples enable load balancing.

```
device# configure terminal
device#(config)# interface port-channel 1
device(config-if-po-1)# load-balance dst-ip
```

```
device# configure terminal
device#(config)# interface port-channel 1
device(config-if-po-1)# load-balance dst-l4-port
```

```
device# configure terminal
device#(config)# interface port-channel 1
device(config-if-po-1)# load-balance protocol
```

```
device# configure terminal
device#(config)# interface port-channel 1
device(config-if-po-1)# load-balance src-dst-ip-l4port
```

```
device# configure terminal
device#(config)# interface port-channel 1
device(config-if-po-1)# load-balance src-dst-ip-l4port-tid
```

```
device# configure terminal
device#(config)# interface port-channel 1
device(config-if-po-1)# load-balance src-ip
```

```
device# configure terminal
device#(config)# interface port-channel 1
device(config-if-po-1)# load-balance src-l4-port
```

```
device# configure terminal
device#(config)# interface port-channel 1
device(config-if-po-1)# load-balance tun-id
```

The following example shows how to resolve a conflicting load-balance type setting.

```
device# show egress-group all

Number of egress-groups: 1
```

```
    Name : egg1
          egress : eg2
          egress : eg3

device# show egress eg2
    Name : eg2
        Precedence : 20
         Interface : port-channel 1

device# show egress eg3
    Name : eg3
        Precedence : 30
         Interface : port-channel 2

device# show run interface port-channel 1
interface port-channel 1
  no shutdown --> load-balance type is default (src-dst-ip-l4port)
device# show run interface port-channel 2

interface port-channel 2
  no shutdown --> load-balance type is default (src-dst-ip-l4port)

device(config)# interface port-channel 1
device(config-if-po-1)# load-balance src-dst-ip-l4port-tid

Error: all egress objects present in group should have same loadbalance type. eg3 has
type SRC_DST_IP_L4_PORT in group egg1

device(config-if-po-1)# exit
device(config)# egress eg2
device(config-egress)# no precedence 20
device(config-egress)# exit

device(config)# egress eg3
device(config-egress)# no precedence 30
device(config-egress)# exit

device(config)# interface port-channel 1
device(config-if-po-1)# load-balance src-dst-ip-l4port-tid
device(config-if-po-1)# exit

device(config)# interface port-channel 2
device(config-if-po-2)# load-balance src-dst-ip-l4port-tid
device(config-if-po-2)#
device(config-if-po-2)# exit

device(config)# egress eg2
device(config-egress)# precedence 20 interface port-channel 1
device(config-egress)# exit

device(config)# egress eg3
device(config-egress)# precedence 30 interface port-channel 2
```

mac access-list

Creates a MAC access control list that contains rules that permit or deny traffic based on packet fields of the L2 OSI layer.

Syntax

mac access-list *name*

no mac access-list [*name* | **all**]

Parameters

name

Specifies the name of the MAC ACL. Names cannot exceed 64 characters and must start with an alphabetic character or an underscore, followed by alphabetic or numeric characters or dots. Reserved keywords cannot be used, such as `all` or `egress`.

all

Specifies all MAC ACLs.

Modes

Config mode

Usage Guidelines

Command-line mode changes from `config` to `config-mac-acl` after new MAC ACL is created.

The `no` form of the command removes the specific or all configured MAC ACLs.

Examples

The following example creates a MAC ACL named L2 and on successful creation, the mode changes to `config-mac acl`.

```
device# configure terminal
device(config)# mac access-list L2
device(config-mac-acl)#

device# show running-config access-list
mac access-list L2

device# show running-config mac access-list L2
mac access-list L2

device# show running-config mac access-list all
mac access-list L2
```

The following example deletes the MAC ACL named L2.

```
device# configure terminal
device(config)# no mac access-list L2
```

match ip access-list

Configures or deletes IPv4 access list (ACL) match criteria assigned to a route-map or listener-policy instance.

Syntax

match ip access-list *name*

no match ip access-list *name*

Parameters

name

Specifies the name of the IPv4 ACL to be matched and assigned to the current route map.

Modes

Route-map config mode

Listener-policy config mode

Usage Guidelines

If match criteria succeed, the next action is decided by the permit | deny clause of route map:

- If permitted, packet-forwarding behavior is based on the match and set actions.
- If denied, packets are dropped.

If match criteria fail, this command is not applied and packets are evaluated by other route-map clauses.

Examples

The following example configures IPv4 ACL matching criteria for `ipv4-1` for the route-map instance.

```
device(conf-route-map)# match ip access-list ipv4-1
```

The following example deletes the IPv4 ACL named `ipv4-1` from the current route map.

```
device(conf-route-map)# no match ip access-list ipv4-1
```

match ipv6 access-list

Configures or deletes IPv6 ACL match criteria assigned to a route-map or listener-policy instance.

Syntax

match ipv6 access-list *aclname*

no match ipv6 access-list *aclname*

Parameters

aclname

Specifies the name of the IPv6 ACL to be matched and assigned to the current route map.

Modes

Route-map config mode

Listener-policy config mode

Usage Guidelines

If match criteria succeed, the next action is decided by the permit | deny clause of route map:

- If permitted, packet-forwarding behavior is based on the match and set actions.
- If denied, packets are dropped.

If match criteria fail, this command is not applied and packets are evaluated by other route-map clauses.

Examples

The following example configures the IPv6 ACL named `ipv6-1` to be matched for the current route map.

```
device(conf-route-map)# match ip access-list ipv6-1
```

The following example deletes the IPv6 ACL named `ipv6-1` from the current route map.

```
conf-route-map#
(conf-route-map)# no match ip access-list ipv6-1
```

match mac access-list

Configures or deletes L2/MAC access list (ACL) match criteria for the current route-map or listener-policy instance.

Syntax

match mac access-list *aclname*

no match mac access-list *aclname*

Parameters

aclname

Specifies the name of the L2/MAC ACL to be matched and assigned to the current route map.

Modes

Route-map config mode

Listener-policy config mode

Usage Guidelines

If match criteria succeed, the next action is decided by the permit | deny clause of route map:

- If permitted, packet-forwarding behavior is based on the match and set actions.
- If denied, packets are dropped.

If match criteria fail, this command is not applied and packets are evaluated by other route-map clauses.

Examples

The following example configures the L2/MAC ACL named to be matched for the current route map.

```
device(conf-route-map)# match mac access-list mac-1
```

The following example deletes the L2/MAC ACL named from the current route map.

```
device(conf-route-map)# no match mac access-list mac-1
```

mirror

Configures the mirror object to monitor traffic.

Syntax

mirror *name*

no mirror *name*

Parameters

name

Specifies the name of the configured mirror object.

The name cannot exceed 64 characters. The name must start with an alphabet character or an underscore. The name must contain alphanumeric characters and special characters (underscores, hyphens, or periods).

Modes

Config mode

Usage Guidelines

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

If the `no` form of the command is run with the configuration, all sub-mode configurations are removed automatically.

Examples

The following example configures the mirror object to monitor traffic.

```
device# configure
device(config)# mirror mirr_1
device(config-mirror)#

device# show mirror mirr_1
                  Name : mirr_1
           Description : -
             Interface : none
```

mtu

Configures the global or interface value for Maximum Transmission Unit (MTU).

Syntax

mtu *value*

no mtu *value*

Parameters

value

Specifies MTU value of an interface. Valid range is 1500 through 9216. Default MTU value is 9216.

Modes

Interface config mode

Usage Guidelines

The MTU configured in the specified interface overrides the global MTU.

The **no** form of the command sets the MTU to the default value, 9216.

This command is available only to users with the admin role.

Running this command causes changes that trigger port flap. As a best practice, run this command during a maintenance window to avoid service disruptions.

Examples

The following examples show how to configure global and interface MTU value.

```
device# configure terminal
device(config)# mtu 4000

device# configure terminal
device(config)# interface ethernet 1/10
device(config-if-eth 1/10)# mtu 4000


device# show running interface ethernet 1/10
interface ethernet 1/10
mtu 4000
shutdown
```

new-scope

Configures scope shift for the current tunnel of the received packet.

Syntax

new-scope

no new-scope

Modes

Route-map config mode

Usage Guidelines

The **no** form of the command disables scope shift for the route-map.

When scope shift is enabled, the packet headers are not decapsulated. The scope of the header is shifted to inner headers in the packet. Further blocks in the packet processing pipeline start using inner headers of the packet.

Examples

The following example configures scope shift for the route-map.

```
device(conf)# route-map rmap1 10

device(conf-route-map)# new-scope
device(config-route-map)# do show route-map all
route-map rmap1 10
forward-action deny
decap
new-scope
Policy matches: 0 packets, 0 bytes, 0 Packets/sec, 0 Bits/sec
```

ntp

Enables and configures Network Time Protocol (NTP).

Syntax

ntp enable

ntp server [*ip address* | *domain name*]

ntp peer [*ip address* | *domain name*]

no ntp enable

no ntp server [*ip address* | *domain name*]

no ntp peer [*ip address* | *domain name*]

Command Default

NTP is disabled by default.

Parameters

enable

Enables the NTP feature.

domain name

Specifies the domain name.

ip address

Specifies the IPv4 or IPv6 address.

peer

Specifies the NTP peer.

server

Specifies the NTP server. The maximum number of NTP servers is eight.

Modes

Config mode

Usage Guidelines

Both IPv4 and IPv6 addresses are supported.

This command is available only to users with the admin role.

NTP is disabled by default. You must enable it explicitly when configuring NTP servers and peers.

The `no ntp enable` command disables the NTP feature.

The `no ntp server` command deletes the NTP server.

The `no ntp peer` command disables the NTP peer.

Examples

The following example disables NTP.

```
device# configure terminal
device(config)# no ntp enable
```

The following example deletes the NTP server from the system.

```
device# configure terminal
device(config)# no ntp server 1.1.1.1
```

The following example deletes the NTP peer from the system.

```
device# configure terminal
device(config)# no ntp peer 1.1.1.1
```

ping

Sends ICMP echo requests to the specified IP or host.

Syntax

ping [[*A.B.C.D* | *NAME*] | [**ipv6** [*IPADDR* | *NAME*]] [**count** *1-1000* | **datagram-size** *64-9000* | **quiet** | **timeout** *1-60*]

Parameters

A.B.C.D

Specifies the destination IPv4 address.

IPADDR

Specifies the destination IPv6 address.

NAME

Specifies the destination host name.

count *1-1000*

Specifies the number of attempts to ping the host. The range is 1-1000, default is 5.

datagram-size *18-9000*

Specifies the size of the ping frame. The range is 64-9000, default is 64 bytes.

quiet

Specifies that there is no output except the start-up and finishing line.

timeout

Specifies the timeout value in seconds. The range is 1-60. The default is 5 seconds.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

This command is also supported on gNOI.

Examples

The following example shows how to use the ping command.

```
device# ping 10.20.73.129 count 3 datagram-size 1000 timeout 2

PING 10.20.73.129 (10.20.73.129) 1000(1028) bytes of data.
1008 bytes from 10.20.73.129: icmp_seq=1 ttl=63 time=1.91 ms
1008 bytes from 10.20.73.129: icmp_seq=2 ttl=63 time=0.684 ms
1008 bytes from 10.20.73.129: icmp_seq=3 ttl=63 time=0.592 ms
```

```
 --- 10.20.73.129 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.592/1.064/1.916/0.603 ms

device# ping www.google.com
PING www.google.com (172.217.165.132) 64(92) bytes of data.
72 bytes from 172.217.165.132 (172.217.165.132): icmp_seq=1 ttl=107 time=66.4 ms
72 bytes from 172.217.165.132 (172.217.165.132): icmp_seq=2 ttl=107 time=66.4 ms
72 bytes from 172.217.165.132 (172.217.165.132): icmp_seq=3 ttl=107 time=66.4 ms
72 bytes from 172.217.165.132 (172.217.165.132): icmp_seq=4 ttl=107 time=66.4 ms
72 bytes from 172.217.165.132 (172.217.165.132): icmp_seq=5 ttl=107 time=66.5 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 66.469/66.488/66.502/0.010 ms

device# ping -6 www.google.com
PING www.google.com(sfo03s01-in-x04.1e100.net) 56 data bytes
64 bytes from sfo03s01-in-x04.1e100.net: icmp_seq=1 ttl=121 time=1.44 ms
64 bytes from sfo03s01-in-x04.1e100.net: icmp_seq=2 ttl=121 time=1.51 ms
64 bytes from sfo03s01-in-x04.1e100.net: icmp_seq=3 ttl=121 time=1.52 ms
64 bytes from sfo03s01-in-x04.1e100.net: icmp_seq=4 ttl=121 time=1.54 ms
64 bytes from sfo03s01-in-x04.1e100.net: icmp_seq=5 ttl=121 time=1.51 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.446/1.510/1.545/0.041 ms
```

precedence

Configures or deletes precedence for the specified interface or port channel. Precedence indicates the priority given to a port or port channel. The lower the number, the higher the priority.

Syntax

precedence *number* **interface** [**ethernet** *IFNAME* | **port-channel** *1-255*]

no precedence *number*

Parameters

precedence *number*

Specifies the precedence value. The valid range is 1 through 65535.

interface

Specifies the interface type.

ethernet *IFNAME*

Specifies the Ethernet interface name.

port-channel *1-255*

Specifies the port channel. The valid range is 1 through 255.

Modes

Egress config mode

Usage Guidelines

A valid interface for the platform must be provided.

The `no` version of the command deletes the interface from the egress instance.

If the interface is a port-channel, the load-balance method configured in other egress-objects that co-exist in the same egress-group must match the new load-balance setting.

If there is a conflict in load-balance setting with other egress objects:

1. Remove the port-channels from other egress objects co-existing in egress-groups.
2. Configure the new load-balance method in all port-channels that co-exist in egress-groups with the current port-channel.
3. Add the port-channels back to egress objects with the original configuration.

Examples

The following example configures the egress object, egress-123 at precedence 10 and 20.

```
device (conf)# egress egress-123
device(conf-egress)# precedence 10 interface ethernet 2/10

Show running:
egress egress-123
precedence 10 interface ethernet 2/10
```

The following example shows how to resolve a conflicting load-balance type setting.

```
device(config)# do show egress-group egg1

    Name : egg1
          egress : eg1
          egress : eg2
device(config)# egress eg2
device(config-egress)# precedence 20 interface port-channel 2
Error: all egress objects present in group should have same loadbalance type.
eg1 has type SRC_DST_IP_L4_PORT in group egg1
device(config-egress)#

device(config)# egress eg1
device(config-egress)# no precedence 10
device(config-egress)# exit
device(config)#
device(config)# interface port-channel 1
device(config-if-po-1)# load-balance src-dst-ip-l4port-tid
device(config-if-po-1)# exit
device(config)#
device(config)# egress eg1
device(config-egress)# precedence 10 interface port-channel 1
device(config-egress)# exit

device(config)# egress eg2
device(config-egress)# precedence 20 interface port-channel 2
device(config-egress)#
device(config-egress)# exit
```

port

Configures the port number of the Remote syslog server (Rsyslog).

Syntax

port [*514-530*]

Parameters

port *514-530*

Specifies port numbers between 514-530.

Modes

Host configuration mode

Examples

The following example configures the port number of the Remote syslog server.

```
device(config-logging-host-H1)# port 514
Warning: Existing Host configuration changed
```

protocol lacp

Enables the link aggregation control protocol (LACP) globally.

Syntax

protocol lacp

no protocol lacp

Parameters

lacp

Enables or disables LACP.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

After enabling LACP globally, there is no need to run LACP on all LAGs on the switch. You can enable LACP on each channel mode using the `channel-group mode` command.

The **no feature lacp** command disables LACP globally.

Examples

The following example enables LACP globally.

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

device# show running-configuration
protocol lacp
hardware
 connector 1/8
  breakout 4x10g
 connector 2/8
  breakout 4x10g
interface ethernet 1/1
 shutdown
```

protocol lldp

Represents system level state of the LLDP protocol and enables LLDP globally.

Syntax

protocol lldp

no protocol lldp

Parameters

lldp

Enables or disables LLDP.

Modes

Config mode

Usage Guidelines

The `no protocol lldp` command disables LLDP globally.

Examples

The following example enables LLDP globally and then disables globally.

```
device# configure terminal

device(config)# protocol lldp

device(config)# no protocol lldp

device# show running-configuration
no protocol lldp
```

qos

Sets the device to Quality of Service (QoS) configuration.

Syntax

qos

Modes

Config mode

QoS config mode

Usage Guidelines

Only admin users can perform this procedure.

This command is allowed only in the Config mode.

When executed, Config mode puts the system in the QoS config mode.

Examples

The following example sets the device into the QoS config mode.

```
device(config)# qos
device(config-qos)#
```

qos-forwarding-group

Configures a Quality of Service (QoS) forwarding group for matched packets.

Syntax

qos-forwarding-group *group-name*

no qos-forwarding-group

Parameters

group-name

The group name of the QoS forwarding group.

no qos-forwarding-group

Negates the command.

Modes

Config mode

Route-map config mode

Examples

The following example configures a route-map, named **map1 1**, to contain a QoS forwarding group name of **FG1**.

```
device(Config)# qos
device(config-qos)# forwarding-group FG1
```

queue

Creates a Quality of Service (QoS) queue.

Syntax

queue *queue-name*

no queue *queue-name*

Parameters

queue-name

Specifies the QoS queue name in the format q0 (default) through q7. The highest queue priority is q7 and q0 is the lowest queue priority.

Modes

Config mode

QoS config mode

QoS forwarding group config mode

Usage Guidelines

The **no queue** command resets the queue name to the default value, q0.

Examples

The following example resets to the default value, q0.

```
(config)# no queue
```

The following example assigns the queue as q1.

```
device(config-qos-group)# queue q1
```

route-map

Configures a route-map instance that dictates the packet forwarding behavior based on the match and set actions for ingress ACLs.

Syntax

route-map *name sequence_number*

no route-map { *name sequence_number* } | **all**

Parameters

name

Specifies the name of the route-map to be used for packet forwarding as part of this ingress group. Valid range is 1 through 64.

The name must start with an alphabet character or an underscore character, followed by alphanumeric characters or special characters (underscores, hyphens, or periods).

sequence_number

Assigns sequence number to the route-map instance. This defines the order of route-map instances within a route-map. Valid range is 1 through 65535.

all

Specifies all route-maps when using the `no` form of this command.

Modes

Config mode

Usage Guidelines

Two route-map instances cannot have the same sequence-number.

Any attempts to remove an unconfigured route-map are ignored.

The **no route-map name** command deletes a route-map and **no route-map [name] [sequence-number]** command deletes the route-map with the specified sequence number.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Examples

The following examples show how to configure a route-map named rmap1 with the sequence number 10.

```
device# configure terminal
device(config)# route-map rmap1 10
device(config-route-map)# match mac access-list mac_acl1
device(config-route-map)# match ip access-list ipv4_acl1
device(config-route-map)# match ipv6 access-list ipv6_acl1
device(config-route-map)# set egress-group eg200

device# show route-map all
route-map rm1 1
forward-action permit
match ip access-list acl4 (active)
match mac access-list acl2 (pending)
egress-group eg1
Policy matches: 0 packets, 0 bytes, 0 Packet/sed, 0 Bits/sec
```

The following examples delete a route map and a route map with a sequence number.

```
device# configure terminal
device(config)# no route-map rm1
device(config)# no route-map rmap1 10
```

seq (ip access-list rules)

Inserts or removes filtering rules in IPv4 access control lists (ACLs).

Syntax

seq { *1-4095* } [**permit** | **deny**] [**tcp** | **udp** | **icmp** | **igmp** | **ip** |**esp** | *1-254*] | [**vxlan** | **nvgre** | **gre** | **ipip** |**gtpc** | **gtpu**] { *1-4294967295* } [**src-ip** | **prefix-length** | **src-ip src-mask**] [**dst-ip** | **prefix-length** | **dst-ip dst-mask**] { **sport** *1-65535*} { **dport** *1-65535* } {**sport-end** *1-65535* } { **dport-end 1-65535** } { **dscp 1-63** } { **length** *64-9000* | **length-end** *65-9000* } { **push** } { **sync** } { **ack** } { **fin** } { **urg** } { **cwr** } { **ece** } { **reset** } {{ { **morefragment** | **dontfragment** }} { **vlan** *0-4095*} { **count** } { **log** } { **qos-forwarding-group** *group-name* }

no seq *ID*

Parameters

seq *ID*

Specifies the sequence ID for the rule. This parameter is optional. Valid values range from 1 through 4095 and the value must be unique within the selected IP ACL. If the value is not specified, a non-assigned value starting from 10 with an increment of 10 is assigned.

permit |**deny**

Specifies the forwarding action for the matching traffic.

tcp|**udp** | **icmp** |**igmp** | **ip** | **esp**

Specifies the numerical protocol type of the traffic for non-tunneled packets.

number

Specifies the custom protocol number to be matched. Valid values range from 1 through 254.

push |**sync** | **ack** |**fin** |**urg** |**cwr** | **ece** | **reset**

Specifies the TCP protocol configuration. (Valid for only the TCP protocol.)

vxlan |**nvgre** | **gre** | **ipip** | **gtpc** | **gtpu**

Specifies the tunnel types supported for tunneled traffic.

For tunnel types, IP address and masks are mapped to the outer header. Valid values range from 1 through 4294967295.

- VXLAN and NVGRE tunnels allow VNID or VSID values in the range of 1 through 16777215.
- GTP-U and GTP-C tunnels allow tunnel ID values in the range of 1 through 4294967295.

src-ip | **prefix-length** | **src-mask** | **dst-ip** | **prefix-length** | **dst-mask**

Specifies the source IP address, the source IP mask, the destination IP address, and destination IP address mask of the traffic.

IP addresses and masks display in a dot-separated, decimal format.

Instead of using the IP address mask, the subnet prefix length can be specified with the source IP address and the destination IP address keywords.

length | **length-end**

Specifies the length of the IPv4 packets. The valid value range is 64 through 9000.

The length range, and length end parameters are provided to match based on range. Valid ranges are from 65 through 9000.

When specifying range, the length value is mandatory.

Specifying length end alone is not valid. Length must be less than the length end.

sport | **sport-end**

Specifies the sport source port value. The valid value range is 1 through 65535.

The source port range and parameters are provided to match on range.

When specifying range, the source port value is mandatory.

Specifying source port end alone is not valid.

The source port value must be less than the source port end.

dport | **dport-end**

Specifies the destination port and the destination port end. Valid values range from 1 through 65535.

When specifying a match based on the range, destination port range, and destination port parameters are provided.

When specifying range, the destination port value is mandatory.

Specifying destination end alone is not valid.

The destination port value must be less than the destination port end.

count

Enables counters for the rule.

log

Enables the system log (syslog) for the rule.

dscp

Specifies the type of service field for IPv4 protocol. The valid value ranges are through 1 to 63.

vlan *vlan-ID*

Specifies the VLAN ID. The valid values ranges are from 0 to 4095.

morefragment | **dontfragment**

Specifies the fragment parameters.

qos-forwarding-group *group-name*

Specifies the name of the Quality of Service (QoS) forwarding group.

Modes

IP ACL config mode

Usage Guidelines

GRE tunnel-type:

- Version-1 packets are not filtered with this setting.
- Version-0 packets are filtered successfully with this setting when checksum, key, or sequence number are not configured.

GTP-U tunnel type:

- Packets with outer IP and UDP port settings (ACL configured with the IP address and the combination of source port and destination port) are not forwarded to the egress.

The IPv4 address and IPv4 mask must be configured in dotted-decimal notation.

Duplicate ACL rules are not allowed.

Conflicting ACL rules (rules with same match condition and different forwarding action) are not allowed.

The following specified length limitation applies to the specified port end and destination port end range length configuration.

Important

If you configure an IPv4 or an IPv6 ACL rule to match a specific IP length and also configure an IPv4 or IPv6 ACL with an overlapping IP length range, then the rule with specific length will not work.

IPv*n* rules configured with specified lengths that overlap IPv*n* length-range configurations fail silently.

Example 1. The IPv6 ACL rule in this example will not work because the rule with a specific length (**bold font**) overlaps the configured IP ACL range from 100 through 200. The rule with the overlapping specified length fails silently.

```
ip access-list v4acl
 seq 10 permit ip any 1.0.0.1 255.255.255.0 length 100 length-end 200

ipv6 access-list v6acl
 seq 10 permit ipv6 any bbbb::bbbb ffff::ffff length 150
```

Example 2. The IPv6 ACL rule (**bold font**) in this example will not work because the rule with a specific length overlaps the range from 100 through 200. The rule with the overlapping specified length fails silently.

```
ipv6 access-list v6acl
 seq 10 permit ipv6 any aaaa::aaaa ffff::ffff length 100 length-end 200
 seq 20 permit ipv6 any bbbb::bbbb ffff::ffff length 150
```

Example 3. This IPv6 ACL rule example will not work because in this configuration, because the rule with a specific length (**bold font**) overlaps the range from 100 through 200. The rule with the overlapping specified length fails silently.

```
ipv6 access-list v6acl-1
 seq 10 permit ipv6 any aaaa::aaaa ffff::ffff length 100 length-end 200

ipv6 access-list v6acl-2
 seq 10 permit ipv6 any bbbb::bbbb ffff::ffff length 150
```

Examples

The following example configures **`seq 1`** for IP access list P4.

```
device# configure terminal
device(config)#ip access-list P4
device(config-ip-acl)# seq 1 permit udp
1.1.1.1 255.0.0.0 2.2.2.2 255.0.0.0 dontfragment

device# show running-config access-list
ip access-list ip-acl
  seq 20 permit ip 10.0.0.1 255.0.0.0 20.0.0.2 255.0.0.0

device# show running-config ip access-list ip-acl
ip access-list ip-acl
  seq 20 permit ip 10.0.0.1 255.0.0.0 20.0.0.2 255.0.0.0

device# show running-config ip access-list all
ip access-list ip-acl
  seq 20 permit ip 10.0.0.1 255.0.0.0 20.0.0.2 255.0.0.0
```

The following example deletes **seq 1**.

```
device(config-mac-acl)# no seq 1
```

seq (ipv6 access-list rules)

Inserts filtering rules in IPv6 access lists (ACLs).

Syntax

seq { *1-4095* } [**permit** | **deny**] [**tcp** | **udp** | **icmpv6** | **igmpv6** | **ipv6** | **esp** | *1-254*] | [**vxlan** | **nvgre** | **gre** | **ipip**| **gtpc** | **gtpu**] { *1-4294967295* } [**src-ip** | **prefix-length** | **src-ip src-mask**] [**dst-ip** | **prefix-length** | **dst-ip dst-mask**] { **sport** *1-65535*} { **dport** *1-65535* } { **sport-end** *1-65535* } { **dport-end** *1-65535* } { **dscp** *1-63* } { **length** *64-9000* | **length-end** *65-9000* } { **push** } { **sync** } { **ack** } { **fin** } { **urg** } { **cwr** } { **ece** } { **reset** } {{ **morefragment** | **dontfragment** }} { **vlan** *0-4095*} { **count** } { **log** } { **qos-forwarding-group** *group-name* }

no seq *ID*

Parameters

seq *ID*

Specifies the sequence ID for the rule. This parameter is mandatory. Valid values range from 1 through 4095, and the value must be unique within the selected IP ACL.

If the value is not specified, a non-assigned value starting from 10 with an increment of 10 is assigned.

permit |**deny**

Specifies the forwarding action for the matching traffic.

tcp|**udp** | **icmpv6** |**igmpv6** | **ipv6** | **esp** | *protocol-number*

Specifies the protocol type of the traffic for non-tunneled packets.

Valid values range from 1 through 254.

vxlan |**nvgre** | **gre** | **ipip** | **gtpc** | **gtpu**

Specifies the tunnel types supported for tunneled traffic. For tunnel types IP address and masks are mapped to the outer header.

VNI and TEID are configured for the VXLAN and GTP-U tunnels, respectively. Valid values range from 1 through 4294967295.

- VXLAN and NVGRE tunnels allow VNID and VSID values in the range of 1 through 16777215.
- GTP-U and GTP-C tunnels allow tunnel ID values in the range of 1 through 4294967295.

src-ip | **prefix-length** | **src-mask** | **dst-ip** | **prefix-length** | **dst-mask**

Specifies the source IP address, source mask, destination IP address, and destination mask of the traffic.

IP addresses and IP masks display in hexadecimal format.

Instead of subnet mask, the subnet prefix length also can be specified.

sport |**sport-end**

Specifies the source port value. The valid values range is from 1 through 65535.

Provides matching based on sport range and sport range end parameters.

When specifying a range, source port value is mandatory.

Specifying the source port end value alone is not valid.

The source port value must be less than the sport port end.

dport |**dport-end**

Specifies the destination port. The valid values range is from 1 through 65535.

To match based on range, use the provided destination port value and the destination port end parameters.

The destination port value must be less than the destination port end value.

dscp

Specifies the type of service field for the IPv6 protocol. The valid values range is from 1 through 63.

length |**length-end**

Specifies the length of the IPv6 packets. The valid values range is from 64 to 9000.

To match based on length range, use the provided length and length-end parameters. The valid values range is from 65 through 9000.

When specifying range, length value is mandatory.

Specifying length-end alone is not valid.

Length must be less than the length-end.

push |**sync** | **ack** | **cwr** | **ece** |**reset** | **fin** |**urg**

Specifies the TCP protocol configuration.

vlan *vlan-id*

Specifies the VLAN ID. The valid values range is 0 through 4095.

morefragment | **dontfragment**

Specifies the fragment parameters.

count

Enables counters for the rule.

log

Enables the system log (syslog) for the rule.

qos-forwarding-group *group-name*

Specifies the name of a Quality of Service (QoS) forwarding group.

Modes

IP ACL config mode

Usage Guidelines

GRE tunnel-type:

- Version-1 packets are not filtered with this setting.
- Version-0 packets are filtered successfully with this setting.

The following specified length limitation applies to the `sport-end` and `dport-end` range length configuration.

Important

If you configure an IPv4 or IPv6 ACL rule to match a specific IP length and also configure an IPv4 or IPv6 ACL with an overlapping IP length range, then the rule with specific length will not work.

IPv*n* rules configured with specified lengths that overlap IPv*n* length-range configurations fail silently.

Example 1. The IPv6 ACL rule in this example will not work because the rule with a specific length (**bold font**) overlaps the configured IP ACL range from 100 through 200. The rule with the overlapping specified length fails silently.

```
ip access-list v4acl
 seq 10 permit ip any 1.0.0.1 255.255.255.0 length 100 length-end 200

ipv6 access-list v6acl
 seq 10 permit ipv6 any bbbb::bbbb ffff::ffff length 150
```

Example 2. The IPv6 ACL rule (**bold font**) in this example will not work because the rule with a specific length overlaps the range from 100 through 200. The rule with the overlapping specified length fails silently.

```
ipv6 access-list v6acl
 seq 10 permit ipv6 any aaaa::aaaa ffff::ffff length 100 length-end 200
 seq 20 permit ipv6 any bbbb::bbbb ffff::ffff length 150
```

Example 3. This IPv6 ACL rule example will not work because in this configuration, because the rule with a specific length (**bold font**) overlaps the range from 100 through 200. The rule with the overlapping specified length fails silently.

```
ipv6 access-list v6acl-1
 seq 10 permit ipv6 any aaaa::aaaa ffff::ffff length 100 length-end 200

ipv6 access-list v6acl-2
 seq 10 permit ipv6 any bbbb::bbbb ffff::ffff length 150
```

Duplicate ACL rules are not allowed.

Conflicting ACL rules, rules with same match condition and different forwarding action are not allowed.

Examples

The following example configures an IPv6 ACL.

```
device# configure terminal
device(config)#ipv6 access-list ip6-acl
device(config-ip6-acl)# seq 1 permit 2000::1 FFFF::1 any any count log
```

```
device# show running-config access-list
ipv6 access-list ip6-acl
  seq 10 permit ipv6 2001::1 2001::0 2002::2 2002::0

device# show running-config ipv6 access-list all
ipv6 access-list ip6-acl
  seq 10 permit ipv6 2001::1 2001::0 2002::2 2002::0

device# show running-config ipv6 access-list all
ipv6 access-list ip6-acl
  seq 10 permit ipv6 2001::1 2001::0 2002::2 2002::0
```

seq (mac access-list rules)

Inserts filtering rules in L2 (MAC) access control lists (ACL) to permit or deny traffic based on matching L2 protocols fields.

Syntax

seq *ID* [**permit** | **deny**] {**vxlan** | **gre** |**nvgre** |**gtpu** |**ipip** }{ *src-mac* | *src-mask* | *dst-mac* | *dst-mask* } { **vlan** | **etype** |**pcp** |**count** |**log** } { **qos-forwarding-group** *group-name* }

no seq *ID*

Parameters

seq *ID*

Specifies the sequence ID for the rule. This parameter is mandatory. Valid values range from 1 through 4095. If the value is not specified, a non-assigned value starting from 10 with an increment of 10 is assigned.

permit |**deny**

Specifies the forwarding action for the matching traffic.

vxlan |**gre** |**nvgre** |**gtpu** |**ipip**

Specifies the optional parameters provided to support different tunnel types.

For VXLAN or GTP-U tunnel types, VNI or TEID or TEID can be configured.

The tunnel ID parameter can be supplied for only VXLAN, GTP-U, and GTP-C protocols, and there is no CLI token for this parameter.

- Valid range for VXLAN is 1 through 16777215
- Valid range for GTP-U is 1 through 4294967295
- Valid range for GTP-C is 1 through 429496729

src-mac

Specifies the source MAC address. There is no explicit keyword. MAC addresses are represented by a colon-separated, one-byte hexadecimal format. Zero padding must be used to make one-byte data into 2-digit value. For example, supply the MAC address 2:2:2:2:2:2 as 02:02:02:02:02:02.

src-mask

Specifies the mask for the configured `src-mac`. To opt out of `src-mask`, use `any` instead of `src-mac`. There is no explicit keyword. MAC addresses are represented by a colon-separated, one-byte hexadecimal format. Zero padding must be used to make one-byte data into 2-digit value. For example, supply the MAC address 2:2:2:2:2:2 as 02:02:02:02:02:02.

dst-mac

Specifies the destination MAC address. There is no explicit keyword. MAC addresses are represented by a colon-separated, one-byte hexadecimal format. Zero padding must be used to make one-byte data into 2-digit value. For example, supply the MAC address 2:2:2:2:2:2 as 02:02:02:02:02:02.

dst-mask

Specifies the destination MAC mask.

To opt out of using destination MAC address and destination mask, use *any* instead.

MAC addresses are represented by colon-separated, one-byte hexadecimal format. Zero padding must be used to make one-byte data into 2-digit value. For example, supply the MAC address 2:2:2:2:2:2 as 02:02:02:02:02:02.

There is no explicit keyword.

vlan-tag

Specifies the value of VLAN tag. Valid values range is from 1 to 4095. This is an optional parameter.

etype

Specifies the value of either type given in hexadecimal format. Valid values range from 0x01 to 0xFFFF, (**excluding 0x8100**). Alternatively, select one the following protocol names, ARP, IPv4, and IPv6. This is an optional parameter.

pcp

Specifies the traffic class mapped to the outgoing PCP value when a packet egresses the switch. Valid values range is from 0 through 7.

count

Enables counter for the current rule.

log

Enables logging for the current rule.

qos-forwarding-group*group-name*

Specifies the name for a Quality of Service (QoS) forwarding group.

Modes

IP ACL config mode

Usage Guidelines

GRE tunnel-type:

- Version-1 packets are not filtered with this setting.
- Version-0 packets are filtered successfully with this setting.

GTP-U tunnel type:

- Packets with outer IP and UDP port settings (ACL configured with *ip address* and *sport/dport* combination) are not forwarded to the egress.

This command configures rules to permit or drop traffic based on MAC address source and destination.

The order of the rules in an ACL is critical. The first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If the sequence value is not specified, the rule is added to the end of the list.

To delete a rule from an ACL:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, enter **no** and then enter the full syntax without the sequence value.

Duplicate ACL rules are not allowed.

Conflicting ACL rules, rules with same match condition and different forwarding action are not allowed.

The **no** form of the command removes the MAC ACL rule entry that matches the supplied sequence id within the current MAC ACL context.

Examples

The following example configures MAC ACL l2.

```
device# configure terminal
device(config)# mac access-list L2
device(config-mac-acl)# seq 1 permit 01:23:45:67:89:ab FF:FF.FF:FF.FF:FF
01:23:41:67:89:ac FF:FF.FF:FF.FF:00
```

The following example verifies that the MAC ACL was configured.

```
device(config-mac-acl)# show running-config access-list
mac access-list L2
  seq 10 permit 02:02:02:02:02:02 02:02:02:02:02:02
02:02:02:02:02:03 02:02:02:02:02:03

device# show running-config mac access-list all
mac access-list L2
  seq 10 permit 02:02:02:02:02:02 02:02:02:02:02:02
02:02:02:02:02:03 02:02:02:02:02:03
```

set egress

Sets the egress to be used by an egress group.

Syntax

set egress *name*

no set egress *name*

Parameters

name

Specifies the name of the configured egress. Supports 1-64 characters.

The name must start with an alphabet character or an underscore character, followed by alphanumeric characters or special characters (underscores, hyphens, or periods).

Modes

Egress-group config mode

Usage Guidelines

This command is available only to users with the admin role.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

If the new egress object contains port-channel, the load-balance method of that port-channel must match the load-balance method configured in other egress-objects of the group.

If there is a conflict in load-balance setting with other egress objects:

1. Remove the port-channels from other egress objects co-existing in egress-groups.
2. Configure the same load-balance method in all port-channels that exist in egress-groups and the new egress object.
3. Add the port-channels to the existing egress objects in egress-groups.
4. Add the new egress object to the group.

Examples

The following example binds an egress to an egress group.

```
device# configure terminal
device(config)# egress-group eg1
device(config-egress-group)# set egress egress_1

device# show running-config egress-group
```

```
egress-group eg1
  set egress egress_1
```

The following example unbinds an egress from an egress group.

```
device# configure terminal
device(config)# egress-group eg1
device(config-egress-group)# no set egress egress_1
```

The following example shows how to resolve a conflicting load-balance type setting.

```
device(config)# egress-group egg1
device(config-egress-group)#
device(config-egress-group)# set egress eg1
device(config-egress-group)#
device(config-egress-group)# set egress eg2
Error: all egress objects present in group should have same loadbalance type. new
egress(eg2) has conflicting type
device(config-egress-group)#
device(config-egress-group)# exit

device(config)# egress eg1
device(config-egress)# no precedence 10
device(config-egress)# exit
device(config)# interface port-channel 1
device(config-if-po-1)# load-balance src-dst-ip-l4port
device(config-if-po-1)# exit
device(config)#
device(config)# egress-group egg1
device(config-egress-group)# set egress eg2
device(config-egress-group)#
```

set egress-group

Sets the egress group to be used by the route map for forwarding matched packets.

Syntax

set egress-group *name*

no set egress-group *name*

Parameters

name

Specifies the configured egress group to be bound to the route map and used for packet forwarding. Name must not exceed 64 characters and must start with an alphabetic character or an underscore followed by an arbitrary sequence of alphabetic or numeric characters, underscores, hyphens, or dots.

Modes

Route-map config mode

Usage Guidelines

This command is available only to users with the admin role.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Examples

The following example configures `egress-group egr1` to be used by the route map for forwarding matched packets.

```
device# configure terminal
device(config)# route-map rmap1 10
device(config-route-map)# set egress-group egr1
device(config-route-map)# end

device# show route-map all
route-map R1 10
forward-action permit
match ip access-list test_1 (active)
egress-group eg_1
Policy matches: 0 packets, 0 bytes, 0 PacketRate, 0 BitRate
```

The following example sets the egress for the `egress-group` and uses the `show running-config` command to verify the setting.

```
device# configure terminal
device(conf)# egress-group eg-100
device(conf-egress-group)#set egress egress-100
```

```
device# show running-config egress-group
egress-group eg-100
  set egress egress-100
```

The following example unbinds the `egress-group egr1` from the route map.

```
device# configure terminal
device(config)# route-map rmap1 10
device(config-egress-group)# no set egress-group egr1
```

set encap

Sets tunnel encapsulation for an egress.

Syntax

set encap *name*

no set encap *name*

Parameters

name

Specifies the configured encap to be bound to the egress ro tunnel termination.

Modes

Config mode

Usage Guidelines

Tunnel encap must be configured before binding an encap with an egress.

Examples

The following example configures encap en1 to be used by egress_1 for encapsulation and uses the show command to verify the setting.

```
device# configure terminal
device(config)# egress egress_1
device(config-egress)# set encap en1
device(config-egress)# end

device# show egress all
egress egress_1
  set encap en1
```

The following example unbinds the encap en1 from egress_1.

```
device# configure terminal
device(config)# egress egress_1
device(config-egress)# no set encap en1
```

set ingress-group

Sets the ingress group to be used by the an interface or transport tunnel for forwarding matched packets.

Syntax

set ingress-group *name*

no set ingress-group *name*

Parameters

name

Specifies the configured ingress group. Supports 64 characters.

The name must start with an alphabet character or an underscore character, followed by alphanumeric characters or special characters (underscores, hyphens, or periods).

Modes

Interface config mode

Transport tunnel config mode

Usage Guidelines

This command is available only to users with the admin role.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Examples

The following examples configure ingress-groups for forwarding the matched packets.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# set ingress-group ig1

device# configure terminal
device(config)# transport-tunnel tt1
device(config-tranport-tunnel)# set ingress-group ig1

device# show running-config interface ethernet 1/1
interface port-channel 1
  set ingress-group ig1
interface ethernet 1/1
  set ingress-group ig1
transport-tunnel tt1
  set ingress-group ig1
```

The following example unbinds the ingress-group from the transport tunnel.

```
device# configure terminal
device(config)# transport-tunnel tt1
device(config-tranport-tunnel)# no set ingress-group ig1
```

set interface ethernet

Configures packet mirroring by specifying the egress port for the monitored traffic.

Syntax

set interface ethernet *name*

no set interface ethernet *name*

Parameters

interface ethernet *name*

Specifies the name of the interface for the mirror destination.

Modes

Config mode

Usage Guidelines

The name identifier must be a valid interface for the platform.

The name must be in slot/port format.

If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.

Examples

The following examples show how to configure description for an interface.

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

set listener-policy

Sets the listener policy to be used at egress for forwarding matched packets.

Syntax

set listener-policy *name*

no set listener-policy *name*

Parameters

name

Specifies the configured listener policy to be applied to matching packets at egress for packet forwarding. Name must not exceed 64 characters and must start with an alphabetic character or an underscore followed by an arbitrary sequence of alphabetic or numeric characters, underscores, hyphens, or dots.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Examples

The following example configures listener-policy lp100 to be used by egress_1 for packet forwarding.

```
device# configure terminal
device(config)# egress egress_1
device(config-egress)# set listener-policy lp100
device(config-egress)# end
device#
```

The following example verifies the configuration for egress_1.

```
device# show running-config egress egress_1
egress egress_1
  set listener-policy lp100
```

The following example unbinds the listener-policy lp100 from egress_1.

```
device# configure terminal
device(config)# egress egress_1
device(config-egress)# no set listener-policy lp100
```

set route-map

Sets the route map to be used by an ingress group for forwarding matched packets.

Syntax

set route-map *name*

no set route-map *name*

Parameters

name

Specifies the configured route map to be applied to matching packets for an ingress group for packet forwarding. Name must not exceed 64 characters and must start with an alphabetic character or an underscore followed by an arbitrary sequence of alphabetic or numeric characters, underscores, hyphens, or dots.

Modes

Ingress-group config mode

Usage Guidelines

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

Examples

The following example configures route map rm1 to be used by ingress group ig1 for packet forwarding.

```
device# configure terminal
device(config)# ingress-group ig1
device(config-ingress-group)# set route-map rm1
device(config-ingress-group)# end
```

The following example uses the show command to verify the configuration for ingress group ig1.

```
device# show running-config ingress-group ig1
  ingress-group ig1
    set route-map rm1
```

The following example unbinds route map rm1 from ingress group ig1.

```
device# configure terminal
device(config)# ingress-group ig1
device(config-ingress-group)# no set route-map rm1
```

show

Displays the contents of a flash or USB file.

Syntax

show *FLASH-FILE*

show *USB-FILE*

Parameters

FLASH-FILE

Specifies the flash file path in format `flash://flash-type/file-name`.

USB-FILE

Specifies the USB file path in format `usb://file-name`.

Modes

Exec mode

Examples

The following example shows details of the `config-file`, `test`.

```
device# show flash://config-file/test

interface ethernet 1/1
  shutdown
interface ethernet 1/2
  shutdown
interface ethernet 1/3
  shutdown
interface ethernet 1/4
  shutdown
interface ethernet 1/5
  shutdown
interface ethernet 1/6
  shutdown
interface ethernet 1/7
  shutdown
interface ethernet 1/8
  shutdown
interface ethernet 1/9
  shutdown

device#  show usb://test
interface ethernet 0/1
 shutdown
interface ethernet 0/2
 shutdown
interface ethernet 0/3
 shutdown
interface ethernet 0/4
 shutdown
```

```
interface ethernet 0/5
 shutdown
interface ethernet 0/6
 shutdown
interface ethernet 0/7
 shutdown
interface ethernet 0/8
 shutdown
interface ethernet 0/9
 shutdown
```

show acl-config

Displays the ACL global configurations.

Syntax

show acl-config

Parameters

acl-config

Specifies ACL common configurations.

Modes

Exec mode

Examples

The following example displays the ACL global configurations.

```
device(config)# show acl-config
acl-config
  no enable acl-counter
```

show capture packet config

Displays all packet capture configurations on Ethernet ports.

Syntax

show capture packet config

Modes

Exec mode

Examples

The following example shows all packet capture configurations on Ethernet interfaces.

```
device# show capture packet config
All protocol RX capture is enabled on interface Eth 1/2
All protocol RX capture is enabled on interface Eth 1/3
All protocol RX capture is enabled on interface Eth 1/1
All protocol TX capture is enabled on interface Eth 1/1
```

show capture packet interface

Displays content of the active or latest PCAP file.

Syntax

show capture packet interface [**all** | **ethernet** *IFNAME*]

Parameters

all

Specifies interfaces on which packet capture is enabled.

ethernet *IFNAME*

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

Modes

Exec mode

Usage Guidelines

The active PCAP file is updated at an interval of 10 seconds.

This command can decode and display packets with the following headers: ARP, Dot1Q, EAPOL, Ethernet, GTP, ICMP, ICMPv6, IPv4, Ipv6, LACP, LLC, LLDP, TCP, and UDP.

Examples

The following example shows content of the active PCAP file.

```
device# show capture packet interface all
-------------------------------------
Frames Logged on interface =  All
-------------------------------------


-----------------------------------------------------
Pkt Capture Metadata: #1 of 1 Packets
--------------------:--------------------------------
Frame Received  Time : Fri, 04 Dec 2020 20:25:02 UTC
Packet Length(bytes) : 64
Packet Direction     : RX
Packet Filter        : All
Front Panel Port     : 1/1
---------------------:--------------------
ETHERNET HEADER      :
---------------------:
SrcMAC               : 00:00:11:da:4d:72
DstMAC               : 00:00:00:f0:c9:b9
EtherType            : IPv4(0x800)
---------------------:--------------------
IPv4 HEADER          :
---------------------:
Src IP Address       : 1.0.10.2
```

```
Dst IP Address       : 1.0.10.1
Type of service      : 0
Total Length         : 28 Bytes
Identification       : 0x0
Fragmentation        : 0
TTL                  :  64
Protocol             : ICMPv4(1)
IP Checksum          : 0x24df
---------------------:--------------------
ICMP DETAILS         :
---------------------:
ICMP Hdr Type        : EchoRequest
ICMP Hdr Code        : 0x0
ICMP Hdr Checksum    : 0xf7f7
ICMP ID              : 0x0
ICMP Sequence No     : 0x8
---------------------:--------------------
--More--
```

show capture packet pcapfile-info

Displays metadata of packet capture files with the following headers: Ethernet, Dot1Q, IPv4, TCP, UDP, ARP, ICMP, EAPOL, LLC, LLDP, LACP, Ipv6, ICMPv6, GTP.

Syntax

show capture packet pcapfile-info

Parameters

pcapfile-info

Shows metadata of all packet capture files.

Modes

Exec mode

Examples

The following example shows metadata of all packet capture files.

```
NPB# show capture packet pcapfile-info
-------------------------------------------------
PCAP File(s)  Details:
-------------------------------------------------
Pcap  File Name : pktcapture_1.pcapng
Last Modified   : Fri Dec  4 11:54:08  2020 (UTC +0000)
PcapFile Size   : 0.48 KB
Packet Count    : 2

Pcap  File Name : pktcapture_2.pcapng
Last Modified   : Fri Dec  4 17:16:37  2020 (UTC +0000)
PcapFile Size   : 2.4 KB
Packet Count    : 10
-------------------------------------------------
```

show inventory

Displays the inventory detail for slot cards, power supply units, or both that are currently in use and whose status is UP.

Syntax

show inventory { **slot** | **power-supply** | **all** }

Parameters

slot

Specifies show inventory detail for slot cards.

power-supply

Specifies show inventory detail for power-supply units.

all

Specifies show inventory detail for all slot and power-supply units.

Modes

Exec mode

Examples

The following example displays inventory details for all slot cards.

```
device# show inventory slot
       Module    : Slot-1
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10036
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

       Module    : Slot-2
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10035
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

       Module    : Slot-3
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10034
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15
```

The following example shows all inventory detail for power supply units.

```
device# show inventory power-supply
       Module    : PSU-0
        Model    : 9920-ACPWR-1600W-F
     SystemNo    : 801115-00-01
     SerialNo    : AE042050B-40007
      Version    : S0F

       Module    : PSU-1
        Model    : 9920-ACPWR-1600W-F
     SystemNo    : 801115-00-01
     SerialNo    : AE042050B-40014
      Version    : S0F
```

The following example shows inventory detail for all cards and power supplies.

```
device# show inventory all
       Module    : Slot-1
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10036
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

       Module    : Slot-2
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10035
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

       Module    : Slot-3
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10034
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

 Module    : PSU-0
        Model    : 9920-ACPWR-1600W-F
     SystemNo    : 801115-00-01
     SerialNo    : AE042050B-40007
      Version    : S0F

       Module    : PSU-1
        Model    : 9920-ACPWR-1600W-F
     SystemNo    : 801115-00-01
     SerialNo    : AE042050B-40014
      Version    : S0F
```

show chassis

Displays the status for components in the device.

Syntax

show chassis

Modes

Exec mode

Examples

The following example displays Extreme 9920 chassis information.

```
NPB# show chassis
        PlatformName: x86_64-extremenetworks-chassis-9920
        Product Name: Extreme 9920-NPB-8
        FPGA Version: v2.12
        Hardware Rev: Beta
     ManufactureDate: 01/12/2021 00:30:00
        Manufacturer: Extreme Networks, Inc.
          PartNumber: 801103-00-04
        SerialNumber: AE012102Y-10006
              Vendor: Extreme Networks Inc.
         description: Extreme 9920-NPB-8, 4.14.49-OpenNetworkLinux, Version
NGNPB_v0.6.0-20210302_150946_UTC
              Status: Online
       Reboot Reason: None
      System Contact: jnixon@extremenetworks.com
     System Location: SJ_HQ2:EK20:U27
       System Uptime: 15m34s
                 Mac: 40:88:2f:c1:18:00
            MacRange: 1024
            LC Slots: 8
           Fan Count: 5
           Led Count: 4
           PSU Count: 4
        Sensor Count: 27
```

show clock

Displays the current time.

Syntax

show clock

Parameters

clock

Specifies the system clock.

Modes

Exec mode

Examples

The following example shows current time.

```
device# show clock

2020-11-18 10:24:01 UTC +0000
```

show counters egress

Displays egress counters information for the specified egress.

Syntax

show counters egress *name*

Parameters

name

Specifies the name of the egress for counter show. The egress name supports 1 through 32 characters. Characters allowed are alpha-numeric, underscore, and dot. Underscore is not allowed as the first character.

Modes

Exec mode

Usage Guidelines

Valid egress-name must be provided.

The `clear counters egress` command can be used to clear egress counters.

Examples

The following example shows egress statistics for egr1.

```
device# show counters egress egr1
Egress-group Packet Statistics
   TX Frames : 10
    TX Bytes : 1430
```

The following example shows egress statistics for all egresses.

```
device# show counters egress all
Egress Packet Statistics : ep_eg01_01
   TX Frames : 250000000
    TX Bytes : 130000000000

Egress Packet Statistics : ep_eg01_02
   TX Frames : 250000000
    TX Bytes : 130000000000
```

show counters egress-group

Displays the egress group counters for the specified egress group.

Syntax

show counters egress-group {*name* | **all** }

Parameters

name

Specifies show counters for the the named egress group.

The `egress-group-name` supports 1-32 characters. Characters allowed are alpha-numeric, underscore, and dot. Underscore is not allowed as the first character.

all

Specifies show counters for all configured egress groups.

Modes

Exec mode

Usage Guidelines

Valid egress group name must be provided.

Examples

The following example shows egress group counters information.

```
device# show counters egress-group eg1
Egress-group Packet Statistics : eg_01

   TX Frames : 500000000
    TX Bytes : 260000000000

Egress-group Packet Statistics : eg_02

   TX Frames : 500000000
    TX Bytes : 260000000000
```

show counters encap

Displays encap counters statistic for the specified or all encap objects.

Syntax

show counters encap { *all* |*name* }

Parameters

all

Specifies all encap counters.

name

Specifies the encap name.

Modes

Exec mode

Usage Guidelines

Valid encap name must be provided.

Examples

The following example shows information about encap counter encap_1.

```
device# show counters encap encap_1

Tunnel Encapsulation Statistics(GRE)
    Egress port : ethernet 1/2
      RX Frames : 0
       RX Bytes : 0
```

The following example shows information about all encap counters.

```
device# show counters encap all
```

show counters ingress-group

Displays ingress-group counters information.

Syntax

show counters ingress-group [*name* | **all**]

Parameters

name

Specifies the name of an ingress group.

all

Specifies counters information for all ingress groups.

Modes

Exec mode

Usage Guidelines

The traffic type must be configured for the ingress group.

Counters for non-transport tunnel type ingress groups is not supported.

Examples

The following example displays all ingress group counters information.

```
device# show counters ingress-group all
Number of ingress-groups: 2
Ingress-group Packet Statistics (Vxlan Tunnel)
        Name : IgVxlanVni100
   RX Frames : 0
    RX Bytes : 0
Outer Tunnel (Vxlan)
    Rx Frames: 4
    RX Bytes: 788
```

The following examples show the output for the `show counters ingress-group`.

VXLAN outer tunnel configuration:

```
device# show counters ingress-group vxlangtp

Ingress-group Packet Statistics (GTPU Tunnel)
   RX Frames : 2
    RX Bytes : 288
```

Outer tunnel configuration:

```
device# show counters ingress-group vxlangtp
```

```
Ingress-group Packet Statistics (GTPU Tunnel)

   RX Frames : 2
    RX Bytes : 288

Outer tunnel (Vxlan):
   RX Frames : 2
    RX Bytes : 288
```

MPLS outer tunnel configuration:

```
device# show counters ingress-group iggAnyMpls

Ingress-group Packet Statistics (GTPU Tunnel)
   RX Frames : 0
    RX Bytes : 0

Outer tunnel (MPLS):
   RX Frames : 585
    RX Bytes : 74880
```

show counters interface ethernet

Displays the counters of Ethernet interface.

Syntax

show counters interface ethernet [*IFNAME*| **all** | **brief**]

Parameters

IFNAME

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

all

Specifies all interfaces.

brief

Displays brief interface statistics.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example shows counters of the Ethernet interface.

```
device# Interface Statistics: ethernet 1/1
Carrier Transitions: 0
           LastClear: 1h51m53.558433595s
Input:
              Total pkts: 20000000
          Broadcast pkts: 0
            Discard pkts: 0
             Errors pkts: 0
              FCS Errors: 0
              MCast pkts: 0
                  Octets: 7760000000
              UCast pkts: 20000000
               Runt pkts: 0
              CRC Errors: 0
Input Distribution:
             64 byte pkts: 0
         65-127 byte pkts: 0
        128-255 byte pkts: 0
        256-511 byte pkts: 10000000
       512-1023 byte pkts: 10000000
      1024-1518 byte pkts: 0
              Jumbo pkts: 0
Out:
```

```
              Total pkts: 0
          Broadcast pkts: 0
            Discard pkts: 0
             Errors pkts: 0
              MCast pkts: 0
                  Octets: 0
              UCast pkts: 0
Rate Info:
                   Input: 0.000000 Mbits/sec, 0 pkts/sec 0.00% of line-rate
                  Output: 0.000000 Mbits/sec, 0 pkts/sec 0.00% of line-rate
```

The following example shows brief statistics of the Ethernet interface.

```
device# show counters interface ethernet brief
           Packets   Error     Discards   CRC
Interface  rx  tx    rx  tx    rx  tx     rx
=======   ========  ========   =======   ======
Eth 1/1    0   0      0   0     0   0     0
Eth 1/2    0   0      0   0     0   0     0
Eth 1/3    0   0      0   0     0   0     0
Eth 1/4    0   0      0   0     0   0     0
Eth 1/5    0   144    0   0     0   0     0
```

show counters interface management

Displays counter information for specified management interface.

Syntax

show counters interface management *number*

Parameters

number

Specifies the management interface by number.

Modes

Exec mode

Examples

The following example shows counters information for management interface 0.

```
device# sh counters interface management 0
Statistics
 Carrier Transitions: 0
           LastClear: 0s
Input:
              Total pkts: 36892
          Broadcast pkts: 2833
            Discard pkts: 0
             Errors pkts: 0
              CRC Errors: 0
              MCast pkts: 32459
                  Octets: 3016973

Out:
              Total pkts: 1793
          Broadcast pkts: 379
            Discard pkts: 0
             Errors pkts: 0
              MCast pkts: 44
                  Octets: 480103
Rate Info:
                   Input: 0.014576 Mbits/sec, 15 pkts/sec 0.00% of line-rate
                  Output: 0.004194 Mbits/sec, 3 pkts/sec 0.00% of line-rate
```

show counters lacp

Displays the LACP counter information.

Syntax

show counters lacp

Parameters

counters lacp

Specifies the LACP counters.

Modes

Exec mode

Examples

The following example displays the LACP counter information.

```
device# show counters lacp

Port               in-pkts   out-pkts   TxErr   RxErr   unknownErr   LacpErr
-------------------------------------------------------------------------------
Channel group: 1
ethernet 1/8:1         4         5       0       0          0          0

Channel group: 100
ethernet 1/8:2        10        13       0       0          0          0
```

show counters lldp

Displays LLDP counters information.

Syntax

show counters lldp

show counters lldp interface ethernet [**all** | *IFNAME*]

Parameters

interface ethernet

Displays LLDP counters for ethernet interfaces.

all

Specifies all interfaces.

IFNAME

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

Examples

The following example shows LLDP interface level statistics.

```
device# show counters lldp interface ethernet 1/2

LLDP Interface Statistics: ethernet 1/2
             FrameIn: 0
            FrameOut: 0
            LastClear: 1h41m22s
```

show counters lldp summary

Displays LLDP global statistics.

Syntax

show counters lldp summary

Parameters

summary

Displays the global LLDP counters summary.

Modes

This command is supported in all modes.

Examples

The following example shows global LLDP counters statistics.

```
device# show counters lldp summary

LLDP Global Statistics:
             FrameIn: 0
            FrameOut: 0
            LastClear: 1h41m22s
```

show counters link-fault-signaling

Displays current link-fault-signaling counter information.

Syntax

show counters link-fault-signaling

Modes

Exec mode

Examples

The following example shows link-fault-signaling counter information.

```
device# show counters link-fault-signaling

Port      Local-Fault-Count  Last-Local-Fault     Remote-Fault-Count Last-Remote-Fault
========= =================  ===================  ==================  ==================
Eth 1/8:1    2               2021-08-17T18:01:07Z       0             NA
Eth 1/8:2    2               2021-08-17T18:01:07Z       0             NA
Eth 1/8:3    2               2021-08-17T18:01:41Z       0             NA
Eth 1/8:4    2               2021-08-17T18:01:41Z       1             2021-08-17T18:01:25Z
```

show counters transport-tunnel

Displays transport tunnel counters information for the specified transport tunnel.

Syntax

show counters transport-tunnel [*name*| **all**]

Parameters

name

Specifies the tunnel name for displaying transport tunnel counters information.

all

Specifies all transport-tunnel counters.

Modes

Exec mode

Examples

The following example shows transport tunnel counters information for tunnel-1.

```
# show counters transport-tunnel tunnel-1

ERSPAN Terminated Packet Statistics
   RX Frames : 0
    RX Bytes : 0
ERSPAN Dropped Packet Statistics
 Dropped Frames : 0
  Dropped Bytes : 0
```

show crypto ca certificates

Displays CA certificates used by the switch.

Syntax

show crypto ca certificates

Modes

Exec mode

Usage Guidelines

Output includes effective date and certificate identifiers.

Examples

The following example shows installed CA certificate information for the current switch.

```
device# show crypto ca certificates
SHA256

Fingerprint=7F:87:87:28:C1:E3:0B:EF:BB:08:3F:8F:E3:0D:FE:15:D7:79:EA:5C:1E:9A:67:15:C5:E6:
44:32:7B:B4:C2:A8

  Subject: CN=ngnpb.extremenetworks.com

  Issuer: CN=NGNPB Intermediate CA,OU=Extreme
  Networks NextGenNPB,O=Extreme Networks,ST=CA,C=US

    Not Before: Sep 14 17:31:15 2020 UTC
    Not After : Sep 14 17:31:15 2021 UTC
```

show egress

Displays egress operational information for the specified egress or all egresses.

Syntax

show egress [*name* | **all**]

Parameters

name

Specifies the name of the egress for show egress. The egress name supports 1-32 characters. Characters allowed are alpha-numeric, underscore, and dot. Underscore is not allowed as the first character.

all

Specifies all egresses for show egress.

Modes

Exec mode

Usage Guidelines

A valid egress name must be provided.

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows operational egress information for ep1.

```
device# show egress ep1
            Name : ep1
       Description : egress_obj_1
Encap : encap_gre
    Listener Policy : lp1
         Precedence : 10
             Interface : ethernet 1/2
```

The following example show operational information for all configured egresses.

```
device# show egress all
    Name : e1
       Description : egress_obj_1
               Encap : encap_gre
       Listener Policy : v4
         Precedence : 12
               Interface : ethernet 1/9
```

show egress-group

Displays egress group configuration for the specified egress group or all egress-groups.

Syntax

show egress-group [*egress-group-name*| **all**]

Modes

Exec mode

Parameters

all

Specifies all egress groups.

egress-group-name

Specifies the egress group name for config show.

Supports 1-32 characters. Characters allowed are alpha-numeric, underscore, and dot. Underscore is not allowed as the first character.

Usage Guidelines

Valid egress-group-name must be provided.

Examples

```
device# show egress-group eg1

    Name : eg1
     Description : -
          egress : e1

device# show egress-group all
Number of egress-groups: 1

    Name : eg1
     Description : -
          egress : e1
```

show encap

Displays encap information for all or specified encap.

Syntax

show encap [**all** | **encap-name**]

Parameters

all

Displays all encaps.

encap-name

Specifies the name of the encap.

Modes

Exec mode

Usage Guidelines

Valid encap name must be provided.

Examples

The following example shows encap information for encap-1.

```
device# show encap encap-1
 encap encap-1
 encap-type        : erspan
 encap-id        : 123456
 source-ipv4-addr    : 10.10.10.1
 destination-ipv4-addr    : 20.20.20.1
 destination-mac-addr    : 00:01:02:03:04:05
 vlan-id        : 1234
 vlan-pcp        : 6
```

show firmware

Displays the current firmware version and rollback firmware version of the system along with BMC firmware version on hardware.

Syntax

show firmware

Modes

Exec mode

Examples

The following example displays the firmware version information.

```
device# show firmware
Current Firmware Version:           NPB-21.1.2.0-NPB-20211218_043748_UTC
Rollback Firmware Version:          NPB-21.1.2.0-NPB-20211217_143922_UTC
Is Current Firmware Committed:      false
Rollback Version after Commit:      NPB-21.1.2.0-NPB-20211218_022830_UTC
BMC Firmware Version:               1.32
```

The following example displays the firmware version information after a system firmware commit.

```
device# show firmware
Current Firmware Version:           NPB-21.1.2.0-NPB-20211218_043748_UTC
Rollback Firmware Version:          NPB-21.1.2.0-NPB-20211217_143922_UTC
Is Current Firmware Committed:      true
BMC Firmware Version:               1.32
```

The following example displays the firmware version information when the current firmware is not committed.

```
device# show firmware
Current Firmware Version:           NPB-21.1.2.0-NPB-20211218_043748_UTC
Rollback Firmware Version:          NPB-21.1.2.0-NPB-20211123_081647_UTC
Is Current Firmware Committed:      false
BMC Firmware Version:               1.32
```

The following example displays the default device firmware version information.

```
device# show firmware
Current Firmware Version:           NPB-21.1.2.0-NPB
Rollback Firmware Version:          None
Is Current Firmware Committed:      true
BMC Firmware Version:               1.32
```

show firmware history

Displays firmware version history.

Syntax

show firmware history

Modes

Exec mode

Examples

The following example shows the last 5 firmware versions on the switch.

```
device# show firmware history

Firmware Version                          Install Date
------------------------------------------------------------------------
device_v21.0.7.0-20210408_012657_UTC     Mon, 12 Apr 2021 14:07:38 UTC
device_v21.0.7.0-20210412_050245_UTC     Mon, 12 Apr 2021 13:58:46 UTC
device_v21.0.7.0-20210408_012657_UTC     Fri, 09 Apr 2021 18:17:22 UTC
device_v21.0.7.0-20210409_012648_UTC     Fri, 09 Apr 2021 18:13:26 UTC
device_v21.0.7.0-20210408_012657_UTC     Fri, 09 Apr 2021 17:56:30 UTC
```

show grpc-server gnmi capabilities

Provides capability information

Syntax

show grpc-server gnmi capabilities

Parameters

capabilities

Display gNMI service version, the versioned data models it supports, and the supported data encoding.

Modes

Exec mode

Usage Guidelines

This information is used in subsequent RPC messages from the client to indicate the set of models that the client can use (GET, SUBSCRIBE, SET) and the encoding to be used for the data.

Examples

The following example shows detail for gNMI capabilities.

```
device# show grpc-server gnmi capabilities
gNMI version: 0.7.0
Supported YANG modules:
Module Name                     Organization                    Version
------------------------------------------------------------------------------
extreme-acl-ext                 Extreme Networks, Inc.          1.0.0
extreme-acl-ipv4-ext            Extreme Networks, Inc.          1.0.0
extreme-acl-ipv6-ext            Extreme Networks, Inc.          1.0.0
extreme-acl-mac-ext             Extreme Networks, Inc.          1.0.0
extreme-common-types            Extreme Networks, Inc.          1.0.0
extreme-egress-group            Extreme Networks, Inc.          1.0.0
extreme-egress                  Extreme Networks, Inc.          1.0.0
extreme-eth-ext                 Extreme Networks, Inc.          1.0.0
extreme-ingress-group           Extreme Networks, Inc.          1.0.0
extreme-lag-ext                 Extreme Networks, Inc.          1.0.0
extreme-listener-policy         Extreme Networks, Inc.          1.0.0
extreme-lldp-ext                Extreme Networks, Inc.          1.0.0
extreme-pcap                    Extreme Networks, Inc.          1.0.0
extreme-policy-statistics       Extreme Networks, Inc.          1.0.0
extreme-routemap                Extreme Networks, Inc.          1.0.0
extreme-saps                    Extreme Networks, Inc.          1.0.0
extreme-sfcs                    Extreme Networks, Inc.          1.0.0
extreme-sfs                     Extreme Networks, Inc.          1.0.0
extreme-snmp                    Extreme Networks, Inc.          1.0.0
extreme-system-logging-ext      Extreme Networks, Inc.          1.0.0
extreme-transport-tunnel        Extreme Networks, Inc.          1.0.0
extreme-tunnel-encap            Extreme Networks, Inc.          1.0.0
```

```
openconfig-acl                  OpenConfig working group        1.0.1
openconfig-interfaces           OpenConfig working group        2.4.3
openconfig-platform             OpenConfig working group        0.11.0
openconfig-system               OpenConfig working group        0.5.0
openconfig-network-instance     OpenConfig working group        0.10.2
------------------------------------------------------------------------------
Supported Encoding:
PROTO
```

show grpc-server gnmi statistics

Displays gNMI subscription detail.

Syntax

show grpc-server gnmi statistics

Parameters

statistics

Display detail of active gNMI stream subscriptions.

Modes

Exec mode

Usage Guidelines

gNMI stream details include the number of active stream subscriptions and subscription details for client, mode, number of subscribed keypaths, keypath details, and subscription interval.

Examples

The following example shows statistics for active gNMI stream subscriptions.

Note
The 10.42.x.x IP addresses are microservices subscribed to data streams for internal use.

```
device# show grpc-server gnmi statistics
Number of active subscriptions: 3
Subscription Details:

Client:10.42.150.21:41102   Mode:STREAM     Subscribed Path Count:8     Start Time: Sun May 26 11:38:56
UTC 2024
Keypath                                     Subscription Mode    Interval
-------------------------------------------------------------------------------------------------------
-
/components/component[name=slot-1]          ON_CHANGE            0s
/components/component[name=slot-2]          ON_CHANGE            0s
/components/component[name=slot-3]          ON_CHANGE            0s
/components/component[name=slot-4]          ON_CHANGE            0s
/components/component[name=slot-5]          ON_CHANGE            0s
/components/component[name=slot-6]          ON_CHANGE            0s
/components/component[name=slot-7]          ON_CHANGE            0s
/components/component[name=slot-8]          ON_CHANGE            0s
-------------------------------------------------------------------------------------------------------
-

Client:10.42.150.63:39656   Mode:STREAM     Subscribed Path Count:8     Start Time: Sun May 26 11:38:58
UTC 2024
Keypath                                     Subscription Mode    Interval
```

```
------------------------------------------------------------------------------------------------------------
-
/components/component[name=slot-1]          ON_CHANGE             0s
/components/component[name=slot-2]          ON_CHANGE             0s
/components/component[name=slot-3]          ON_CHANGE             0s
/components/component[name=slot-4]          ON_CHANGE             0s
/components/component[name=slot-5]          ON_CHANGE             0s
/components/component[name=slot-6]          ON_CHANGE             0s
/components/component[name=slot-7]          ON_CHANGE             0s
/components/component[name=slot-8]          ON_CHANGE             0s
------------------------------------------------------------------------------------------------------------
--

Client:10.42.150.29:58528   Mode:STREAM     Subscribed Path Count:2     Start Time: Sun May 26 11:39:12
UTC 2024
Keypath
Subscription Mode   Interval
------------------------------------------------------------------------------------------------------------
----------------------------
/interfaces/interface[name=management 0]/subinterfaces/subinterface[index=0]/ipv4/addresses
ON_CHANGE           0s
/interfaces/interface[name=management 0]/subinterfaces/subinterface[index=0]/ipv6/addresses
ON_CHANGE           0s
------------------------------------------------------------------------------------------------------------
----------------------------
```

show ingress-group

Displays ingress group configuration for the given ingress group or all ingress groups.

Syntax

show ingress-group [*ingress-group-name* | **all**]

Parameters

ingress-group-name

Specifies the name of the ingress group.

all

Specifies all ingress groups.

Modes

Exec mode

Usage Guidelines

A valid ingress-group-name must be provided.

Examples

```
device# show ingress-group ing

    Name : ing
              Route-Map : -
            Description : -
             Interfaces : none
           Traffic-Type : GTPU
              Tunnel-Id : 5000
                   Mode : decap
   Destination-ip-addr : any
        Source-ip-addr : any

   Outer Tunnel Config :
          Traffic-Type : VxLAN
              Tunnel-Id : 7000
   Destination-ip-addr : 192.168.20.2
   Destination-ip-mask : 255.255.255.0
        Source-ip-addr : any
                Mirror : none

device# show ingress-group all
Number of ingress-groups: 2

    Name : ing
              Route-Map : -
            Description : -
             Interfaces : none
           Traffic-Type : GTPU
              Tunnel-Id : 5000
```

```
                  Mode : decap
   Destination-ip-addr : any
        Source-ip-addr : any

   Outer Tunnel Config :
          Traffic-Type : VxLAN
             Tunnel-Id : 7000
   Destination-ip-addr : 192.168.20.2
   Destination-ip-mask : 255.255.255.0
        Source-ip-addr : any
                Mirror : none

    Name : ing2
             Route-Map : -
           Description : -
            Interfaces : none
          Traffic-Type : NVGRE
             Tunnel-Id : 5000
                  Mode : none
   Destination-ip-addr : any
        Source-ip-addr : 192.168.2.3
        Source-ip-mask : 255.255.255.0

    Outer Tunnel Config :
          Traffic-Type : VxLAN
             Tunnel-Id : 5000
   Destination-ip-addr : 192.168.10.2
   Destination-ip-mask : 255.255.255.0
        Source-ip-addr : any
                Mirror : mirr_2

device# show running-config ingress-group
ingress-group ing
  traffic-type gtpu teid 5000 mode decap
  traffic-type gtpu ip any any
  traffic-type vxlan outer vni 7000
  traffic-type vxlan outer ip any 192.168.20.2 255.255.255.0

ingress-group ing2
  traffic-type nvgre vsid 5000
  traffic-type nvgre ip 192.168.2.3 255.255.255.0 any
  traffic-type vxlan outer vni 5000
  traffic-type vxlan outer ip any 192.168.10.2 255.255.255.0
  traffic-type vxlan outer mirror mirr_2

device(config-ingress-group)# do show ingress-group igg1
Number of ingress-groups: 1
   Name : igg1
     Route-Map : rmap1
    Description : -
    Interfaces : ethernet 0/1

  Outer Tunnel Config :
    Traffic-Type : MPLS
  Header1 (Bottom of Stack header):
        label : 12345
    Traffic Class : any
    Time to Live : any
       Mirror : mirr_2

device# show running-config ingress-group
ingress-group igg1
 traffic-type mpls outer header1 12345 any any
 traffic-type mpls outer mirror mirr_2
```

show interface brief

Displays brief information about interfaces in the system.

Syntax

show interface brief

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example shows brief interface information.

```
device# show interface brief

Number of interfaces 20
Name      Mtu     Admin-State   Oper-State  Speed Ifindex  Description
--------------------------------------------------------------------------------
Eth 1/1   9216    DOWN          DOWN        0x10000008     100G ethernet port
Eth 1/2   9216    DOWN          DOWN        0x10000009     100G ethernet port
Eth 1/3   9216    DOWN          DOWN        0x1000000a     100G ethernet port
Eth 1/4   9216    DOWN          DOWN        0x1000000b     100G ethernet port
Eth 1/5   9216    DOWN          DOWN        0x1000000c     100G ethernet port
Eth 1/6   9216    DOWN          DOWN        0x1000000d     100G ethernet port
Eth 1/7   9216    DOWN          DOWN        0x1000000e     100G ethernet port
Eth 1/8   9216    DOWN          DOWN        0x1000000f     100G ethernet port
Eth 1/9   9216    DOWN          DOWN        0x10000010     100G ethernet port
Eth 1/10  9216    DOWN          DOWN        0x10000011     100G ethernet port
Eth 1/11  9216    DOWN          DOWN        0x10000012     100G ethernet port
Eth 1/12  9216    DOWN          DOWN        0x10000013     100G ethernet port
Eth 1/13  9216    DOWN          DOWN        0x10000014     100G ethernet port
Eth 1/14  9216    DOWN          DOWN        0x10000015     100G ethernet port
Eth 1/15  9216    DOWN          DOWN        0x10000016     100G ethernet port
Eth 1/16  9216    DOWN          DOWN        0x10000017     100G ethernet port
Eth 1/17  9216    DOWN          DOWN        0x10000018     100G ethernet port
Eth 1/18  9216    DOWN          DOWN        0x10000019     100G ethernet port
Eth 1/19  9216    DOWN          DOWN        0x1000001a     100G ethernet port
Mgmt 0    1514    UP            UP       1G 0x60000010     Management
```

show interface ethernet

Displays the details of Ethernet interface or range of interfaces.

Syntax

show interface ethernet [*IFNAME* | **all**]

Parameters

IFNAME

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

all

Specifies all Ethernet interfaces for the show command.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example displays information pertaining to an Ethernet interface.

```
NPB# show int e 1/2
ethernet 1/2 Admin state UP      Operational state UP
 Interface index is 268435868 (0x1000019c)
 MTU 9000 bytes
 Hardware is Ethernet  mac address
 Current Speed  100G

Statistics
Carrier Transitions: 0
           LastClear: 0s
Input:
              Total Pkts: 570850
           Broadcast Pkts: 3
             Discard Pkts: 0
              Errors Pkts: 0
               FCS Errors: 0
               MCast Pkts: 18
                   Octets: 381845280
               UCast Pkts: 44478
                Runt pkts: 0
               CRC Errors: 0

Input Distribution:
            64 byte pkts: 0
        65-127 byte pkts: 21
       128-255 byte pkts: 0
```

```
       256-511 byte pkts: 0
      512-1023 byte pkts: 0
     1024-1518 byte pkts: 0
              Jumbo pkts: 44478

Out:
              Total Pkts: 0
          Broadcast Pkts: 0
            Discard Pkts: 0
             Errors Pkts: 0
              MCast Pkts: 0
                  Octets: 0
              UCast Pkts: 0

Rate Info:
                   Input: 1680.724704 Mbits/sec, 24426 pkts/sec 1.68% of line-rate
                  Output: 0.000000 Mbits/sec, 0 pkts/sec 0.00% of line-rate
```

show interface management

Displays the details of management interface and the IP address configured on the interface.

Syntax

show interface management *interface-number*

Parameters

management *interface-number*

Specifies the management interface number.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example shows the details of the specified management interface.

```
device# show interface management 0
 management 0 Admin state UP      Operational state UP
 MTU 1514 bytes
 Hardware is Ethernet  mac address d8:84:66:f9:3c:03
 Current Speed  1G
 DHCPv4 Disabled
 IPv4 address 192.168.122.160/24
 IPv4 gateway 192.168.122.1
 DHCPv6 Disabled
 IPv6 address 2001::100/120
 IPv6 gateway 2001::1
Statistics
 Carrier Transitions: 0
Input:
              Total pkts: 424129
          Broadcast pkts: 22621
            Discard pkts: 0
             Errors pkts: 0
              CRC Errors: 0
              MCast pkts: 248183
                  Octets: 227726675
Out:
              Total pkts: 45587
          Broadcast pkts: 2858
            Discard pkts: 0
             Errors pkts: 0
              MCast pkts: 247
                  Octets: 3974088
Rate Info:
```

```
                    Input: 0.017180 Mbits/sec, 17 pkts/sec 0.00% of line-rate
                   Output: 0.007562 Mbits/sec, 5 pkts/sec 0.00% of line-rate
```

show interface port-channel

Displays the port-channel information.

Syntax

show interface port-channel *PORANGE* **detail**

show interface port-channel brief

Parameters

port-channel *PORANGE*

Specifies the channel number or channel number range. The range is 1-255.

detail

Displays detail information of the specified port-channel.

port-channel brief

Displays brief information of the specified port-channel.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following examples show interface port-channel information.

```
device# show interface port-channel 1
port-channel 1 is up
    MTU 9216 Bytes
    IfIndex 0x40000201
    Port mode is Full Duplex, 100 Gb/s
    LagType is Static
    MinLinks is 1
    Load balance method uses Src/Dst IP, Src/Dst L4 port and
      protocol
    Active Members in this channel: Eth 1/1
    Members in this channel: Eth 1/1

Statistics
 Carrier Transitions: 3
           LastClear: 37m48.716951005s
Input:
          Broadcast Pkts: 0
            Discard Pkts: 0
             Errors Pkts: 0
              FCS Errors: 0
              MCast Pkts: 0
                  Octets: 0
```

```
              UCast Pkts: 0
       Unknown Protocols: 0
Out:
          Broadcast Pkts: 0
            Discard Pkts: 0
             Errors Pkts: 0
              MCast Pkts: 0
                  Octets: 0
              UCast Pkts: 0

device# show interface port-channel 1-2,5
port-channel 1 is down
    MTU 9216 Bytes
    IfIndex 0x40000200
    Port mode is Full Duplex, SpeedUnknown
    LagType is Static
    MinLinks is 1
    Load balance method uses Src/Dst IP, Src/Dst L4 port and protocol
    Active Members in this channel: Nil
    Members in this channel: Nil

Statistics
 Carrier Transitions: 0
           LastClear: 0s
Input:
          Broadcast pkts: 0
            Discard pkts: 0
             Errors pkts: 0
              FCS Errors: 0
              MCast pkts: 0
                  Octets: 0
              UCast pkts: 0
       Unknown Protocols: 0
Out:
          Broadcast pkts: 0
            Discard pkts: 0
             Errors pkts: 0
              MCast pkts: 0
                  Octets: 0
              UCast pkts: 0

port-channel 2 is down
    MTU 9216 Bytes
    IfIndex 0x40000201
    Port mode is Full Duplex, SpeedUnknown
    LagType is Static
    MinLinks is 1
    Load balance method uses Src/Dst IP, Src/Dst L4 port and protocol
    Active Members in this channel: Nil
    Members in this channel: Nil

Statistics
 Carrier Transitions: 0
           LastClear: 0s
Input:
          Broadcast pkts: 0
            Discard pkts: 0
             Errors pkts: 0
              FCS Errors: 0
              MCast pkts: 0
                  Octets: 0
              UCast pkts: 0
       Unknown Protocols: 0
Out:
```

```
          Broadcast pkts: 0
            Discard pkts: 0
             Errors pkts: 0
              MCast pkts: 0
                  Octets: 0
             UCast pkts: 0
port-channel 5 is down
    MTU 9216 Bytes
    IfIndex 0x40000204
    Port mode is Full Duplex, SpeedUnknown
    LagType is Static
    MinLinks is 1
    Load balance method uses Src/Dst IP, Src/Dst L4 port and protocol
    Active Members in this channel: Nil
    Members in this channel: Nil
Statistics
 Carrier Transitions: 0
           LastClear: 0s
Input:
          Broadcast pkts: 0
            Discard pkts: 0
             Errors pkts: 0
              FCS Errors: 0
              MCast pkts: 0
                  Octets: 0
             UCast pkts: 0
       Unknown Protocols: 0
Out:
          Broadcast pkts: 0
            Discard pkts: 0
             Errors pkts: 0
              MCast pkts: 0
                  Octets: 0
             UCast pkts: 0
```

The following examples show detail information of the port-channel when same speed member-ports are present.

```
device# show interface port-channel 2 detail

port-channel 2 is up
    Number of Active Members: 4
    Number of Members: 4

Port         Status        Speed
---------------------------------------------
Eth 2/8:1    active        10G
Eth 2/8:2    active        10G
Eth 2/8:3    active        10G
Eth 2/8:4    active        10G

device# show interface port-channel 2 detail

port-channel 2 is up
    Number of Active Members: 3
    Number of Members: 4

Port         Status        Speed
---------------------------------------------
Eth 2/8:1    passive       10G
Eth 2/8:2    active        10G
Eth 2/8:3    active        10G
Eth 2/8:4    active        10G
```

The following example shows detail information of the port-channel when different speed member-ports are present.

```
device# show interface port-channel 2 detail

port-channel 2 is down
    Reason: Different speed member-ports are present !
    Number of Active Members: 0
    Number of Members: 5

Port         Status        Speed
-----------------------------------------------
Eth 1/1      passive       100G
Eth 2/8:1    passive       10G
Eth 2/8:2    passive       10G
Eth 2/8:3    passive       10G
Eth 2/8:4    passive       10G
```

The following example shows brief information of the port-channel.

```
device# show interface port-channel brief

Number of interfaces 23
Port    Mtu     Admin-State   Oper-State  Speed  Ifindex         Description
-------------------------------------------------------------------------------
Po1     9216    DOWN          DOWN        10G    0x40000200    Port-Channel Interface
Po2     9216    UP            UP          10G    0x40000201    Port-Channel Interface
Po3     9216    UP            UP          10G    0x40000202    Port-Channel Interface
```

show inventory

Displays the inventory detail for slot cards, power supply units, or both that are currently in use and whose status is UP.

Syntax

show inventory { **slot** | **power-supply** | **all** }

Parameters

slot

Specifies show inventory detail for slot cards.

power-supply

Specifies show inventory detail for power-supply units.

all

Specifies show inventory detail for all slot and power-supply units.

Modes

Exec mode

Examples

The following example displays inventory details for all slot cards.

```
device# show inventory slot
       Module    : Slot-1
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10036
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

       Module    : Slot-2
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10035
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

       Module    : Slot-3
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10034
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15
```

The following example shows all inventory detail for power supply units.

```
device# show inventory power-supply
       Module    : PSU-0
        Model    : 9920-ACPWR-1600W-F
     SystemNo    : 801115-00-01
     SerialNo    : AE042050B-40007
      Version    : S0F

       Module    : PSU-1
        Model    : 9920-ACPWR-1600W-F
     SystemNo    : 801115-00-01
     SerialNo    : AE042050B-40014
      Version    : S0F
```

The following example shows inventory detail for all cards and power supplies.

```
device# show inventory all
       Module    : Slot-1
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10036
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

       Module    : Slot-2
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10035
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

       Module    : Slot-3
        Model    : 9920-16C
       PartNo    : 801112-00-04
     SerialNo    : AE022102Y-10034
      Version    : 4
Manufacturer    : Extreme Networks Inc.
     Mfg Date    : Fri Jan 15 09:30:00 2021
    ECVersion    : 15

 Module    : PSU-0
        Model    : 9920-ACPWR-1600W-F
     SystemNo    : 801115-00-01
     SerialNo    : AE042050B-40007
      Version    : S0F

       Module    : PSU-1
        Model    : 9920-ACPWR-1600W-F
     SystemNo    : 801115-00-01
     SerialNo    : AE042050B-40014
      Version    : S0F
```

show ip access-list

Displays specific IPv4 access control list (ACL), all configured IPv4 access lists, or IPv4 ACLs bound to a route map or listener policy.

Syntax

show ip access-list {*name* | **all** }

show ip access-list all route-map

show ip access-list all listener-policy

Parameters

name

Shows information for the named IPv4 ACL.

all

Shows all configured IPv4 ACLs.

route-map

Shows all IPv4 ACLs bound to a route map.

listener-policy

Shows all IPv4 ACLs bound to a listener policy.

Modes

Exec mode

Usage Guidelines

To display all IPv4 ACLs bound to a route map or listener policy, the **route-map** and **listener policy** optional parameters are available.

Examples

The following example shows the configured ACL named IPv4-1.

```
device# show ip access-list IPv4-1
ip access-list IPv4-1
    seq 66 permit tcp any any (0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )
    seq 65 permit udp any any (0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )
```

The following example shows all configured ACLs and all ACLs bound to a route map or listener policy options..

```
device# show ip access-list all
ip access-list IPv4-1
seq 66 permit tcp any any ( 0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )

device# show ip access-list all route-map
```

```
Route map: rm1
  ip access-list v4
    seq 10 permit ip any any ( 0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )
  ip access-list ip-3
    seq 70 permit udp any any dport 20000 dport-end 20010 sport 10000 sport-end 10010
    ➥( 0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )

device# show ip access-list all listener-policy
Listener policy: LP1
  ip access-list ip-eg-acl
    seq 10 permit ip any any ( 0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )
```

show ip dns

Displays the details of IP DNS configuration information.

Syntax

show ip dns

Parameters

ip dns

Specifies the DNS IP address.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example show IP DNS information.

```
device# sh ip dns
ip dns domain name
corp.extremenetworks.com
extremenetworks.com
ip dns name-server
10.6.16.32
10.6.24.30
1111:2222::1
```

show ipv6 access-list

Displays all or specific configured IPv6 access control list (ACL) or IPv6 ACLs bound to a route map or listener policy.

Syntax

show ipv6 access-list { *name* | **all** }

show ipv6 access-list all route-map

show ipv6 access-list all listener-policy

Parameters

name

Specifies the name of IPv6 ACL.

all

Specifies all configured IPv6 ACLs.

route-map

Specifies the name of the route-map.

listener-policy

Specifies the name of the listener-policy.

Modes

Exec mode

Examples

The following example shows settings for the IPv6 access list, IPV6-1.

```
device# show ipv6 access-list IPv6-1
seq 66 permit tcp any any ( 0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )
```

The following example shows all IPv6 access lists.

```
device# sshow ipv6 access-list all
ipv6 access-list ip6-2
  seq 10 permit gtpu any any ( 0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )
  seq 20 permit ipv6 2001::1 2001:0::0:1 any ( 0 Packets, 0 Bytes, 0 Packets/sec, 0
Bits/sec )
ipv6 access-list ip6-3
  seq 40 permit ipv6 2002::2 2002:: 2003::3 2003::0 ( 0 Packets, 0 Bytes, 0 Packets/sec,
0 Bits/sec )
```

The following example shows all configured IPv6 access lists bound to a route map.

```
device# show ipv6 access-list all route-map
Route map: rm1
  ipv6 access-list ip6-3
```

```
    seq 40 permit ipv6 2002::2 2002:: 2003::3 2003::0 ( 0 Packets, 0 Bytes, 0 Packets/
sec, 0 Bits/sec )
```

The following example shows all IPv6 access lists bound to a listener policy.

```
device# show ipv6 access-list all listener-policy
Listener policy: LP1
  ipv6 access-list ip6-2
    seq 10 permit gtpu any any ( 0 Packets, 0 Bytes, 0 Packets/sec, 0 Bits/sec )
    seq 20 permit ipv6 2001::1 2001:0::0:1 any ( 0 Packets, 0 Bytes, 0 Packets/sec, 0
Bits/sec )
```

show lacp interface ethernet

Displays the LACP information for a specific interface.

Syntax

show lacp interface ethernet *IFNAME*

Parameters

interface ethernet *IFNAME*

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

Modes

Exec mode

Examples

The following example shows LACP information.

```
device# show lacp interface ethernet 1/8:1
interface Eth 1/8:1 is up
   Channel group is 100 port channel is Po100
   PDUs sent: 72
   PDUs rcvd: 71
   LACP Rx errors: 0
   LACP Tx errors: 0
   LACP unknown errors: 0
   LACP errors: 0
Local Port: Eth 1/8:1  MAC Address = 40:88:2f:c1:02:00
  System Identifier = 80:00:40:88:2f:c1:02:00
  Port Identifier = 0x8000, 0x1a0
  Operational key = 100
  LACP_Activity = active
  LACP_Timeout = Long Timeout (30s)
  Synchronization = IN_SYNC
  Collecting = true
  Distributing = true

Partner information
  Partner-id = 80:00:60:9c:9f:b1:3a:00
  Partner-key = {1, 11}
```

show lacp system-identifier

Displays the LACP system identification information.

Syntax

show lacp system-identifier

Parameters

system-identifier

Displays the system priority and MAC address.

Modes

Exec mode

Examples

The following example shows the LACP system identification.

```
device# show lacp system-identifier
System ID: 0x4d2, 40:88:2f:c1:02:00

device# configure terminal
device(config)# show lacp system-identifier
32768, aa:bb:cc:dd:ee:ff
```

show link-fault-signaling

Displays link-fault-signaling information.

Syntax

show link-fault-signaling

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

This command is not allowed on management interface.

Examples

The following example shows how to configure link-fault-signaling on a device.

```
device(config)# int e 1/1-16,2/1-16

device(config-if-eth-1/1-16,2/1-16)# no link-fault-signaling

devicedevice(config-if-eth-1/1-16,2/1-16)#
```

The following example shows link-fault-signaling information.

```
device# show link-fault-signaling
Port       Link-Fault
========== ===============
Eth 1/1    OFF
Eth 1/2    ON
Eth 1/3    ON
Eth 1/4    ON
Eth 1/5    ON
Eth 1/6    ON
Eth 1/7    ON
```

show listener-policy

Displays a list of all or specified listener policies on the device.

Syntax

show listener-policy { *name* | **all** }

Parameters

name

Specifies the name of the configured listener policy.

all

Displays all configured listener policies on the device.

Modes

Exec mode

Examples

The following example shows configuration parameters for the listener policy IPV6.

```
device# show listener-policy IPV6
 listener-policy IPV6 65
 match ipv6 access-list IPv6-1
 truncate 1280 description policy v6 is applied
 Policy matches: 11 packets, 1573 bytes
```

The following example shows all listener policies.

```
device# show listener-policy all
 listener-policy IPV6
 Policy-1
Policy matches: 11 packets, 1573 bytes
```

show lldp

Displays the LLDP global configuration information.

Syntax

show lldp

show lldp neighbors

show lldp neighbors interface ethernet [*IFNAME* | **all**]

Parameters

neighbors

Displays the LLDP neighbors information.

interface

Displays the LLDP neighbors interface information.
IFNAME

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

all

Specifies all interfaces.

Modes

Exec mode

Examples

The following example shows the LLDP global configuration information.

```
device# show lldp

Global LLDP Information:
Status: ACTIVE
LLDP advertisements are sent every 30 seconds
LLDP hold time advertised is 120 seconds
LLDP transmit: On
LLDP receive: On

Interface LLDP Information:
Intf            State     Rx         Tx
---------i------------------------------
ethernet 1/1    Enable    On         On
ethernet 1/2    Disable   Off        Off
ethernet 1/3    Enable    On         On
ethernet 1/4    Enable    On         On
ethernet 1/5    Enable    On         On
ethernet 1/6    Enable    On         On
```

The following example shows the LLDP neighbors information.

```
device# show lldp neighbors
show LLDP Neighbors Information
Chassis ID        Local-Port      Dead  Rem   Remote          Remote
System
                                  Intvl Life  Port-ID         Port Descr
Name
60:9c:9f:b1:3a:00 ethernet 1/8:1  120   107   Ethernet 0/11   Eth 0/11
SLX
60:9c:9f:b1:3a:00 ethernet 1/8:2  120   107   Ethernet 0/12   Eth 0/12
SLX
60:9c:9f:b1:3a:00 ethernet 1/8:3  120   106   Ethernet 0/13   Eth 0/13
SLX
60:9c:9f:b1:3a:00 ethernet 1/8:4  120   107   Ethernet 0/14   Eth 0/14
SLX
60:9c:9f:b1:3a:00 ethernet 2/8:1  120   108   Ethernet 0/15   Eth 0/15
SLX
60:9c:9f:b1:3a:00 ethernet 2/8:2  120   108   Ethernet 0/16   Eth 0/16
SLX
60:9c:9f:b1:3a:00 ethernet 2/8:3  120   108   Ethernet 0/17   Eth 0/17
SLX
60:9c:9f:b1:3a:00 ethernet 2/8:4  120   109   Ethernet 0/18   Eth 0/18        SLX

Total entries displayed: 8
```

The following example shows the LLDP neighbors ethernet interface information.

```
show lldp neighbors interface ethernet 0/1-2
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

LLDP Interface: ethernet 0/1
Local Port id: ethernet 0/1
Chassis id: 88f0.31f9.a340
Remote Port id: ethernet 1/10
Remote Port Description: ethernet 1/10
System Name: Lab switch1
Dead Interval:   120 seconds
Time remaining: 91 seconds
System Description: "ExtremeXOS (Summit) version 31.1.1.4 v311b4 by release-manager on
Fri Feb 13 16:30:06 EST 2021"
System Capabilities: B, R
Enabled Capabilities: B, R
Management Address: 10.77.143.43
Management Address IPV6: not advertised

LLDP Interface: ethernet 0/2
Local Port id: ethernet 0/2
Chassis id: 88f0.31f9.a341
Remote Port id: ethernet 1/11
Remote Port Description: ethernet 1/11
System Name: Lab switch 2
Dead Interval:   120 seconds
Time remaining: 85 second
System Description: Cisco Nexus Operating System (NX-OS) Software 9.2(1) TAC support:
http://www.cisco.com/tac Copyright (c) 2002-2018, Cisco Systems, Inc. All rights
reserved.
System Capabilities: B, R
Enabled Capabilities: B, R
Management Address: 10.77.143.43
Management Address IPV6: not advertised
```

show logging

Displays logging information.

Syntax

show logging audit [**config** | **firmware** | **security**]

show logging file

show logging id *1-60000*

Parameters

audit

Displays audit logging entries.

config

Displays configuration related log information.

firmware

Displays firmware related log information.

Security

Displays security related log information.

file

Selects file for general log entries.

id *1-60000*

Selects log ID to see the description.

Modes

Exec mode

Examples

The following example shows audit logging firmware information.

```
device# show logging audit firmware
Wed 28 Apr 2021 23:07:27.971 UTC +0000 LogID:5021 Info Msg: Firmware change successful.
Current Firmware Version is NGNPB_v21.0.7.0-20210427_045749_UTC
```

The following example shows logging information for ID 5001.

```
device# NPB# show logging id 5001
Log ID: 5001
  Level         : Fatal
  Message       : Unable to connect to Operational Database
  Probable cause: Database is down
  Remedy        : Check Database status
  Impact        : Service not operational
```

The following example shows audit logging file information.

```
show logging file
2021-04-22 12:17:01.2425 liblogging-stdlog:  [origin software="rsyslogd"
swVersion="8.24.0" x-pid="17744" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
2021-04-22 17:17:02.8468 liblogging-stdlog:  [origin software="rsyslogd"
swVersion="8.24.0" x-pid="17744" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
2021-04-22 21:17:02.3471 liblogging-stdlog:  [origin software="rsyslogd"
swVersion="8.24.0" x-pid="17744" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
--More--
```

The following example shows audit logging configuration information.

```
show logging audit config
Sat 16 Jan 2021 17:02:05.512 UTC +0000 LogID:8001 Info Msg: nouser/norole/none/ssh/cli,
Status:100 Command:'operational assigned to groups:  admin'
Mon 25 Jan 2021 22:52:24.557 UTC +0000 LogID:8001 Info Msg: nouser/norole/none/ssh/cli,
Status:100 Command:'operational assigned to groups:  admin'
Mon 25 Jan 2021 22:57:38.538 UTC +0000 LogID:8001 Info Msg: admin/admin sudo docker/
none/ssh/cli, Status:100 Command:'operational assigned to groups:  admin'
Mon 25 Jan 2021 22:57:42.089 UTC +0000 LogID:8001 Info Msg: admin/admin sudo docker/
none/ssh/cli, Status:0 Command:'operational conf t'
Mon 25 Jan 2021 22:59:34.316 UTC +0000 LogID:8001 Info Msg: admin/admin sudo docker/
none/ssh/cli, Status:0 Command:'configure (config) exit'
Mon 25 Jan 2021 23:18:12.456 UTC +0000 LogID:8001 Info Msg: admin/admin sudo docker/
none/ssh/cli, Status:100 Command:'operational assigned to groups:  admin'
Fri 29 Jan 2021 14:51:42.566 UTC +0000 LogID:8001 Info Msg: nouser/norole/none/ssh/cli,
Status:100 Command:'operational assigned to groups:  admin'

--More--
```

show mac access-list

Displays all or specific MAC ACLs.

Syntax

show mac access-list { *name* | **all** }

show mac access-list all route-map

show mac access-list all listener-policy

Parameters

name

Specifies the name of the MAC ACL or all MAC ACLs and displays a list of MAC ACL rule entries configured for the specified ACL.

all

Displays all MAC ACLS with aggregated stats.

route-map

Displays all MAC ACLS mapped to a route map.

listener-policy

Displays MAC ACLs mapped to a listener policy.

Modes

Exec mode

Examples

The following example shows all MAC ACLs.

```
device# show mac access-list all
mac access-list mac2
  seq 10 permit aa:aa:aa:aa:aa:aa FF:FF:FF:FF:FF:FF any ( 0 Packets, 0 Bytes, 0 Packets/
sec, 0 Bits/sec )

mac access-list mac3
  seq 90 permit gtpu 4294967295 02:02:02:02:02:02 02:02:02:02:02:02 any ( 0 Packets, 0
Bytes, 0 Packets/sec, 0 Bits/sec )
```

The following example shows all ACLs bound to a route map.

```
device# show mac access-list all route-map
Route map: rm1
  mac access-list mac3
    seq 90 permit gtpu 4294967295 02:02:02:02:02:02 02:02:02:02:02:02 any ( 0 Packets, 0
Bytes, 0 Packets/sec, 0 Bits/sec )
```

The following example shows all listener policies bound to a route map.

```
device# show mac access-list all listener-policy
Listener policy: LP1
```

```
  mac access-list mac2
    seq 10 permit aa:aa:aa:aa:aa:aa FF:FF:FF:FF:FF:FF any ( 0 Packets, 0 Bytes, 0 Packets/
sec, 0 Bits/sec )
```

show media

Displays detail information about media on the specified interface.

Syntax

show media detected

show media interface ethernet *IFNAME*

show media supported

Parameters

media

detected

Specifies media detected in the chassis.

interface ethernet *IFNAME*

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

supported

Displays the supported media information.

Modes

Exec mode

Usage Guidelines

Channel information is displayed only for the csupported optics.

Supported passive optics value is 0.

Examples

The following example shows media detected in the chassis.

```
device# show media detected
S/C  Qual  Optical Type   PartNum        Serial Num    Vendor       Description
-------------------------------------------------------------------------------------------
--
1/1   No   QSFP28         AA1405031-E6   16CN10300147  Volex Inc.   Volex QSFP media
1/2   No   QSFP28         AA1405031-E6   16CN10300147  Volex Inc.   Volex QSFP media
1/3   No   QSFP28         AA1405031-E6   16CN10300147  Volex Inc.   Volex QSFP media
1/4   No   QSFP28         AA1405031-E6   16CN10300147  Volex Inc.   Volex QSFP media
2/16  No   SFP28          BBA1405031-E6  18CN10300147  Molex Inc.   Molex QSFP media
```

The following example shows detail for ethernet 1/1.

```
device#  show media interface ethernet 4/4
           Interface: ethernet 4/4
                Cage: 4
```

```
                Slot: 4
                Qual: Yes
             Optical: yes
               State: Inserted
         Module Type: QSFP28
         Part Number: 57-1000336-01
       Serial Number: YMJ11645F66002F
              Vendor: BROCADE
         Description: 100G QSFP28 CWDM
            Channels: 4
            Datecode: 161123
Channel[1]:
             Voltage: 3.240000
         Temperature: 39.500000
             RxPower: -1.690000
              TxBias: 24.140000
             TxPower: 0.960000
Channel[2]:
             Voltage: 3.240000
         Temperature: 39.500000
             RxPower: -3.210000
              TxBias: 24.140000
             TxPower: 1.230000
Channel[3]:
             Voltage: 3.240000
         Temperature: 39.500000
             RxPower: -1.430000
              TxBias: 24.130000
             TxPower: 0.020000
Channel[4]:
             Voltage: 3.240000
         Temperature: 39.500000
             RxPower: -2.780000
              TxBias: 24.480000
             TxPower: -1.180000
```

The following command lists the supported media.

```
device# show media supported
Type           PartNum             Vendor              Description
-----------------------------------------------------------------------------------------

qsfp           57-1000129-01       BROCADE             40GBase-SR4 QSFP
qsfp           57-1000263-01       BROCADE             40G QSFPP-LR4 10KM
qsfp           58-0000033-01       BROCADE             40G-QSFP-QSFP 1m cable passive
qsfp           58-0000034-01       BROCADE             40G-QSFP-QSFP 3m cable passive
qsfp           58-0000035-01       BROCADE             40G-QSFP-QSFP 5m cable passive
qsfp           58-0000041-01       BROCADE             40G-QSFP-QSFP 1m Active Copper
qsfp           58-0000042-01       BROCADE             40G-QSFP-QSFP 3m Active Copper
qsfp           58-0000043-01       BROCADE             40G-QSFP-QSFP 5m Active Copper
qsfp           57-1000325-01       BROCADE             40G-QSFP+ LM4
qsfp           57-1000306-01       BROCADE             40G QSFP to QSFP cable 10m AOC
qsfp           57-1000339-01       BROCADE             40G QSFPP BIDI Optic
qsfp           AFBR-79EBPZ         AVAGO               40G QSFPP BIDI Optic
qsfp           AFBR-79EBRZ         AVAGO               40G QSFPP BIDI Receiver Optic
qsfp           58-0000053-01       BROCADE             4x10G QSFPP 5m Active Copper Cable
```

show mirror

Displays the mirror configuration for the given ingress group or for all mirrors.

Syntax

show mirror [*name* | **all**]

Parameters

name

Specifies the name of the mirror.

`all`

Specifies all mirrors.

Modes

Exec mode

Examples

```
device(config)# mirror mirr_1
device(config-mirror)# description mirror-1
device(config-mirror)# set interface ethernet 1/1

device# show mirror mirr_1
                  Name : mirr_1
           Description : mirror-1
             Interface : ethernet 1/1
```

show ntp association

Displays Network Time Protocol (NTP) association information.

Syntax

show ntp association *detail*

Parameters

association *detail*

Displays NTP association information in detail.

Modes

Exec mode

Examples

The following example shows NTP association information.

```
device# show ntp  association

remote           refid        st  t  when poll reach   delay   offset  jitter
==============================================================================
*10.24.12.107    10.6.24.32   2   u  356  512  377    0.731    0.915   0.137

* synced, # selected, + candidate, - outlayer, x falseticker, ~ configured

device# show ntp as d
[detail] display ntp association in detail

device# show ntp association detail

ind  assid  status  conf  reach  auth  condition  last_event cnt
===========================================================
1    41294  8011    yes   no     none  reject     mobilize 1
2    41295  8011    yes   no     none  reject     mobilize 1
3    41296  8011    yes   no     none  reject     mobilize 1
4    41297  8011    yes   no     none  reject     mobilize 1
```

show ntp status

Displays the Network Time Protocol (NTP) status information.

Syntax

show ntp status

Parameters

status

Displays NTP information.

Modes

Exec mode

Examples

The following example shows NTP status information.

```
device# show ntp status

Clock is synchronized,  stratum 3, reference clock is 10.24.12.107,
precision is -16,
reference time is e35f7b06.7cc6df3e  Wed, Nov 18 2020 10:50:46.487,
clock offset is 0.534396, root delay is 85.256,
root dispersion is 79.806, peer dispersion is 4504,
NTP client mode is enabled

device# show ntp status
Clock is unsynchronized, no reference clock
NTP client mode is disabled
```

show qos forwarding-group

Displays the Quality of Service (QoS) forwarding groups.

Syntax

show qos { **forwarding-group** [**all** | *NAME*] }

Parameters

forwarding-group

Shows the specified forwarding-group.

all

Specifies all forwarding-groups.

NAME

Specifies the QoS forwarding-group name.

Modes

Exec mode

Examples

The following example displays the QoS forwarding-group named FP1.

```
device# show qos forwarding-group Fp1
```

The following example displays all QoS forwarding-groups.

```
device# show qos forwarding-group all
```

show role

Displays all role information.

Syntax

show role

Parameters

role

Displays all role information.

Modes

Exec mode

Examples

The following example shows the defined roles available in the system.

```
device# show role
Role: admin
Type: SYSTEM_DEFINED
Description: Predefined admin role has access to all commands

Role: user
Type: SYSTEM_DEFINED
Description: Predefined user role has access to Show
commands and selected Exec commands
```

show route-map

Displays operational information a configured route map.

Syntax

show route-map [*name* | **all**]

Parameters

name

Specifies the name of the route map.

all

Specifies all configured route maps.

Modes

Exec mode

Output

The **show route-map** command displays match access-list status information, shown in the following examples.

Output field	Description
`match ip access-list acl4 (active)`	`(active)` status indicates that the bound match ACL has been created configured.
`match mac access-list acl2 (pending)`	`(pending)` status indicates that the bound match ACL has not been created or configured.

Examples

The following example shows the route map, `rmap1`.

```
# show route-map rm1
route-map rm1 1
forward-action permit
match ip access-list acl4 (active)
match mac access-list acl2 (pending)
egress-group eg1

Policy matches: 0 packets, 0 bytes, 0 Packets/sec, 0 Bits/sec
```

show running-config aaa

Displays the Authentication, Accounting, and Authorization (AAA) server accounting configuration.

Syntax

show running-config aaa

Modes

Exec mode

Examples

The following example shows the authentication mode.

```
device# show running-config aaa
aaa accounting exec default start-stop tacacs+
aaa accounting commands default start-stop tacacs+
```

show running-config access-list

Syntax

show running-config access-list [*name*]

Parameters

name

Specifies the name of an access-list.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows configuration information for all configured ACLs.

```
device# show running-config access-list
ipv6 access-list ip6-acl
  seq 10 permit ipv6 2001::1 2001::0 2002::2 2002::0

ip access-list ip-acl
  seq 20 permit ip 10.0.0.1 255.0.0.0 20.0.0.2 255.0.0.0

mac access-list L2
```

The following example shows configuration for ip6-acl.

```
device# show running-config access-list ip6-acl
ipv6 access-list ip6-acl
  seq 10 permit ipv6 2001::1 2001::0 2002::2 2002::0
```

show running-config acl-config

Displays the ACL common configuration information.

Syntax

show running-config acl-config

Modes

Exec mode

Examples

The following example shows the authentication mode.

```
device# show running-config acl-config
acl-config
no enable acl-counter
```

show running-config banner

Displays the configured banner message.

Syntax

show running-config banner

Modes

Exec mode

Examples

The following example shows the configured banner message.

```
device# show running-config banner
banner login "This is sample login message"
banner motd "This is sample motd message
```

show running-config clock

Displays the clock time-zone information.

Syntax

show running-config clock

Modes

Exec mode

Examples

The following example shows system clock information.

```
device# show running-config clock
clock timezone Asia/Kolkata
```

show running-config egress

Displays configuration information for configured egress.

Syntax

show running-config egress *name*

Parameters

name

Specifies the name of the egress.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows egress configuration information for ep1.

```
device# show egress ep1
           Name : ep1
       Description : egress_obj_1

Encap : encap_gre
    Listener Policy : lp1
         Precedence : 10
             Interface : ethernet 1/2
```

The following example show configuration information for all configured egresses.

```
device# show egress all
    Name : e1
       Description : egress_obj_1
               Encap : encap_gre
       Listener Policy : v4
         Precedence : 12
               Interface : ethernet 1/9
```

show running-config egress-group

Displays configuration detail for egress groups.

Syntax

show running-config egress-group[*name*]

Parameters

name

Specifies the egress group name.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows configuration information for all configured egress groups.

```
device# show running-config egress-group
egress-group eg_1
  description egress-group_1
  set egress e2
egress-group eg_2
  description egress-group_2
```

show running-config encap

Displays the encap configuration information.

Syntax

show running-config encap

Modes

Exec mode

Examples

The following examples show encap configuration information.

```
device# show running-config encapencap encap1
encap-type gre
source-ipv4-addr 1.1.1.1
destination-ipv4-addr 2.2.2.2
source-mac-addr 00:00:00:11:11:11
destination-mac-addr 00:00:00:22:22:22
vlan-id 100
vlan-pcp 3
```

show running-config ingress-group

Displays ingress-group configuration information.

Syntax

show running-config ingress-group [*name*]

Parameters

ingress-group *name*

Specifies an ingress-group.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows configurations for all configured ingresses.

```
device# show running-config ingress-group
ingress-group ig1
  traffic-type gtpu mode decap
  traffic-type gtpu ip any any
  traffic-type vxlan outer ip any any
  set route-map rm2
ingress-group ig2
  traffic-type gtpu teid 3000 mode new-scope
  traffic-type gtpu ip 10.10.10.1 255.255.255.255 20.20.20.1 255.255.255.255
  traffic-type vxlan outer vni 100
  traffic-type vxlan outer ip any any
  traffic-type vxlan outer mirror m1
  set route-map rm1
ingress-group ig3
  traffic-type gtpu mode decap
  traffic-type gtpu ip 30.30.30.1 255.255.255.255 40.40.40.1 255.255.255.255
  traffic-type vxlan outer ip any any
  set route-map rm2
```

The following example shows configuration for the ingress-group, `ig1`.

```
device# show running-config ingress-group ig1
ingress-group ig1
  traffic-type gtpu mode decap
  traffic-type gtpu ip any any
  traffic-type vxlan outer ip any any
  set route-map rm2
```

show running-config interface

Displays the interface configuration information.

Syntax

show running-config interface ethernet *IFNAME*

show running-config interface management *number*

show running-config interface port-channel *PORANGE*

Parameters

interface

Displays the running-configuration information.

ethernet *IFNAME*

Specifies the interface name in slot/port or slot/port:breakout format. Example: 1/1, 1/1-3, 5, 2/7-9, 10:1-4.

management *number*

Specifies the management interface number.

port-channel *PORANGE*

Specifies the channel number or channel number range.

Modes

Exec mode

Examples

The following examples show running-config interface.

```
device# show running-config interface ethernet 1/1
interface ethernet 1/1
shutdown
```

```
device# show running-config interface management 0
interface management 0
no ip address dhcp
ip gateway 10.20.73.138
no ipv6 address dhcp
ipv6 address fc00:0:0:12:10:20:73:155/64
ipv6 gateway fc00:0:0:12::1
no shutdown
```

```
show running-config interface port-channel 1
interface port-channel 1
load-balance src-dst-ip-l4port-tid
no shutdown
```

show running-config ip

Displays the IP configuration information.

Syntax

show running-config ip

show running-config ip access-list [**all** | *NAME*]

show running-config ip

Modes

Exec mode

Examples

The following examples show running IP access-list configurations.

```
device# show running-config ip access-list P4
ip access-list P4

device# show running-config ip access-list all
ip access-list P4
```

show running-config ip dns

Displays configuration detail for IP DNS configurations.

Syntax

show running-config ip dns

Modes

Exec mode

Examples

The following example shows configuration detail for all IP domain name servers.

```
device# show running-config ip dns
ip dns domain-name corp.extremenetworks.com
ip dns domain-name extremenetworks.com
ip dns name-server 10.6.16.32
ip dns name-server 10.6.24.30
ip dns name-server 1111:2222::1
```

show running-config ipv6

Displays the IPv6 configuration information.

Syntax

show running-config ipv6

show running-config ipv6 access-list [**all** | *NAME*]

Modes

Exec mode

Examples

The following examples show running IPv6 access-list configurations.

```
device# show running-config ipv6 access-list ip6-acl
ipv6 access-list ip6-acl

device# show running-config ipv6 access-list all
ipv6 access-list ip6-acl
```

show running-config lacp

Displays LACP configuration information.

Syntax

show running-configuration lacp

Modes

Exec mode

Examples

The following example shows LACP configuration information.

```
device# show running-configuration lacp
protocol lacp
  lacp system-priority 631
interface port-channel 100
  lacp min-links 2
  lacp system-mac 0001.0002.0003
  lacp system-priority 256
interface ethernet 1/4
  channel-group 100 mode active
interface ethernet 2/9
  channel-group 100 mode passive
  lacp rate fast
  lacp port-priority 123
interface ethernet 3/16
  channel-group 100 mode active
```

show running-config listener-policy

Displays configuration detail of a listener policy for an egress.

Syntax

show running-config listener-policy [*name*]

Parameters

name

Specifies the name of the listener policy.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows the IPv4 listener policy configuration.

```
device# show running-config listener-policy
listener-policy LP1 1
  forward-action permit
  match ip access-list ip1
  truncate 200
  strip vlan-tag
```

show running-config lldp

Displays LLDP configuration information.

Syntax

show running-configuration lldp

Modes

Exec mode

Examples

The following example shows LLDP configuration information.

```
device# show running-configuration lldp

Global LLDP Configurations:
no protocol lldp
lldp hello-timer 120
lldp holdtime 300
no lldp transmit
no lldp receive

Interface Level configurations:
Interface ethernet 1/1
no lldp enable
no lldp transmit
no lldp receive
```

show running-config mac

Displays the MAC configuration information.

Syntax

show running-config mac

show running-config mac access-list [**all** | *NAME*]

Modes

Exec mode

Examples

The following examples show running MAC access-list configurations.

```
device# show running-config mac access-list L2
mac access-list L2

device# show running-config mac access-list all
mac access-list L2
```

show running-config mirror

Displays the mirror configuration information.

Syntax

show running-config mirror

Modes

Exec mode

Examples

The following examples show the mirror configuration.

```
device# show running-config mirror
mirror m1
  description mirror-1
  set interface ethernet 1/4
mirror m2
  description mirror-2
  set interface ethernet 2/4

device# show running-config mirror m1
mirror m1
  description mirror-1
  set interface ethernet 1/4
```

show running-config ntp

Displays the ntp configuration information.

Syntax

show running-config ntp [**server** | **peer**]

Parameters

server

Specifies the NTP server IP address.

peer

Specifies the NTP peer IP address.

Modes

Exec mode

Examples

The following example shows the configured NTP details.

```
device# show running-config ntp
ntp enable
ntp peer 10.12.145.32
ntp server 10.12.145.36
ntp server 10.12.155.42
```

The following examples show the configured NTP peers.

```
device# show running-config ntp peer
ntp peer 10.12.145.32
```

The following examples show the configured NTP servers.

```
device# show running-config ntp server
ntp server 10.12.145.36
ntp server 10.12.155.42
```

show running-config qos

Displays the QoS configuration information.

Syntax

show running-config qos

Modes

Exec mode

Examples

The following example shows the configured QoS information.

```
device# show running-config qos

qos
  forwarding-group Fp1
    description group-for-site-A-to-B
    queue q1
```

show running-config route-map

Displays route-map configuration information for the current system.

Syntax

show running-config route-map *name*

Parameters

name

Specifies the name of the route-map.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows configuration information for rmap1.

```
device# show running-config route-map rmap1
route-map rmap1 10
  forward-action permit
```

The following example shows configuration information for all route-maps.

```
device# show running-config route-map
route-map R1 10
  forward-action permit
  match ip access-list test_1
  set egress-group eg_1
route-map R1 12
  forward-action permit
  match ip access-list test_2
route-map rmap1 10
  forward-action permit
```

show running-config snmp-server

Displays running SNMP configurations on the device.

Syntax

show running-config snmp-server

Modes

Exec mode

Examples

The following example shows all SNMP configurations tried on the device.

```
device# show running-config snmp-server
snmp-server community test123
snmp-server host 1.1.1.1 comm1 162 version 2c

device# show running-config snmp-server
snmp-server user user1 auth md5 auth-key authkey1 priv aes priv-key privkey1
snmp-server user user2 auth sha auth-key authkey2 priv nopriv
snmp-server user user3 noauth
```

show running-config system logging host

Displays logging host configuration details.

Syntax

show running-config system logging host *name*

Parameters

name

Specifies the host name or label.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows configuration for all logging hosts on the device.

```
device# show running-config system logging host
system logging host H1
  address 1.1.1.1

system logging host logger
  address 192.168.1.1
  port 514
  transport TCP
  secure-forwarding TLS

system logging host myServer
  address 10.20.30.40
  port 515
```

The following example shows configuration information for the logging host `logger`.

```
device# show running-config system logging host logger
system logging host logger
  address 192.168.1.1
  port 514
  transport TCP
  secure-forwarding TLS
```

show running-config system logging service

Displays configured logging severity levels for microservices.

Syntax

show running-config system logging service *name*

Parameters

name

Specifies the name of the service. Example: `chassis-mgr`, `interface-mgr`, `snmp`, `api-gw`, `packet-mgr`.

Supports 1-64 characters.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all.

Examples

The following example shows the configuration for the chassis service.

```
device# show running-config system logging service chassis-mgr
```

show running-config tacacs-server

Display the TACACS+ server configuration.

Syntax

show running-config tacacs-server

Modes

Exec mode

Examples

The following example shows the TACACS+ server configuration.

```
device# show running-config tacacs-server
tacacs-server host 10.24.65.6
     encrypted-key "jahasjikjdoaskjuihuhiaoljsiaknkaiua="
```

show running-config transport-tunnel

Displays the transport tunnel configuration information.

Syntax

show running-config transport-tunnel

Modes

Exec mode

Examples

The following examples show transport tunnel configuration.

```
device# show running-config transport-tunnel
transport-tunnel tt1
  tunnel-type gre ipv4-src 10.202.180.10 255.255.255.0
  deny ipv4-dest 103.10.150.225 255.255.255.0
  set ingress-group ig1
transport-tunnel tt2
  tunnel-type gre ipv4-src 10.202.181.10 255.255.255.0
  deny ipv4-dest 103.10.151.225 255.255.255.0
  set ingress-group ig2

device# show running-config transport-tunnel tt1
transport-tunnel tt1
  tunnel-type gre ipv4-src 10.202.180.10 255.255.255.0
  deny ipv4-dest 103.10.150.225 255.255.255.0
  set ingress-group ig1
```

show running-config username

Displays all usernames and role, password, and encryption level for each.

Syntax

show running-config username

Modes

Exec mode

Examples

The following example shows username, role, password, and encryption level for each.

```
device# show running-config username

username testuser1 role admin password $6$salt$cevuzTZ/QBjzuZG0/
ebEeedmcTnhyM8ITUu8K032Cp2XvIibq7voqYagm18bwpLBqrg/l/l6YxTmKKibJz5r10 encryption-level 10

username testuser2 role user password $6$salt$cevuzTZ/QBjzuZG0/
ebEeedmcTnhyM8ITUu8K032Cp2XvIibq7voqYagm18bwpLBqrg/l/l6YxTmKKibJz5r10 encryption-level 10
```

show snmp-server

Displays all SNMP-related information on the device.

Syntax

show snmp-server

Modes

Exec mode

Examples

The following example shows SNMP-related information for the device.

```
device# show snmp-server
snmp-server community test123
snmp-server host 1.1.1.1 comm1 162 version 2c

device# show snmp-server
snmp-server user user1 auth md5 auth-key authkey1 priv aes priv-key privkey1
snmp-server user user2 auth sha auth-key authkey2 priv nopriv
snmp-server user user3 auth noauth
```

show sysinfo all

Displays all system HW component information such as FANs, PSUs, sensors, slots, and LEDs.

Syntax

show sysinfo all

Modes

Exec mode

Examples

The following example shows all hardware information.

```
device# show sysinfo all
Fan Information
Id     Status      RPM     Percentage SpeedLevel     Direction
-------------------------------------------------------------
1      Up          7300    41         MEDIUM         FAN_DIR_F2B
2      Up          7300    41         MEDIUM         FAN_DIR_F2B
3      Up          7300    41         MEDIUM         FAN_DIR_F2B
4      Up          7300    41         MEDIUM         FAN_DIR_F2B
5      Up          7300    41         MEDIUM         FAN_DIR_F2B

FAN_DIR_F2B - Fan Airflow Direction is FrontToBack

FanSpeedLevel - <40%[LOW],40-70%[MEDIUM],>70%[HIGH]

Led Information
Id     State     Color     Description
-----------------------------------------------------------
led-0  Solid     GREEN     Power Supply Unit
led-1  Solid     GREEN     Fan
led-2  Solid     GREEN     System Status

PSU Information
Id     Status      Type    C[in]   C[out]  P[in]   P[out]  V[in]   V[out]
-------------------------------------------------------------------------
1      Up          AC      3       53      684     632     206     11
2      Up          AC      3       51      660     612     206     11

**C - Current in Amps ,**P - Power in Watts ,**V - Voltage in Volts
Total power budget for chassis = 3200 Watts
Total power used by LC and system core = 2040 Watts
Total power available = 1160 Watts
Power Board CpldVersion = 00 09
Sensor Information
Id   Name        Current(°C/Volt) Warning(°C/Volt) Critical(°C/Volt) Shutdown(°C/Volt)
-------------------------------------------------------------------------------------------------------
1    CPU Core       37                85               90.00            0.00
2    TF2 MAC        42.00             75               80              95.00
3    TF2 Serdes1    56.00             80.00            85.00           95
4    TF2 Serdes2    50.00             80.00            85              95
5    TF2 Serdes3    54                80.00            85              95.00
6    TF2 Serdes4    53                80.00            85.00           95
7    LC1 PHY MAX    70.00             115              120.00          125.00
```

```
8    LC1 QSFP MAX   38                63.00            68.00            73.00
9    LC2 PHY MAX    67               115.00           120              125.00
10   LC2 QSFP MAX   38.00              63               68.00            73.00
11   LC3 PHY MAX    66               115.00           120              125
12   LC3 QSFP MAX   41.00             63.00            68               73.00
13   LC4 PHY MAX    67               115.00           120.00           125.00
14   LC4 QSFP MAX   40                63.00            68               73
15   LC5 PHY MAX    67               115.00           120.00           125
16   LC5 QSFP MAX   36                63               68               73.00
17   LC6 PHY MAX    59.00            115.00           120.00           125.00
18   LC6 QSFP MAX   28.00             63.00            68.00            73.00
19   LC7 PHY MAX    57.00            115.00           120.00           125
20   LC7 QSFP MAX    0.00             63               68.00            73
21   LC8 PHY MAX    64.00            115.00           120.00           125.00
22   LC8 QSFP MAX   44.00             63               68.00            73
23   DIMM1          36                80               85.00             0
24   DIMM2          32                80               85.00             0
25   DIMM3          35                80               85.00             0.00
26   DIMM4          33.00             80               85.00             0.00
27   SSD            39.00             75.00            80.00             0.00
28   BMC-12V        12.00              0               12               12.00
29   BMC-3_3V        3                 0.00             3.00             3
30   SWB-075V        0                 0                0               0.00
31   SWB-3_3V        3.00              0.00             3                3.00
32   SWB-2_5V        2.00              0.00             2.00             2.00
33   SWB-1_8V        1                 0.00             1.00             1
34   SWB-1_5V        1.00              0.00             1.00             1
35   SWB-1_2V        1.00              0                1                1.00

Slot Information
Slot  State         FRU-Id  FRU-Type    Description
-------------------------------------------------------------------
1     Online        1       LC16x100G   16x100G QSFP28 Line Card
2     Online        1       LC16x100G   16x100G QSFP28 Line Card
3     Online        1       LC16x100G   16x100G QSFP28 Line Card
4     Online        1       LC16x100G   16x100G QSFP28 Line Card
5     Online        1       LC16x100G   16x100G QSFP28 Line Card
6     Online        1       LC16x100G   16x100G QSFP28 Line Card
7     Online        1       LC16x100G   16x100G QSFP28 Line Card
8     Online        1       LC16x100G   16x100G QSFP28 Line Card
```

show sysinfo fan

Displays all 5 FAN HW component information.

Syntax

show sysinfo fan

Modes

Exec mode

Usage Guidelines

The airflow direction is by default FrontToBack.

Examples

The following example shows all hardware information.

```
device# show sysinfo fan

Fan Information
Id     Status      RPM     Percentage SpeedLevel     Direction
-------------------------------------------------------------------------------
1      UP          4300    24         LOW            FAN_DIR_F2B
2      UP          4100    23         LOW            FAN_DIR_F2B
3      UP          4300    24         LOW            FAN_DIR_F2B
4      UP          4300    24         LOW            FAN_DIR_F2B
5      UP          4300    24         LOW            FAN_DIR_F2B

FAN_DIR_F2B - Fan Airflow Direction is FrontToBack
FanSpeedLevel - <40%[LOW],40-70%[MEDIUM],>70%[HIGH]
```

show sysinfo led

Displays the front panel system LED values.

Syntax

show sysinfo led

Modes

Exec mode

Usage Guidelines

The steady Green LEDs indicate that there are no issues and the steady or blinking Amber LEDs indicate a warning.

Examples

The following example shows system LED status.

```
device# show sysinfo led

Led Information
Id     State     Color     Description
-----------------------------------------------------------------
led-0  Solid     GREEN     Power Supply Unit
led-1  Solid     GREEN     Fan
led-2  Solid     GREEN     System Status
```

show sysinfo power-supply

Displays the hardware power supply information.

Syntax

show sysinfo power-supply

Modes

Exec mode

Examples

The following example configures the VXLAN traffic type.

```
device# show sysinfo power-supply

PSU Information
Id     Status      Type    C[in]   C[out]  P[in]   P[out]  V[in]   V[out]
-------------------------------------------------------------------------------
1      UP          AC      2       33      408     130     210     11
2      UP          AC      2       32      424     143     210     11
3      Unplugged   Empty   0       0       0       0       0       0
4      Unplugged   Empty   0       0       0       0       0       0

Total power budget for chassis = 3200 Watts
Total power used by LC and system core = 2040 Watts
Total power available = 1160 Watts
```

show sysinfo sensor

Displays sensor data.

Syntax

show sysinfo sensor [**all** | **cpu** | **lc** | **mem_mod** | **voltage**]

Parameters

all

Displays information for all sensors.

cpu

Displays CPU information.

lc

Displays line card (slot) information.

mem_mod

Displays memory module information.

voltage

Displays voltage information.

Modes

Exec mode

Examples

The following example shows information for all sensors.

```
device# show sysinfo sensor all
Sensor Information
Id   Name        Current(°C/Volt) Warning(°C/Volt) Critical(°C/Volt) Shutdown(°C/Volt)
-------------------------------------------------------------------------------------
1    CPU Core        33              85               90.00             0
2    TF2 MAC         41              75               80                95.00
3    TF2 Serdes1     56              80.00            85.00             95
4    TF2 Serdes2     50.00           80.00            85                95
5    TF2 Serdes3     54.00           80.00            85.00             95
6    TF2 Serdes4     53.00           80               85.00             95.00
7    LC1 PHY MAX     70             115              120               125
8    LC1 QSFP MAX    38              63.00            68.00             73
9    LC2 PHY MAX     67.00          115.00           120.00            125.00
10   LC2 QSFP MAX    38.00           63.00            68.00             73
11   LC3 PHY MAX     66.00          115.00           120.00            125.00
12   LC3 QSFP MAX    41.00           63.00            68.00             73.00
13   LC4 PHY MAX     67.00          115.00           120.00            125.00
14   LC4 QSFP MAX    40              63               68                73
15   LC5 PHY MAX     67             115              120.00            125.00
16   LC5 QSFP MAX    36              63.00            68.00             73
17   LC6 PHY MAX     59             115.00           120.00            125.00
18   LC6 QSFP MAX    28.00           63.00            68                73.00
19   LC7 PHY MAX     57             115              120.00            125
```

```
20   LC7 QSFP MAX     0.00           63.00           68.00           73.00
21   LC8 PHY MAX     64             115             120.00          125
22   LC8 QSFP MAX    44.00           63              68.00           73
23   DIMM1           36              80.00           85.00            0.00
24   DIMM2           32              80.00           85               0.00
25   DIMM3           35.00           80.00           85               0
26   DIMM4           33.00           80              85.00            0.00
27   SSD             39              75              80               0
28   BMC-12V         12               0              12.00           12
29   BMC-3_3V         3.00            0               3.00            3
30   SWB-075V         0               0.00            0.00            0.00
31   SWB-3_3V         3.00            0               3               3
32   SWB-2_5V         2               0               2.00            2.00
33   SWB-1_8V         1.00            0               1               1.00
34   SWB-1_5V         1               0.00            1               1
35   SWB-1_2V         1               0               1.00            1.00
```

The following example shows CPU information.

```
device# show sysinfo sensor cpu

Sensor Information
Id    Name       Current(°C/Volt) Warning(°C/Volt) Critical(°C/Volt) Shutdown(°C/Volt)
-------------------------------------------------------------------------------------
1   CPU Core        33               85.00           90.00            0
2   TF2 MAC         41               75.00           80               95
3   TF2 Serdes1     56.00            80.00           85.00            95
4   TF2 Serdes2     50.00            80              85.00            95.00
5   TF2 Serdes3     54.00            80              85               95
6   TF2 Serdes4     53.00            80.00           85               95
```

The following module show line card (slot) information.

```
device# show sysinfo sensor lc

Sensor Information
Id   Name        Current(°C/Volt) Warning(°C/Volt) Critical(°C/Volt) Shutdown(°C/Volt)
-------------------------------------------------------------------------------------
7   LC1 PHY MAX       70             115.00           120              125.00
8   LC1 QSFP MAX      38.00           63.00            68               73.00
9   LC2 PHY MAX       67             115.00           120              125.00
10  LC2 QSFP MAX      38.00           63               68.00            73
11  LC3 PHY MAX       66             115              120.00           125
12  LC3 QSFP MAX      41.00           63.00            68               73.00
13  LC4 PHY MAX       67             115              120              125
14  LC4 QSFP MAX      40.00           63.00            68               73
15  LC5 PHY MAX       67             115              120              125
16  LC5 QSFP MAX      36.00           63               68               73
17  LC6 PHY MAX       59.00          115.00           120.00           125
18  LC6 QSFP MAX      28.00           63               68               73.00
19  LC7 PHY MAX       57.00          115.00           120.00           125
20  LC7 QSFP MAX       0.00           63.00            68               73.00
21  LC8 PHY MAX       64             115.00           120.00           125.00
22  LC8 QSFP MAX      44              63.00            68.00            73
```

The following example shows memory module information.

```
device# show sysinfo sensor mem_mod

Sensor Information
Id   Name  Current(°C/Volt) Warning(°C/Volt) Critical(°C/Volt) Shutdown(°C/Volt)
-------------------------------------------------------------------------------
23  DIMM1       36             80               85                0
24  DIMM2       32             80.00            85.00             0.00
```

```
25  DIMM3       35              80.00             85.00              0.00
26  DIMM4       33              80.00             85.00              0
27  SSD         39.00           75                80.00              0.00
```

The following example shows voltage information.

```
device# show sysinfo sensor voltage

Sensor Information
Id   Name      Current(°C/Volt) Warning(°C/Volt)  Critical(°C/Volt) Shutdown(°C/Volt)
-------------------------------------------------------------------------------------
28   BMC-12V      12.00             0                 12.00              12.00
29   BMC-3_3V      3.00             0                  3.00               3.00
30   SWB-075V      0.00             0.00               0                  0
31   SWB-3_3V      3.00             0.00               3.00               3.00
32   SWB-2_5V      2.00             0.00               2                  2.00
33   SWB-1_8V      1                0.00               1.00               1
34   SWB-1_5V      1.00             0.00               1                  1.00
35   SWB-1_2V      1.00             0                  1.00               1.00
36   SWB-1V        1                0                  1                  1
37   SWB-VCORE     0                0                  0                  0
```

show sysinfo slot

Displays the line card or slot status.

Syntax

show sysinfo slot

Modes

Exec mode

Examples

The following example displays the line card or slot status information.

```
device# show sysinfo slot
Slot Information
Slot  State         FRU-Id  FRU-Type    Description
-------------------------------------------------------------------
1     Initializing  1       LC16x100G   16x100G QSFP28 Line Card
2     Initializing  1       LC16x100G   16x100G QSFP28 Line Card
3     Initializing  1       LC16x100G   16x100G QSFP28 Line Card
4     Initializing  1       LC16x100G   16x100G QSFP28 Line Card
5     Initializing  1       LC16x100G   16x100G QSFP28 Line Card
6     Initializing  1       LC16x100G   16x100G QSFP28 Line Card
7     Initializing  1       LC16x100G   16x100G QSFP28 Line Card
8     Initializing  1       LC16x100G   16x100G QSFP28 Line Card

Slot Information
Slot  State         FRU-Id  FRU-Type    Description
-------------------------------------------------------------------
1     Online        1       LC16x100G   16x100G QSFP28 Line Card
2     Online        1       LC16x100G   16x100G QSFP28 Line Card
3     Online        1       LC16x100G   16x100G QSFP28 Line Card
4     Online        1       LC16x100G   16x100G QSFP28 Line Card
5     Online        1       LC16x100G   16x100G QSFP28 Line Card
6     Online        1       LC16x100G   16x100G QSFP28 Line Card
7     Online        1       LC16x100G   16x100G QSFP28 Line Card
8     Online        1       LC16x100G   16x100G QSFP28 Line Card
```

show system internal

Shows data stored in the specified database in JSON format.

Syntax

show system internal {{ **cdb** | **sdb**| **psdb** } *keypath* }

Parameters

cdb

Specifies data in the config database.

sdb

Specifies data in the state database.

psdb

Specifies data in the persistent state database.

keypath

Specifies a YANG-compliant path.

Modes

Exec mode

Usage Guidelines

Depending on selected Database type and provided keypath, configured data will be showed in JSON format.

If the command is run with a keypath where data is not present in database, a “No Data” message is displayed.

Examples

The following example shows internal config database information for route maps.

```
device# show system internal cdb /routemaps

key /routemaps
{
  "routemap": [
   {
    "name": "rm1",
    "routemap-instances": {
     "routemap-instance": [
      {
       "config": {
        "egress-group": "est",
        "ipv4-acl": "acl1",
        "permit-deny": true
       },
       "sequence-id": 10
```

```
        }
      ]
    }
  }
```

show system logging host

Displays successfully applied logging host details.

Syntax

show system logging host [*name*]

Parameters

name

Specifies the hostname or label.

Modes

Exec mode

Usage Guidelines

No information displays if the specified host is not found.

Examples

The following example shows logging information for all system logging hosts.

```
device# show system logging host
System Logging Hosts: System Logging Hosts:

HOSTNAME          ADDRESS            PORT    TRANSPORT    SECURE-FORWARDING

-------------------------------------------------------------------------

H1                1.1.1.1             514          UDP                 NONE

logger            192.168.1.1         514          TCP                  TLS

myServer          10.20.30.40         515          UDP                 NONE
```

The following example shows logging information for system host `logger`.

```
device# show system logging host logger
System Logging Hosts:
HOSTNAME    ADDRESS     PORT  TRANSPORT  SECURE-FORWARDING
-------------------------------------------------------------------------
logger     192.168.1.1    514    TCP       TLS
```

show system logging service

Displays severity level for the specified or all services.

Syntax

show system logging service *name*

Parameters

name

Specifies the name of the service. Example: `chassis-mgr`, `interface-mgr`, `snmp`, `api-gw`, `packet-mgr`.

Supports 1-64 characters.

Modes

Exec mode

Usage Guidelines

You can run this command without specifying a name to display configuration information for all system services.

Examples

The following example shows the configured logging severity for all services.

```
device(config)#show system logging service
Service                   Severity
========================= ========
api-gw                    DEBUG
chassis-mgr               DEBUG
interface-agent           DEBUG
interface-mgr             DEBUG
nexthop-agent             DEBUG
packet-mgr                DEBUG
pbd-agent                 DEBUG
pcap-agent                DEBUG
pipeline-agent            DEBUG
security                  DEBUG
sfcs-agent                DEBUG
snmp                      DEBUG
svcplane-agent            DEBUG
target-proxy-agent        DEBUG
```

show system service

Displays all services and corresponding versions.

Syntax

show system service

Modes

Exec mode

Examples

The following example shows all system services.

```
device# show system service

SERVICE                 CURRENT          ROLLBACK    READY     STATE       RESTARTS
                        VERSION          VERSION
-------------------------------------------------------------------------------------
api-gw                  1.1.0            None        true      Running     0
chassis-mgr             1.2.0            None        true      Running     0
cli                     1.1.0            None        true      Running     0
config-db               1.1.0            None        true      Running     0
interface-agent         1.1.0            None        true      Running     0
interface-mgr           1.2.0            None        true      Running     0
lacp                    1.0.0            None        true      Running     0
lldp                    1.0.0            None        true      Running     0
msg-bus                 1.1.0            None        true      Running     0
nexthop-agent           1.1.0            None        true      Running     0
packet-mgr              1.2.0            None        true      Running     0
pbd-agent               1.1.0            None        true      Running     0
pcap-agent              1.1.0            None        true      Running     0
persistent-state-db     1.1.0            None        true      Running     0
pipeline-agent          1.1.0            None        true      Running     0
security                1.1.0            None        true      Running     0
sfcs-agent              1.1.0            None        true      Running     0
snmp                    1.1.0            None        true      Running     0
state-db                1.1.0            None        true      Running     0
stratum                 0.4.18-4.14.49   None        true      Running     0
svcplane-agent          1.1.0            None        true      Running     0
target-proxy-agent      1.1.0            None        true      Running     0
```

show transport-tunnel

Displays configuration of all or specified transport tunnels.

Syntax

show transport-tunnel [**all** | *tunnel-name*]

Parameters

all

Displays configurations for all configured transport tunnels.

tunnel-name

Specifies the name of the tunnel.

Modes

Exec mode

Usage Guidelines

Valid transport tunnel name must be provided.

Examples

The following example shows configured transport tunnel information for tunnel-1.

```
# show transport-tunnel tunnel-1
name           : tunnel-1
tunnel-type    : erspan
tunnel-id      : 12345
source IP      : 10.10.10.0
source IP mask : 255.255.255.0
dest IP        : 20.20.20.0
dest IP mask   : 255.0.0.0
ingress-group  : ig1
```

show usb

Displays whether USB access is enabled.

Syntax

show usb

Modes

Exec mode

Examples

The following example displays access status to the USB.

```
device# show usb
USB Enabled: true
```

show users

Displays all active user sessions information.

Syntax

show users

Modes

Exec mode

Examples

The following example shows the active user sessions in the system.

```
device# show users

Username        Role       Host IP          Device          Time Logged In
=============== ========== ================ =============== ===============
root            admin      -                Console         04:40
admin           admin      192.168.122.1    SSH             04:47
user            user       192.168.122.1    SSH             04:48
```

show version

Displays version information for firmware and services.

Syntax

show version

Modes

Exec mode

Examples

```
device# show version

NGNPB Operating System Software
Copyright (c) 2020 Extreme Networks Inc.

Firmware Info:
Current Firmware Version:        NGNPB_v21.0.7.0-20210430_082447_UTC
Rollback Firmware Version:       None
BMC Firmware Version:            None
Kernel:                          4.14.49-OpenNetworkLinux

System Uptime:                   0 day(s), 06:41:35

MicroService Info:
SERVICE            CURRENT   ROLLBACK   READY    STATE     RESTARTS
                   VERSION   VERSION
------------------------------------------------------------------------------
agent-pbd-ms        0.1.0     None      true     Running      0
agent-pipeline-ms   0.1.0     None      true     Running      0
agent-sp-intf-ms    0.1.0     None      true     Running      0
--More--
```

shutdown

Enables (no shutdown) or disables (shutdown) an interface.

Syntax

shutdown

no shutdown

Modes

Interface config mode

Usage Guidelines

The **no shutdown** command enables the interface.

This command is available only to users with the admin role.

Examples

The following example disables the interface.

```
device# configure terminal
device(config)# interface ethernet 1/10
device(config-if-eth 1/10)# shutdown

device(config)# interface ethernet 1/1-5
device(config-if-eth 1/1-5)# shutdown

device# show running interface ethernet 1/10
Interface ethernet 1/10
Shutdown
```

snmp-server community

Configures the SNMP community.

Syntax

snmp-server community *name*

no snmp-server community *name*

Parameters

name

Specifies the community name. Community string must start with a character and can contain only alpha-numeric characters. Valid string range is 2-16 characters.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

A maximum of 256 community strings are supported.

All configured communities have READ-only permissions.

Examples

The following example configures the extremero community for the SNMP server and confirms the configuration with the show command.

```
device# configure terminal
device(config)# snmp-server community extremero
device(config)# end

device# show snmp-server
snmp-server community extremero
snmp-server host 10.23.17.128 public 162 version 2c
```

The following example removes the extremero SNMP community.

```
device# configure terminal
device(config)# no snmp-server community extremero
```

snmp-server host

Configures the agent with the SNMP trap destination information with the community or user-name attached to it.

Syntax

snmp-server { **host** [*ip-address* | *host*] **comm-user** *udp-port* **version** [*1* | *2c* | *3*] }

no snmp-server { **host** [*ip-address* | *host*] **comm-user** }

Parameters

ip-address

Specifies the trap receiver unicast IPv4 or IPv6 address.

host

Specifies the host name of the trap receiver.

comm-user

Specifies the community string associated with SNMP traps. Community string must start with a character and can contain only alpha-numeric characters. The valid string length is 2 through 16 characters.

Supported on SNMP versions 1 and 2c.

udp-port

Specifies the port on which the receiver is listening for SNMP traps. Valid port range is 1 through 65535.

The default port is 162.

version [*1* | *2c* | *3*]

Specifies the SNMP version to be used to send SNMP traps. Default version is 2c.

If SNMP version is 3, the valid length is between 1 and 32 characters.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

This command combines a host and community string.

Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

The `no` form of the command removes the corresponding configuration.

Examples

The following example configures the SNMP server with the community string using version 2c.

```
device# configure terminal
device(config)# snmp-server host 10.23.17.128 public 162 version 2c

device(config)# do show running-config snmp-server
snmp-server host 10.23.17.128 public 162 version 2c
```

The following example removes the configured host and community string.

```
device# configure terminal
device(config)# no snmp-server host 10.23.17.128 public
```

snmp-server user

Configures the SNMP v3 user for authenticating.

Syntax

snmp-server { **user** [*user name*] **auth** [*noauth* | *md5* | *sha*] **auth-key** [*auth-key*] **priv** [*nopriv* | *aes* | *des*] **priv-key** [*priv-key*] }

Parameters

user *user name*

Specifies the SNMPv3 user name. Valid length is 1 to 32 characters.

auth [*noauth* | *md5* | *sha*]

Specifies the supported authentication method.

auth-key *auth-key*

Specifies the key phrase to be used for authentication. The auth-key string can contain only alpha-numeric characters. Valid string length is 8 to 40 characters.

priv [*nopriv* | *aes* | *des*]

Specifies the supported encryption method.

priv-key [*priv-key*]

Specifies the key phrase to be used for encryption. Valid priv-key length is 8 to 40 characters.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example configures an SNMP server user.

```
device(config)# snmp-server user user8 auth sha auth-key authKey1 priv aes priv-key
user1privkey

device(config)# snmp-server user user2 auth md5 auth-key authkey12 priv nopriv

device(config)# snmp-server user user3 auth noauth
```

source-ipv4-addr

Configures the source IP address for encapsulation of outgoing packets.

Syntax

source-ipv4-addr *ip-addr*

no source-ipv4-addr *ip-addr*

Parameters

ip-addr

Specifies the source IP address.

Modes

Encap config mode

Usage Guidelines

Validations for the command are as follows:

- Valid IP addresses must be provided.
- One IP address per encapsulation is allowed. The configured IP address must be removed before you configure a new IP address.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures the source IPv4 address.

```
device(config-encap-1)# source-ipv4-addr 10.10.10.1
device(config-encap-1)#

Show running:
device# show running-configuration

encap encap-1
source-ipv4-addr 10.10.10.1
```

source-mac-addr

Configures the source MAC address for encapsulation of outgoing packets.

Syntax

source-mac-addr *mac-addr*

no source-mac-addr *mac-addr*

Parameters

mac-addr

Specifies the source MAC address.

Modes

Encap config mode

Usage Guidelines

Validations for the command are as follows:

- A valid MAC address must be provided.
- One MAC address per encapsulation is allowed. The configured MAC address must be removed before you configure a new MAC address.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures the source MAC address.

```
device(config-encap)# source-MAC-addr 00:01:02:03:04:05

device# show running-configuration
encap encap-1
destination-mac-addr 00:01:02:03:04:05
```

speed (ethernet interfaces)

Configures the port speed on Ethernet interfaces.

Syntax

speed [**40000** | **100000** | **auto**]

Parameters

40000

Specifies 40 Gbps port speed.

100000

Specifies 100 Gbps port speed.

auto

Specifies auto detection. This is the default port speed.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is supported on Ethernet interfaces.

Examples

The following example configures the port speed on Ethernet interfaces.

```
device# configure terminal
device(config)# interface ethernet 2/16
device(config-if-mgmt-0)# speed 40000

device# show running-config interface e 2/16
interface ethernet 2/16
  speed 40000
  shutdown
```

speed (management interfaces)

Configures the port speed on management interfaces.

Syntax

speed [**10** | **100** | **auto**]

Parameters

10

Specifies 10 Mbps port speed.

100

Specifies 100 Mbps port speed.

auto

Specifies 1 Gbps port speed with auto negotiation. This is the default port speed.

Modes

Interface config mode

Usage Guidelines

This command is available only to users with the admin role.

This command is supported on management interfaces.

Examples

The following example configures the port speed on management interfaces.

```
device# configure terminal
device(config)# interface management 0
device(config-if-mgmt-0)# speed 100

device# show running-config interface management 0
interface management 0
speed 100
no shutdown
```

strip

Removes the specified headers from incoming packets (802.1BR, VN, or VLAN).

Syntax

strip [**br-tag** | **vlan-tag** | **vn-tag**]

no strip [**br-tag** | **vlan-tag** | **vn-tag**]

Parameters

br-tag

Strips 802.1BR tag from the packet header.

vlan-tag

Strips VLAN tag from the packet header.

vn-tag

Strips VN tag from the packet header.

Modes

Listener-policy config mode

Usage Guidelines

If `br-tag` is already enabled, `vn-tag` cannot be enabled.

The **no strip** command removes the strip configuration.

Examples

The following example removes the specified headers.

```
device# configure terminal
device(config)# listener-policy lp1 <sId>
device(config-listener-policy)# strip br-tag
device(config-listener-policy)# strip vlan-tag

listener-policy rt 45
  strip br-tag
  strip vlan-tag
```

system firmware commit

Commits the firmware version that is currently running.

Syntax

system firmware commit

Modes

Exec mode

Usage Guidelines

You must have the admin role to run this command.

You cannot commit a previously committed version.

There is no auto-commit after firmware update.

- If you are satisfied with the new update, run this command when the system reboots to commit the new firmware version.
- If the new firmware does not come up properly, you must run the **system firmware rollback** and remove the new image from the device.

Note
It is not necessary to run **system firmware commit** after you run **system firmware rollback**.

Examples

The following example runs the command to accept the running software version.

```
device# system firmware commit
```

system firmware rollback

Rolls back the firmware version to the previous running version.

Syntax

system firmware rollback

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example rolls back the firmware version to the previous running version.

```
device# system firmware rollback
```

system firmware update

Updates the system firmware.

Syntax

system firmware update FLASH-FILE

system firmware update USB-FILE

system firmware update SCP-FILE

system firmware update SFTP-FILE

system firmware update HTTP-FILE

system firmware update HTTPS-FILE

Parameters

FLASH-FILE

Specifies the flash file path in format `flash://firmware/filename`.

USB-FILE

Specifies the USB file path in format `usb://file-name`.

SCP-FILE

Specifies the SCP file path in format `scp://username:password@host[:port]/filepath`.

SFTP-FILE

Specifies the SFTP file path in format `sftp://username:password@host[:port]/filepath`.

HTTP-FILE

Specifies the HTTP file path in format `http://[username:password@]host[:port]/filepath`.

HTTPS-FILE

Specifies the HTTPS file path in format `https://[username:password@]host[:port]/filepath`.

username

Account name of the authorized user.

password

Password of the authorized user.

Note
As a best practice, do not list the password in the command line for security purposes.

hostname

Specifies the server by name or IP address. Both IPv4 and IPv6 are supported.

Hostname usage requires that DNS resolution is configured on the device.

port

Specifies the port number, which must be preceded by a colon. If the port is not included, the default port is assumed.

filepath

Specifies the path to the file.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Host IP must be in the format of a valid IPv4 or IPv6 address.

Firmware images are `.bin` files with the version format, `YearBorn.Major.Minor.Patch`.

There is no auto-commit after firmware update.

- After the firmware update, use the **`system firmware commit`** command to commit the new firmware version.
- Use the **`system firmware rollback`** command to remove the new image from the device.

Examples

The following examples update the system firmware.

```
device# system firmware update system firmware update flash://firmware/NPB-21.1.1.0-
NPB.bin

device# system firmware update usb://NPB-21.1.1.0-NPB.bin

device# system firmware update http://1.1.1.1:8000/path/NPB-21.1.0.0-NPB.bin

device# system firmware update scp://test:pass@1.1.1.1/path/NPB-21.1.0.0-NPB.bin

device# system firmware update sftp://test:pass@1.1.1.1/path/NPB-21.1.0.0-NPB.bin
```

system logging host

Enters into a sub-configuration mode for logging host parameter configuration.

Syntax

system logging [**host** *hostname*] [**address** *ip-address*] [**port** *port-number*] **transport** [*udp* | *tcp*] **secure-forwarding** [*tls* | *none*]

no system logging [**host** *hostname*]

Command Default

Default transport protocol: UDP

Default secure-forwarding encryption (host): none

Parameters

hostname

Specifies the name or label of the host. Valid length is 1 though 64 characters.

ip-address

Specifies the IP address for the host. Valid format is IPv4 dotted-decimal notation.

port-number

Specifies the port number of the remote syslog server. Valid port-number range is 514 through 530.

udp

Sends syslogs to remote server using UDP protocol. This is the default protocol.

tcp

Sends syslogs to remote server using TCP protocol.

tls

Sends syslogs to remote server using TLS encryption. Syslog CA certificates must be installed before configuring TLS encryption.

none

Sends syslogs in plain text. This is the default configuration for the host.

Modes

Exec mode

Usage Guidelines

You can configure a maximum of 10 logging hosts.

If the `no` version of the command is without the *hostname* option, all hosts are removed.

Syslog CA certificates must be installed before configuring TLS encryption.

Syslog CA certificates can be imported using the **`crypto import`** command.

Examples

The following example configures the host H1 as the system logging host and uses the show command to confirm the configuration.

```
device# configure terminal
device(config)# system logging host sysLogHost1
device(config-logging-host-sysLogHost1)# address 10.25.125.5
device(config-logging-host-sysLogHost1)# port 6154
device(config-logging-host-sysLogHost1)# transport TCP
device(config-logging-host-sysLogHost1)# secure-forwarding TLS

device# do show running-config system logging host
system logging host sysLogHost1
  address 10.25.125.5
  port 6514
  transport TCP
  secure-forwarding TLS
```

The following example configures transport TCP.

```
device(config-logging-host-H1)# transport TCP
Warning: Existing Host configuration changed
```

The following example removes all system logging hosts.

```
device# configure terminal
device(config)# no system logging host
```

system service rollback

Restores the specified system service to the previous running version.

Syntax

system service rollback *name*

Parameters

name

Specifies the name of the service. Example: `chassis-mgr`, `interface-mgr`, `snmp`, `api-gw`, `packet-mgr`.

Supports 1-64 characters.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example restores the previous running version of the `chassis-mgr` service.

```
device# system service rollback chassis-mgr
```

system logging service severity

Sets the logging level of a microservice.

Syntax

system logging service *name* **severity** [**alert** | **critical** | **emergency** | **error** | **warning** | **notice** | **info** | **debug** | **trace**]

no system logging service *name* **severity** [**alert** | **critical** | **emergency** | **error** | **warning** | **notice** | **info** | **debug** | **trace**]

Command Default

Default log level is DEBUG.

Parameters

name

Specifies the name of the service. Example: `chassis-mgr`, `interface-mgr`, `snmp`, `api-gw`, `packet-mgr`.

Supports 1-64 characters.

severity [**alert** | **critical** | **emergency** | **error** | **warning** | **notice** | **info** | **debug** | **trace**]

Specifies the logging level for the specified service.

Modes

Config mode

Usage Guidelines

The service name must be valid.

The `no` form of the command puts the log level back to the default log level (DEBUG level).

Examples

The following example configures the severity logging level for `chassis-mgr` and for `interface-mgr`.

```
device# configure terminal
device(config)# system logging service chassis-mgr severity error
device(config)# system logging service interface-mgr severity trace
```

system service update

Updates the service to a different version with minimal downtime.

Syntax

system service update FLASH-FILE

system service update USB-FILE

system service update SCP-FILE

system service update SFTP-FILE

system service update HTTP-FILE

system service update HTTPS-FILE

Parameters

FLASH-FILE

Specifies the flash file path in format `flash://ms-images/filename`.

USB-FILE

Specifies the USB file path in format `usb://filename`.

SCP-FILE

Specifies the SCP file path in format `scp://username:password@host[:port]/filepath`.

SFTP-FILE

Specifies the SFTP file path in format `sftp://username:password@host[:port]/filepath`.

HTTP-FILE

Specifies the HTTP file path in format `http://[username:password@]host[:port]/filepath`.

HTTPS-FILE

Specifies the HTTPS file path in format `https://[username:password@]host[:port]/filepath`.

username

Account name of the authorized user.

password

Password of the authorized user.

Note
As a best practice, do not list the password in the command line for security purposes.

hostname

Specifies the server by name or IP address (IPv4 or IPv6). Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.

Hostname usage requires that DNS resolution is configured on the device.

port

Specifies the port number, which must be preceded by a colon. If the port is not included, the default port is assumed.

filepath

Specifies the path to the file.

Modes

Exec mode

Usage Guidelines

Service images are `tar.gz` files with the version format, `major.minor.patch`.

Validations for the command are as follows:

- This command is available only to users with the admin role.
- The target destination must be valid and reachable.
- The *major.minor* version numbers must be identical between the current and new images.

Examples

The following example updates system service.

```
device# system service update flash://ms-images/chassis-mgr_1.1.0.tar.gz

device# system service update usb://chassis-mgr_1.1.0.tar.gz

device# system service update scp://test:pass@1.1.1.1/home/test/chassis-mgr_1.1.0.tar.gz

device# system service update sftp://test:pass@1.1.1.1/home/test/
interface_mgr_1.1.0.tar.gz

device# system service update http://1.1.1.1:8000/home/test/packet-mgr_1.1.0.tar.gz
```

tacacs-server

Configures a Terminal Access Controller Access-Control System plus (TACACS+) server.

Syntax

tacacs-server host *ip address* { *plain-key* | *encrypted-key* }

no tacacs-server host *ip address* **no key**

Parameters

host

Specifies the IPv4 or IPv6 address of the TACACS+ server.

plain-key

Specifies a secret string shared with the TACACS+ server in plain-text format. Supports 1 through 40 characters.

encrypted-key

Specifies a secret string shared with the TACACS+ server in encrypted format. Supports 1 through 128 characters.

Modes

Config mode

Usage Guidelines

A maximum of five TACACS servers are supported.

The following list shows non-configurable default settings:

```
DefaultPort = 49
DefaultTimeout = 5
DefaultRetries = 3
Protocol = "CHAP"
```

Use the `no` form of the command to remove the configuration.

Examples

The following example configures a TACACS+ server with an encrypted key.

```
device# configure terminal
device(config)# tacacs-server host 10.24.15.201
device(config-tacacs-config)# encrypted-key QjQkJLQUF3ncI1ooQCOaoEsBn5epVI3GsQwFD6i_BW
device# show running-config tacacs-server
tacacs-server host 10.2.3.5
   key zgR4B-sop6rYJdrp5zmg3zDKx_N-LKQF8ubf4OWuYGo
```

The following example shows the tacacs-server host being set as well as a plain-key.

```
device# configure terminal
device(config)# tacacs-server host 10.24.15.201
device(config-tacacs-config)# plain-key testKey
```

The following example shows information about configured TACAC+ servers.

```
device# show running tacacs-server
tacacs-server host 1.2.3.4
   encrypted-key JMeYDVdBN4Vb-wx35d7HnXIE8BL9KLUcEcePFwMNGoo
tacacs-server host 10.20.73.134
   encrypted-key QjQkJLQUF3ncI1ooQCOaoEsBn5epVI3GsQwFD6i_BWw
tacacs-server host 10.24.15.200
   encrypted-key  aimBmdAKcaduyaPNfE68IiWGEYOMywtFxVv8Ftu5bqc
```

The following example removes the encrypted key from the server.

```
device(config)# tacacs-server host 10.24.15.201
device(config-tacacs-config)# no encrypted-key
```

terminal

Configures screen length and timeout settings for a terminal.

Syntax

terminal [**length** *lines* | **no length** | **timeout** *seconds* | **no timeout**]

Parameters

length *lines*

Specifies the number of lines on the screen.

no length

Resets the length to the default value of 24 lines.

timeout *seconds*

Specifies the number of seconds that the CLI waits for input before timing out.

no timeout

Sets the timeout to the default value.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following examples show how to set the timeout and length parameters.

```
device# terminal timeout 2148
device# terminal length 512
```

traceroute

Sends ICMP echo requests with increasing TTL value to the specified IP.

Syntax

traceroute [[**IPADDR** | **NAME**] | [**ipv6** [**IPADDR** | **NAME**]] [**max-ttl** *1-255* | **min-ttl** *1-255* | **timeout** *1-60*]

Parameters

IPADDR

Specifies the destination IPV4 or IPV6 address.

NAME

Specifies the destination host name.

max-ttl *1-255*

Specifies the maximum TTL, number of hops. Valid range is 1-255, default is 30.

min-ttl *1-255*

Specifies the minimum TTL, number of hops. Valid range is 1-255, default is 1.

timeout *1-60*

Specifies the timeout value in seconds. The range 1-60, default is 5 seconds.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

This command is also supported on gNOI.

Examples

The following example sends ICMP echo requests.

```
device# traceroute 172.217.165.132

traceroute to 172.217.165.132 (172.217.165.132), 30 hops max, 60 byte packets
1 host.internal (10.42.0.1) 0.053 ms 0.020 ms 0.018 ms
2 10.20.73.129 (10.20.73.129) 0.330 ms 0.458 ms 0.478 ms
3 10.22.3.6 (10.22.3.6) 0.897 ms 1.675 ms 1.751 ms
4 10.22.3.17 (10.22.3.17) 0.950 ms 1.752 ms 1.746 ms
5 10.22.3.13 (10.22.3.13) 8.126 ms 8.143 ms 8.199 ms
6 10.254.127.58 (10.254.127.58) 3.409 ms 0.499 ms 0.578 ms
7 134.141.55.25 (134.141.55.25) 0.497 ms 0.552 ms 0.542 ms
8 208.185.247.161.IPYX-150368-ZYO.zip.zayo.com (208.185.247.161) 1.078 ms 1.228 ms 1.009
ms
9 100.ge-11-3-4.mpr3.sjc7.us.zip.zayo.com.zip.zayo.com (208.185.247.73) 0.673 ms 0.663
ms 0.656 ms
```

```
10 ae16.cr1.sjc2.us.zip.zayo.com (64.125.31.12) 4.104 ms 4.126 ms 4.237 ms
11 ae27.cs1.sjc2.us.eth.zayo.com (64.125.30.230) 3.512 ms 3.487 ms 5.108 ms
12 * * *
13 142.250.160.46 (142.250.160.46) 2.449 ms 2.440 ms 2.451 ms
14 209.85.243.50 (209.85.243.50) 2.209 ms 2.188 ms 2.180 ms
15 108.170.242.83 (108.170.242.83) 2.827 ms 2.846 ms 2.935 ms
16 142.250.234.137 (142.250.234.137) 2.722 ms 2.865 ms 2.858 ms
17 142.250.237.172 (142.250.237.172) 9.852 ms 9.826 ms 9.870 ms
18 * 142.250.235.172 (142.250.235.172) 51.634 ms *
19 * * *
20 216.239.57.137 (216.239.57.137) 68.178 ms * *
21 108.170.226.122 (108.170.226.122) 67.973 ms 66.627 ms 66.614 ms
22 108.170.248.1 (108.170.248.1) 67.274 ms 67.365 ms 67.498 ms
23 142.250.224.245 (142.250.224.245) 67.081 ms 67.077 ms 67.100 ms
24 172.217.165.132 (172.217.165.132) 67.678 ms 66.427 ms 66.502 ms

device# traceroute -6 www.google.com

traceroute to www.google.com (2404:6800:4004:808::2004), 30 hops max, 80 byte packets
1 2001:2e8:665:0:2:2:0:1 (2001:2e8:665:0:2:2:0:1) 0.100 ms 0.052 ms 0.066 ms
2 2001:2e8:22:204::2 (2001:2e8:22:204::2) 1.123 ms 1.082 ms 1.089 ms
3 2001:2e8:20::22:11 (2001:2e8:20::22:11) 1.712 ms 1.603 ms 1.522 ms
4 2001:3e0:5001:12::1 (2001:3e0:5001:12::1) 6.361 ms 6.278 ms 6.386 ms
5 2001:7fa:7:1:0:1:5169:1 (2001:7fa:7:1:0:1:5169:1) 1.367 ms 1.346 ms 1.235 ms
6 2001:4860:0:1002::1 (2001:4860:0:1002::1) 1.675 ms * *
7 * * *
8 nrt20s08-in-x04.1e100.net (2404:6800:4004:808::2004) 1.718 ms 1.602 ms 1.553 ms
```

traffic-type gre

Configures or removes the gre header type to be matched for traffic classification.

Syntax

traffic-type gre ip [*A.B.C.D* | *X:X::X:X* | *any*]

traffic-type gre mode [**decap** | **new-scope**]

no traffic-type gre [**ip** | **mode**]

Parameters

gre

Specifies the gre header to be matched for classifying the packet.

ip

Specifies the IP address for matching packets.

A.B.C.D

Specifies the IPv4 address.

X:X::X:X

Specifies the IPv6 address.

any

Specifies any source IP address.

mode

Specifies the actions for matching packets.

decap

Removes the encapsulated header.

new-scope

Shifts the scope of headers to inner headers for further processing.

Modes

Ingress-group config mode

Usage Guidelines

Validations for the command are as follows:

- This command is available only to users with the admin role.
- Valid decapsulation type and corresponding ID must be provided.
- Only one traffic type per ingress group is allowed.
- The configured traffic type must be removed before you configure a new traffic type.
- Both IPv4 and IPv6 addresses are supported.

- Valid IP addresses must be provided. The following IP addresses are not valid:
  - Unspecified IPv4 address (0.0.0.0)
  - Broadcast IPv4 address (255.255.255.255)
  - Unspecified IPv6 address (“::”)
  - Broadcast IPv6 address (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff)
- Existing traffic type cannot be configured again with a different ID, IP, or scope.
- The mode of the existing traffic type can be deleted, but cannot be modified. The existing mode must be removed and reconfigured with the new mode.
- The overlapping IP combination between different ingress-group traffic-type is not allowed.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- The `no` form of the command removes both traffic type and mode even if the mode is not specified.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following examples configure the `gre` traffic type with `decap` and `new-scope` modes.

```
device(config)# ingress-group ing-1
device(config-ingress-group)# traffic-type gre mode decap
device(config-ingress-group)# end

device# show running-config ingress-group ing-1
ingress-group ing-1
traffic-type gre mode decap

Show running:
device# show running-configuration ingress-group ing-1
ingress-group ing-1
traffic-type mode new-scope
```

traffic-type gtpu

Configures or removes the gtpu header type to be matched for traffic classification.

Syntax

traffic-type gtpu ip [*A.B.C.D* | *X:X::X:X* | *any*]

traffic-type gtpu mode [**decap** | **new-scope**]

traffic-type gtpu teid *teid-value*

no traffic-type [**ip** | **mode** | **teid**]

Parameters

gtpu

Specifies the gtpu header to be matched for classifying the packet.

ip

Specifies the actions for matching packets.

A.B.C.D

Specifies the IPv4 address.

X:X::X:X

Specifies the IPv6 address.

any

Specifies any source IP address.

mode

Specifies the actions for matching packets.

decap

Removes the encapsulated header.

new-scope

Shifts the scope of headers to inner headers for further processing.

teid *teid-value*

Specifies the teid value. Valid TEID range is 1-4294967295.

Modes

Ingress-group config mode

Usage Guidelines

Validations for the command are as follows:

- This command is available only to users with the admin role.
- Valid decapsulation type and corresponding ID must be provided.
- Only one traffic type per ingress group is allowed.

- The configured traffic type must be removed before you configure a new traffic type.
- Both IPv4 and IPv6 addresses are supported.
- Valid IP addresses must be provided. The following IP addresses are not valid:
  - Unspecified IPv4 address (0.0.0.0)
  - Broadcast IPv4 address (255.255.255.255)
  - Unspecified IPv6 address (“::”)
  - Broadcast IPv6 address (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff)
- Existing traffic type cannot be configured again with a different ID or scope.
- The mode of the existing traffic type can be deleted, but cannot be modified. The existing mode must be removed and reconfigured with the new mode.
- The overlapping IP combination between different ingress-group traffic-type is not allowed.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- The `no` form of the command removes both traffic type and mode even if the mode is not specified.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures the `gtpu` traffic type with `decap` mode.

```
device(config-ingress-group)# traffic-type gtpu teid 3000 mode decap
device(config-ingress-group)# end

device# show running-config ingress-group ing
ingress-group ing
  traffic-type gtpu teid 3000
  traffic-type gtpu ip any any

device# conf t
device(config)# ingress-group ing
device(config-ingress-group)# no traffic-type gtpu teid
device(config-ingress-group)# traffic-type gtpu teid 5000 mode decap

show ingress-group ing

            Name : ing
             Route-Map : -
           Description : -
            Interfaces : none
          Traffic-Type : GTPU
             Tunnel-Id : 5000
                  Mode : decap
   Destination-ip-addr : any
        Source-ip-addr : any

device# show running-config ingress-group

ingress-group ing
  traffic-type gtpu teid 5000 mode decap
  traffic-type gtpu ip any any
```

```
device# conf t
device(config)# ingress-group ing
device(config-ingress-group)# no traffic-type gtpu teid
device(config-ingress-group)# end
device# show running-config ingress-group

ingress-group ing
  traffic-type gtpu mode decap
  traffic-type gtpu ip any any
```

traffic-type ipip

Configures the ipip header type to be matched for traffic classification.

Syntax

traffic-type ipip ip [*A.B.C.D* | *X:X::X:X* | *any*]

traffic-type ipip mode [**decap** | **new-scope**]

no traffic-type ipip [**ip** | **mode**]

Parameters

ipip

Specifies the ipip header to be matched for classifying the packet.

ip

Specifies the actions for matching packets.

A.B.C.D

Specifies the IPv4 address.

X:X::X:X

Specifies the IPv6 address.

any

Specifies any source IP address.

mode

Specifies the actions for matching packets.

decap

Removes the encapsulated header.

new-scope

Shifts the scope of headers to inner headers for further processing.

Modes

Ingress-group config mode

Usage Guidelines

Validations for the command are as follows:

- This command is available only to users with the admin role.
- Valid decapsulation type and corresponding ID must be provided.
- Only one traffic type per ingress group is allowed.
- The configured traffic type must be removed before you configure a new traffic type.
- Both IPv4 and IPv6 addresses are supported.

- Valid IP addresses must be provided. The following IP addresses are not valid:
  - Unspecified IPv4 address (0.0.0.0)
  - Broadcast IPv4 address (255.255.255.255)
  - Unspecified IPv6 address (“::”)
  - Broadcast IPv6 address (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff)
- Existing traffic type cannot be configured again with a different ID, IP, or scope.
- The overlapping IP combination between different ingress-group traffic-type is not allowed.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- The `no` form of the command removes both traffic type and mode even if the mode is not specified.

Examples

The following examples configures the `ipip` traffic type.

```
device(config-ingress-group)# traffic-type ipip ip 192.168.2.1 255.255.255.0 192.168.3.2
255.255.255.0

device# show ingress-group ing

    Name : ing
             Route-Map : -
           Description : -
            Interfaces : none
          Traffic-Type : IPIP
             Tunnel-Id : any
                  Mode : none
   Destination-ip-addr : 192.168.3.2
   Destination-ip-mask : 255.255.255.0
        Source-ip-addr : 192.168.2.1
        Source-ip-mask : 255.255.255.0
```

traffic-type mpls

Filters Multiprotocol Label Switching Segment Routing (MPLS-SR) packets.

Syntax

traffic-type mpls outer header1 [*label value* | *any*]

traffic-type mpls outer log

traffic-type mpls outer log_drop

traffic-type mpls outer mirror *NAME*

no traffic-type mpls outer [**header1** | **log** | **log_drop** | **mirror**]

Parameters

mpls outer

Specifies that the MPLS-SR is the outer encapsulation type to be matched to classify packet. MPLS can be the outer encapsulation or the only encapsulation.

header1

Configures the MPLS Bottom of Stack header (inner-most header) values to be matched.

label1

Specifies the label value of the MPLS Bottom of Stack to be matched. Valid range is 0 through 1048575.

any

Matches all values of the specified parameter.

log

Captures the packet matching traffic type.

log_drop

Captures the packet matching traffic type and drop.

mirror

Configures the mirror.

NAME

Specifies the name of the configured mirror. Supports 64 characters.

Modes

Ingress-group config mode

Usage Guidelines

This command is available only to users with the admin role.

This command classifies MPLS-SR packets by removing all MPLS headers and sending payload to the tools. You can use the ingress or egress ACLs to match packets based on the payload fields.

The packets can also be classified based on the Bottom of Stack (inner-most header) MPLS header values.

Removal of MPLS headers is supported for maximum depth of four MPLS labels.

Validations for the command are as follows:

- A maximum of four MPLS labels are supported.
- The configured MPLS header values must be removed before you configure a new header value.
- When MPLS header values are not set, all values in innermost header are classified.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.

Examples

The following example enables classification of packets based on MPLS headers.

```
device(config-ingress-group)# traffic-type mpls outer header1 12345 3 250

device(config-ingress-group)# do show ingress-group all

Number of ingress-groups: 1
  Name : igg1
     Route-Map : rmap1
    Description : -
     Interfaces : ethernet 0/1

  Outer Tunnel Config :
    Traffic-Type : MPLS
  Header1 (Bottom of Stack header):
        label : 12345
    Traffic Class : 3
    Time to Live : 250
       Mirror : none
```

traffic-type nvgre

Configures or removes the nvgre header type to be matched for traffic classification.

Syntax

traffic-type nvgre ip [*A.B.C.D* | *X:X::X:X* | *any*]

traffic-type nvgre mode [**decap** | **new-scope**]

traffic-type nvgre vsid *vsid value*

no traffic-type nvgre [**ip** | **mode** | **vsid**]

Parameters

nvgre

Specifies the nvgre header to be matched for classifying the packet.

ip

Specifies the actions for matching packets.
A.B.C.D

Specifies the IPv4 address.

X:X::X:X

Specifies the IPv6 address.

any

Specifies any source IP address.

mode

Specifies the actions for matching packets.
decap

Removes the encapsulated header.

new-scope

Shifts the scope of headers to inner headers for further processing.

vsid *vsid value*

Valid VSID range is 4096-16777214. The VSID range 1-4095 and VSID value 16777215 are reserved and not configurable.

Modes

Ingress-group config mode

Usage Guidelines

Validations for the command are as follows:

- This command is available only to users with the admin role.
- Valid decapsulation type and corresponding ID must be provided.

- Only one traffic type per ingress group is allowed.
- The configured traffic type must be removed before you configure a new traffic type.
- Both IPv4 and IPv6 addresses are supported.
- Valid IP addresses must be provided. The following IP addresses are not valid:
  - Unspecified IPv4 address (0.0.0.0)
  - Broadcast IPv4 address (255.255.255.255)
  - Unspecified IPv6 address ("::")
  - Broadcast IPv6 address (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff)
- Existing traffic type cannot be configured again with a different ID or scope.
- The mode of the existing traffic type can be deleted, but cannot be modified. The existing mode must be removed and reconfigured with the new mode.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- The `no` form of the command removes both traffic type and mode even if the mode is not specified.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures `nvgre` traffic type with `decap` mode.

```
device(config-ingress-group)# traffic-type nvgre vsid 7000 mode decap
device(config-ingress-group)# end

device# show running-config ingress-group ing

ingress-group ing
               Name : ing
          Route-Map : -
        Description : -
         Interfaces : none
       Traffic-Type : NVGRE
          Tunnel-Id : 7000
               Mode : decap
 Destination-ip-addr : any
      Source-ip-addr : any

device# show running-config ingress-group

ingress-group ing
  traffic-type nvgre vsid 7000 mode decap
  traffic-type nvgre ip any any

device# conf t
device(config)# ingress-group ing
device(config-ingress-group)# no traffic-type nvgre mode
device(config-ingress-group)# end

device# show running-config ingress-group

ingress-group ing
  traffic-type nvgre vsid 7000
  traffic-type nvgre ip any any
```

traffic-type vxlan

Configures the VXLAN outermost header with the IP address in double encapsulation traffic.

Syntax

traffic-type vxlan ip [*A.B.C.D* | *X:X::X:X* | *any*]

traffic-type vxlan mode [**decap** | **new-scope**]

traffic-type vxlan vni *vni-value*

traffic-type vxlan outer { [**ip** [*A.B.C.D* | *X:X::X:X* | *any*]] | **log** | **log_drop** | [**mirror** *NAME*] | [**vni** *vni value*] }

no traffic-type vxlan [**ip** | **mode** | **vni** *vni-value*]

Parameters

vxlan

Specifies the VXLAN outermost header to be matched to classify packet in double encapsulated packet.

ip

Specifies the IP address for matching packets.

A.B.C.D

Specifies the IPv4 address.

X:X::X:X

Specifies the IPv6 address.

any

Specifies any source IP address.

mode

Specifies the actions for matching packets.

decap

Removes the encapsulated header.

new-scope

Shifts the scope of headers to inner headers for further processing.

outer

Specifies the VXLAN outer header.

log

Captures the packet matching traffic type.

log_drop

Captures the packet matching traffic type and drop.

mirror *NAME*

Configures the mirror. Supports 64 characters.

vni *vni value*

Specifies the vni value. The valid range is 1-16777215.

Modes

Ingress-group config mode

Usage Guidelines

This command is available only to users with the admin role.

This command enables mirroring in double encapsulation traffic with VXLAN as outermost header or traffic with MPLS outer encapsulation type. Successfully classified traffic is mirrored to the configured front-panel interface.

Only the VXLAN tunnel is supported for outer config.

Valid IP addresses must be provided. The following IP addresses are not valid:

- Unspecified IPv4 address (0.0.0.0)
- Broadcast IPv4 address (255.255.255.255)
- Unspecified IPv6 address (“::”)
- Broadcast IPv6 address (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff)

IPv6 is not supported for the VXLAN outer configuration.

The overlapping IP combination between different ingress-group traffic-type is not allowed.

If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.

The **no** keyword can remove only the IP configuration.

Examples

The following example configures the VXLAN outermost header.

```
device(config-ingress-group)#
traffic-type vxlan outer ip 192.168.4.2 255.255.255.0 192.168.5.2 255.255.255.0

device# show ingress-group ing

    Name : ing
              Route-Map : -
             Description : -
              Interfaces : none
            Traffic-Type : GTPU
               Tunnel-Id : any
                    Mode : none
   Destination-ip-addr : 192.168.3.2
   Destination-ip-mask : 255.255.255.0
        Source-ip-addr : 192.168.2.1
        Source-ip-mask : 255.255.255.0
```

```
Outer Tunnel Config :
       Traffic-Type : VxLAN
          Tunnel-Id : any
Destination-ip-addr : 192.168.5.2
Destination-ip-mask : 255.255.255.0
     Source-ip-addr : 192.168.4.2
     Source-ip-mask : 255.255.255.0
             Mirror : none
```

transport-tunnel

Creates a new transport tunnel.

Syntax

transport-tunnel *tunnel-name*

no transport-tunnel *tunnel-name*

Parameters

tunnel-name

Specifies the name of the transport tunnel. Supports 64 characters.

The name must start with an alphabet character or an underscore character, followed by alphanumeric characters or special characters (underscores, hyphens, or periods).

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

The following reserved keywords cannot be used as name identifiers: `all`, `ingress-group`, `egress`, `egress-group`, `match`, `list`, `access-list`, `route-map`, and `listener-policy`.

The transport tunnel name cannot be same as the ingress group that is associated with the transport tunnel.

If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

The attached route-map must be a member of at least one interface, LAG, or transport tunnel. Remove the route map from ingress group or attach the ingress group to another interface, LAG, or transport tunnel before removing it from the tunnel.

Examples

The following example configures transport tunnel.

```
device(config)# transport-tunnel tt1
device(config-tranport-tunnel)#

Show running:
device# show running-config transport-tunnel tt1
transport-tunnel tt1
```

truncate

Truncates received packets to the configured length for the current route map or listener policy.

Syntax

truncate *length*

no truncate

Parameters

length

Specifies the truncated length of received packets. The valid range is 64 to 9000.

Modes

Route-map config mode

Listener-policy config mode

Route-map config mode

Examples

The following example configures received packets to a length of 100 for the current route map and uses the show command to verify configuration.

```
device# configure terminal
device(config)# route-map mall2
device(config-route-map)# truncate 100
device(config-route-map)# end

device# show route-map mall2
route-map mall2 45
forward-action permit
truncate 100
Policy matches: 0 packets, 0 bytes, 0 Packets/secRate, 0 Bits/secRate
```

The following example configures received packets to a length of 63 for the listener policy.

```
device# configure terminal
device(config)# listener-policy lp1 <sId>
device(config-listener-policy)#  truncate 63
```

The following example deletes configured truncation for received packets for the current route map.

```
device(config)# route-map mall2
device(config-route-map)# no truncate
```

tunnel-type ipv4

Configures the source IPv4 address with mask and tunnel-type for the transport tunnel packets to be terminated.

Syntax

tunnel-type [**gre** | **erspan**] [**ipv4-src** *ipaddr mask*]

no tunnel-type [**gre** | **erspan**] [**ipv4-src** *ipaddr mask*]

Parameters

gre | **erspan**

Specifies the type of tunnel to be terminated.

ipv4-src *ipaddr mask*

Specifies the source IPv4 address and mask configured in dotted decimal notation. Example: 196.168.0.1.

Modes

Transport tunnel config mode

Usage Guidelines

This command is available only to users with the admin role.

If all the parameters match along with the chassis MAC, the transport header is removed and packets are subjected to further processing.

If the IP address is not provided, all packets matching the tunnel type or transport header type are configured for termination.

Validations for the command are as follows:

- Valid tunnel type must be provided.
- Valid IP address and mask must be provided.
- Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.
- Only one tunnel type per transport tunnel is allowed. The configured tunnel type must be removed before you configure a new tunnel type.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following examples configure the transport tunnel:

```
device(config-transport-tunnel)# tunnel-type erspan ipv4-src 192.168.2.10 255.255.0.0

device(config-transport-tunnel)# tunnel-type gre ipv4-src 10.10.2.3 255.255.255.0

device# show running-config transport-tunnel tt1
transport-tunnel tt1
  tunnel-type gre ipv4-src 10.10.2.3 255.255.255.0
```

tunnel-type ipv6

Configures the source IPv6 address with mask and tunnel type for the transport tunnel packets to be terminated.

Syntax

tunnel-type gre [**ipv6-src** *ipaddr mask*]

no tunnel-type gre [**ipv6-src** *ipaddr mask*]

Parameters

gre

Specifies the type of tunnel to be terminated.

ipv6-src *ipaddr mask*

Specifies the source IPv6 address and mask configured in hexadecimal between 0 and FFFF. Example: 202:304:606:708:90a:b0c:d0e:f11.

The upper 4 bytes and lower 8 bytes of the mask must be zero because only 32 bits out of 128 bits of IPv6 are supported. Example: 0000:0000:FFFF:FFFF:0000:0000:0000:0000.

Modes

Transport tunnel config mode

Usage Guidelines

This command is available only to users with the admin role.

If all the parameters match along with the chassis MAC, the transport header is removed and packets are subjected to further processing.

If the IP address is not provided, all packets matching the tunnel type or transport header type are configured for termination.

Validations for the command are as follows:

- Tunnel type must be GRE.
- Valid IP address and mask must be provided.
- Only valid unicast IP addresses are supported. Multicast IP addresses are not supported.
- Only one tunnel type per transport tunnel is allowed. The configured tunnel type must be removed before you configure a new tunnel type.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures the transport tunnel.

```
device(config-transport-tunnel)# tunnel-type gre ipv6-src
2233:304:606:708:90a:b0c:d0e:f11

device(config)# show transport-tunnel tt1

                  Name : tt1
      Source-Ipv6-Addr : 2233:304:606:708:90a:b0c:d0e:f11
      Source-Ipv6-Mask : 0000:0000:FFFF:FFFF:0000:0000:0000:000
           Tunnel-Type : GRE
         Ingress-Group : none

device# show running-config transport-tunnel
transport-tunnel tt1
  tunnel-type gre ipv6-src 2233:304:606:708:90a:b0c:d0e:f11
0000:0000:FFFF:FFFF:0000:0000:0000:000
```

usb enable

Enables access to the USB.

Syntax

usb enable

no usb enable

Parameters

enable

Enables access to the USB. USB access is disabled by default.

Modes

Exec mode

Usage Guidelines

This command is available only to users with the admin role.

USB access is disabled after firmware upgrade, downgrade, or reboot.

The `no` form of the command disables access to the USB storage device.

Examples

The following example enables access to the USB.

```
device# usb enable
```

username

Configures user along with role for local authentication.

Syntax

username *username* **role** *role* **password** *password* [**encryption-level** *0* | *10*]

no username *username*

Parameters

username

Specifies the user name. The username supports 1-32 characters. Characters allowed are alpha-numeric, underscore, and dot. Underscore is not allowed as the first character.

role

Specifies the predefined role to be assigned to the user. The supported roles are admin and user.

The role supports 1-32 characters. Characters allowed are alpha-numeric, underscore and dot. Underscore is not allowed as the first character.

password

Specifies the password of the user. Supported length of the plain text password is 8-40 and 8-128 for hashed passwords.

encryption-level *0* | *10*

Specifies whether the password input is encrypted. The values 0 and 10 indicate clear-text and encryption. The default value is 0.

Modes

Config mode

Usage Guidelines

This command is available only to users with the admin role.

Examples

The following example configures users with admin and user roles.

```
device# configure terminal
device(config)# username testuser1 role admin password password123 encryption-level 0
device(config)# username testuser2 role user password
$6$salt$cevuzTZ/QBjzuZG0/ebEeedmcTnhyM8ITUu8K032Cp2XvIibq7voqYagm18bwpLBqrg
/1/16YxTmKKibJz5r10 encryption-level 10

device# show running-config username
username testuser1 role admin password
```

```
$6$salt$cevuzTZ/QBjzuZG0/ebEeedmcTnhyM8ITUu8K032Cp2XvIibq7voqYagm18bwpLBqrg
/l/l6YxTmKKibJz5r10 encryption-level 10
username testuser2 role user password
$6$salt$cevuzTZ/QBjzuZG0/ebEeedmcTnhyM8ITUu8K032Cp2XvIibq7voqYagm18bwpLBqrg
/l/l6YxTmKKibJz5r10 encryption-level 10
```

vlan

Configures forwarding actions by VLAN ID to be performed on outgoing packets.

Syntax

vlan *vlan-id*

no vlan *vlan-id*

Parameters

vlan-id

Specifies the VLAN ID to be configured. Valid range is 1 through 4095.

Modes

Listener-policy config mode

Usage Guidelines

Action is determined by forward-action setting in the listener policy.

- If the **forward-action** is set to deny, packets are dropped.
- If the **forward-action** is set to permit, the VLAN ID is changed to the configured value for permitted packets.
- Valid VLAN ID must be provided.
- VLAN ID must be unique per listener policy.

Examples

The following example configures the VLAN ID for listener policy, and then uses the show command to verify the configuration.

```
device# configure terminal
device(config)# listener-policy lp1 12
device(config-listener-policy)# vlan 500
device(config-listener-policy)# end
device#

device# show listener-policy lpl 12
forward-action permit
match ip access-list test_2 (active)
truncate 512
strip vn-tag
vlan 500
Policy matches: 0  packets, 0  bytes, 0 Packets/sec, 0 Bits/sec
```

The following example removes the VLAN ID configuration from the listener policy, and then uses the show command to verify the VLAN ID is removed from the configuration.

```
device# configure terminal
device(config)# listener-policy lp1 12
```

```
device(config-listener-policy)# no vlan
device(config-listener-policy)# end
device#

device# show listener-policy lpl 12
forward-action permit
match ip access-list test_2 (active)
truncate 512
strip vn-tag
Policy matches: 0  packets, 0  bytes, 0 Packets/sec, 0 Bits/sec
```

vlan-id

Configures VLAN ID for encapsulation of outgoing packets.

Syntax

vlan-id *vlan-id-value*

no vlan-id *vlan-id-value*

Parameters

vlan-id

Specifies the VLAN ID to be configured. Valid range is 1 through 4096.

Modes

Encap config mode

Usage Guidelines

Validations for the command are as follows:

- Valid VLAN ID must be provided.
- Single VLAN ID per encapsulation is allowed. Already configured VLAN ID must be removed before configuring a new VLAN ID.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures the VLAN ID.

```
device(config-encap-1)# vlan-id 1234
device(config-encap-1)#

device# show running-configuration
encap encap-1
vlan-id 1234
```

vlan-pcp

Configures VLAN priority (PCP) value for encapsulation of outgoing packets.

Syntax

vlan-pcp *vlan-pcp-value*

no vlan-pcp *vlan-pcp-value*

Parameters

vlan-pcp *vlan-pcp-value*

Specifies the VLAN PCP value. Valid values are 0 through 7.

Modes

Encap config mode

Usage Guidelines

Validations for the command are as follows:

- This command is optional.
- When this parameter is not configured, the outgoing packet does not contain a VLAN header.
- If this command is enabled without configuring vlan-id, the outgoing packet will not contain the VLAN header.
- Valid VLAN PCP value must be provided.
- If another VLAN PCP is already configured, it must be removed before configuring a new VLAN PCP.
- If the same command is run more than once, the second and subsequent instances are ignored and no error is reported.
- If the `no` form of the command is run without the configuration, the command is ignored and no error is reported.

Examples

The following example configures vlan-pcp and verifies the configuration with the show command.

```
device# configure terminal
device(config)# encap encap-1
device#(config-encap)# vlan-id 4000
device(config-encap)# vlan-pcp 2
device(config-encap)# end

device# show running-config encap encap-1
encap encap-1
```

```
vlan-id 4000
vlan-pcp 2
```