Junos® OS for EX Series Ethernet Switches

Device Security for EX Series Switches

Release
14.1X53

Published: 2014-12-18

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS for EX Series Ethernet Switches Device Security for EX Series Switches
Release 14.1X53

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- EX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page ix defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page ix defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**

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

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/

- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Security Features Overview

Security Features for EX Series Switches Overview

Juniper Networks Junos operating system (Junos OS) is a network operating system that has been hardened through the separation of control forwarding and services planes, with each function running in protected memory. The control-plane CPU is protected by rate limiting, routing policy, and firewall filters to ensure switch uptime even under severe attack. Access port security features such as dynamic Address Resolution Protocol (ARP) inspection, DHCP snooping, and MAC limiting are controlled through a single Junos OS CLI command.

Juniper Networks EX Series Ethernet Switches provide the following hardware and software security features:

Console Port—Allows use of the console port to connect to the Routing Engine through an RJ-45 cable. You then use the command-line interface (CLI) to configure the switch.

Out-of-Band Management—A dedicated management Ethernet port on the rear panel allows out-of-band management.

Software Images—All Junos OS images are signed by Juniper Networks certificate authority (CA) with public key infrastructure (PKI).

User Authentication, Authorization, and Accounting (AAA)—Features include:

- User and group accounts with password encryption and authentication.
- Access privilege levels configurable for login classes and user templates.
- RADIUS authentication, TACACS+ authentication, or both, for authenticating users who attempt to access the switch.
- Auditing of configuration changes through system logging or RADIUS/TACACS+.

802.1X Authentication—Provides network access control. Supplicants (hosts) are authenticated when they initially connect to a LAN. Authenticating supplicants before they receive an IP address from a DHCP server prevents unauthorized supplicants from gaining access to the LAN. EX Series switches support Extensible Authentication Protocol (EAP) methods, including EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.

Port Security—Access port security features include:

- DHCP snooping—Filters and blocks ingress DHCP server messages on untrusted ports; builds and maintains an IP-address/MAC-address binding database (called the DHCP snooping database).
- Dynamic ARP inspection (DAI)—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons.
- MAC limiting—Protects against flooding of the Ethernet switching table.
- MAC move limiting—Detects MAC movement and MAC spoofing on access ports.
- Trusted DHCP server—With a DHCP server on a trusted port, protects against rogue DHCP servers sending leases.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. The source IP address in the packet sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is allowed for further processing if the source IP address to source MAC address binding is valid; if the binding is not valid, the packet is discarded.
- DHCP option 82—Also known as the DHCP relay agent information option. Helps protect the EX Series switch against attacks such as spoofing (forging) of IP addresses and MAC addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.
- Unrestricted proxy ARP—The switch responds to all ARP messages with its own MAC address. Hosts that are connected to the switch's interfaces cannot communicate directly with other hosts. Instead, all communications between hosts go through the switch.
- Restricted proxy ARP—The switch does not respond to an ARP request if the physical networks of the source and target of the ARP request are the same. It does not matter whether the destination host has the same IP address as the incoming interface or a different (remote) IP address. An ARP request for a broadcast address elicits no reply.

Device Security—Storm control permits the switch to monitor unknown unicast and broadcast traffic and drop packets, or shut down, or temporarily disable the interface when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. You can enable storm control on access interfaces or trunk interfaces.

Firewall Filters—Allow auditing of various types of security violations, including attempts to access the switch from unauthorized locations. Firewall filters can detect such attempts and create audit log entries when they occur. The filters can also restrict access by limiting traffic to source and destination MAC addresses, specific protocols, or, in combination with policers, to specified data rates to prevent denial of service (DoS) attacks.

Policers—Provide rate-limiting capability to control the amount of traffic that enters an interface, which acts to counter DoS attacks.

Encryption Standards—Supported standards include:

- 128-, 192-, and 256-bit Advanced Encryption Standard (AES)
- 56-bit Data Encryption Standard (DES) and 168-bit 3DES

Related Documentation

- *802.1X for EX Series Switches Overview*
- *Firewall Filters for EX Series Switches Overview*
- *Understanding Port Security*
- *Understanding Proxy ARP on EX Series Switches*
- Understanding Storm Control on EX Series Switches on page 7
- *Understanding the Use of Policers in Firewall Filters*
- *Understanding Centralized Network Access Control and EX Series Switches*

CHAPTER 2

Storm Control Overview

Understanding Storm Control on EX Series Switches

A traffic storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect. The LAN is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service. Storm control enables the switch to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the *storm control level*—is exceeded, thus preventing packets from proliferating and degrading the LAN. As an alternative to having the switch drop packets, you can configure it to shut down interfaces or temporarily disable interfaces (see the action-shutdown statement or the port-error-disable statement) when the storm control level is exceeded.

The default configuration of storm control differs according to the switch line:

- On EX2200, EX3200, EX3300, EX4200, and EX6200 access ports—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control for broadcast and unknown unicast traffic on all switch interfaces, with the storm control level set to 80 percent of the available bandwidth used by the broadcast and unknown unicast traffic streams.
- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all switch interfaces, with the storm control level set to 80 percent of the combined broadcast, multicast, and unknown unicast traffic streams.

You can customize the configuration of storm control, as follows:

NOTE: You can customize the storm control level for a specific interface by explicitly configuring either bandwidth or level.

- bandwidth— Configures the storm control level as the bandwidth in kilobits per second of the applicable traffic streams on that interface.
- level—Configures the storm control level as a percentage of the available bandwidth used by the combined applicable traffic streams that are subject to storm control on that interface.

You cannot configure both bandwidth and level for the same interface.

- You can change the storm control level for a specific interface by configuring the bandwidth value or the storm control level for the combined traffic streams that are subject to storm control on that interface. The type of traffic stream (broadcast, unknown unicast, and multicast) that is included within the bandwidth or storm control level consideration depends on which types of traffic are enabled for storm control monitoring on that interface.
- You can enable storm control selectively for multicast traffic on a specific interface or on all interfaces.
- On all switches—You can disable storm control selectively for either broadcast streams, or multicast streams, or for unknown unicast streams.
- On EX8200 switches—You can also disable storm control selectively for either registered multicast traffic, or unregistered multicast traffic, or for both types of multicast traffic. Registered multicast MAC addresses are multicast MAC addresses that are within the range 01-00-5E-00-00-00 through 01-00-5E-7F-FF-FF. This range has been reserved by the Internet Assigned Numbers Association (IANA) for multicast Ethernet addresses. Multicast MAC addresses that are outside this range are called unregistered multicast addresses.

The sending and receiving of broadcast, multicast, and unicast packets are part of normal LAN operation, so to recognize a storm, you must be able to identify when traffic has reached a level that is abnormal for your LAN. Suspect a storm when operations begin timing out and network response times slow down. As more packets flood the LAN, network users might be unable to access servers or e-mail.

Monitor the level of broadcast, multicast, and unknown unicast traffic in the LAN when it is operating normally. Use this data as a benchmark to determine when traffic levels are too high. Then configure storm control to set the level at which you want to drop broadcast traffic, multicast traffic, unknown unicast traffic, or two or all three of those traffic types.

NOTE: When you configure storm control bandwidth or storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth or level. For example, if you configure a storm control bandwidth of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined traffic streams. Traffic might include broadcast, multicast, and unknown unicast traffic, depending upon the configuration.

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 20
- Disabling or Enabling Storm Control (CLI Procedure) on page 20

CHAPTER 3

Unknown Unicast Forwarding Overview

Understanding Unknown Unicast Forwarding

Unknown unicast traffic consists of unicast packets with unknown destination MAC addresses. By default, the switch floods these unicast packets that are traveling in a VLAN to all interfaces that are members of the VLAN. Forwarding this type of traffic can create unnecessary traffic that leads to poor network performance or even a complete loss of network service. This is known as a traffic storm.

To prevent a storm, you can disable the flooding of unknown unicast packets to all VLAN interfaces by configuring one VLAN or all VLANs to forward all unknown unicast traffic to a specific interface. This channels the unknown unicast traffic to a single interface.

Related Documentation

- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 19
- *Configuring Unknown Unicast Forwarding (CLI Procedure)*
- Understanding Storm Control on EX Series Switches on page 7
- *Understanding Storm Control on Switching Devices*
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*

PART 2

Configuration

CHAPTER 4

Configuration Examples

Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches

Storm control enables you to prevent network outages caused by broadcast storms on the LAN. You can configure storm control on an EX Series switch to rate-limit broadcast traffic, multicast traffic, and unknown unicast traffic at a specified level so that the switch drops packets when the specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN.

This example shows how to configure storm control on a single EX Series switch:

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 9.5 or later for EX Series switches

Overview and Topology

A storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect and resulting in a broadcast storm that can cause network outages.

You can use storm control to prevent broadcast storms by specifying the amount, also known as the *storm control level*, of broadcast traffic, multicast traffic, and unknown unicast traffic to be allowed on an interface. You specify the storm control level as the traffic rate in kilobits per second (Kbps) of the combined applicable traffic streams.

NOTE:

- On EX2200, EX3200, EX3300, and EX4200 switches—Storm control is not enabled for multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams.
- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.
- On EX6200 switches—Storm control is not enabled for multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. Storm control can be disabled for each type of traffic individually.

Storm control monitors the level of applicable incoming traffic and compares it with the level that you specify. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. As an alternative to having the switch drop packets, you can configure it to shut down interfaces or temporarily disable interfaces (see the action-shutdown statement or the port-error-disable statement) when the storm control level is exceeded.

The topology used in this example consists of one switch with 24 ports. The switch is connected to various network devices. This example shows how to configure the storm control level on interface ge-0/0/0 by setting the level to a traffic rate of 15,000 Kbps, based on the traffic rate of the combined applicable traffic streams. If the combined traffic exceeds this level, the switch drops packets for the controlled traffic types to prevent a network outage.

Configuration

CLI Quick Configuration

To quickly configure storm control based on the traffic rate in Kbps per second of the combined traffic streams, copy the following command and paste it into the switch terminal window:

```
[edit]
set ethernet-switching-options storm-control interface ge-0/0/0 bandwidth 15000
```

Step-by-Step Procedure

To configure storm control:

1. Specify the traffic rate in Kbps per second of the combined traffic streams on a specific interface:

   ```
   [edit ethernet-switching-options]
   user@switch# set storm-control interface ge-0/0/0 bandwidth 15000
   ```

Results

Display the results of the configuration:

```
[edit ethernet-switching-options]
```

```
user@switch> show storm-control
interface ge-0/0/0.0 {
  bandwidth 15000;
}
```

Verification

Verifying That the Storm Control Configuration Is in Effect

Purpose Confirm that storm control is limiting the rate of traffic on the interface.

Action Use the **show interfaces ge-0/0/0 detail** operational mode command to view traffic statistics on the storm controlled interface. The input rate (bps) must not exceed the storm control limit.

```
user@switch> show interfaces ge-0/0/0 extensive
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 160, SNMP ifIndex: 503, Generation: 163
  Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x0
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: b0:c6:9a:67:90:84, Hardware address: b0:c6:9a:67:90:84
  Last flapped   : 2013-05-16 22:46:42 UTC (14w3d 03:13 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :            312742788                 512 bps
   Output bytes  :            245552919                   0 bps
   Input  packets:              3550009                   1 pps
   Output packets:              2622101                   0 pps
   IPv6 transit statistics:
    Input  bytes  :                   0
    Output bytes  :                   0
    Input  packets:                   0
    Output packets:                   0
  Dropped traffic statistics due to STP State:
   Input  bytes  :                    0
   Output bytes  :                    0
   Input  packets:                    0
   Output packets:                    0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
    L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
    FIFO errors: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets:
    FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
  Egress queues: 8 supported, 4 in use
  Queue counters:       Queued packets  Transmitted packets      Dropped packets

    0 best-effort                    0                    1                    0

    1 assured-forw                   0                    0                    0
```

```
  5 expedited-fo                 0                    0                    0

  7 network-cont                 0              2622100                    0

Queue number:         Mapped forwarding classes
  0                   best-effort
  1                   assured-forwarding
  5                   expedited-forwarding
  7                   network-control
Active alarms  : None
Active defects : None
MAC statistics:                       Receive         Transmit
  Total octets                              0                0
  Total packets                             0                0
  Unicast packets                           0                0
  Broadcast packets                         0                0
  Multicast packets                         0                0
  CRC/Align errors                          0                0
  FIFO errors                               0                0
  MAC control frames                        0                0
  MAC pause frames                          0                0
  Oversized frames                          0
  Jabber frames                             0
  Fragment frames                           0
  VLAN tagged frames                        0
  Code violations                           0
Autonegotiation information:
  Negotiation status: Incomplete
Packet Forwarding Engine configuration:
  Destination slot: 0
Interface transmit statistics: Disabled
```

Meaning The **Input bytes** field shows the ingress traffic rate in bytes per second (bps). The input rate is within the storm control limit of 15,000 Kbps.

Related Documentation

- Disabling or Enabling Storm Control (CLI Procedure) on page 20
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 20
- Understanding Storm Control on EX Series Switches on page 7

CHAPTER 5

Configuration Tasks

Configuring Unknown Unicast Forwarding (CLI Procedure)

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets to all interfaces associated with a VLAN. Forwarding such traffic to interfaces on the switch can create a security issue.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN out to a specific trunk interface. From there, the destination MAC address can be learned and added to the Ethernet switching table. You can configure each VLAN to divert unknown unicast traffic to different trunk interfaces or use one trunk interface for multiple VLANs.

To configure unknown unicast forwarding options:

NOTE: **Before you can configure unknown unicast forwarding within a VLAN, you must first configure that VLAN.**

1. Configure unknown unicast forwarding for a specific VLAN (here, the VLAN name is **employee**):

   ```
   [edit ethernet-switching-options]
   user@switch# set unknown-unicast-forwarding vlan employee
   ```

2. Specify the trunk interface to which all unknown unicast traffic will be forwarded:

   ```
   [edit ethernet-switching-options]
   user@switch# set unknown-unicast-forwarding vlan employee interface ge-0/0/3.0
   ```

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 53
- Understanding Unknown Unicast Forwarding on page 11

- Understanding Storm Control on EX Series Switches on page 7

Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)

An Ethernet switching access interface on an EX Series switch might shut down or be disabled as a result of one of the following port-security or storm-control configurations:

- MAC limiting—**mac-limit** statement is configured with action **shutdown**.
- MAC move limiting—**mac-move-limit** statement is configured with action **shutdown**.
- Storm control—**storm-control** statement is configured with the action **shutdown**.

You can configure the switch to automatically restore the disabled interfaces to service after a specified period of time. Autorecovery applies to all the interfaces that have been disabled due to MAC limiting, MAC move limiting, or storm control errors.

NOTE: You must specify the disable timeout value for the interfaces to recover automatically. There is no default disable timeout. If you do not specify a timeout value, you need to use the clear ethernet-switching port-error command to clear the errors and restore the interfaces or the specified interface to service.

To configure autorecovery from the disabled state due to MAC limiting, MAC move limiting, or storm control shutdown actions:

```
[edit ethernet-switching-options]
user@switch# set port-error-disable disable-timeout 60
```

Related Documentation

- *Example: Configuring Basic Port Security Features*
- *Configuring MAC Limiting (CLI Procedure)*
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- *Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches*
- Understanding Storm Control on EX Series Switches on page 7

Disabling or Enabling Storm Control (CLI Procedure)

The factory default configuration enables storm control on all EX Series switch interfaces, with the storm control level set to 80 percent of the combined applicable traffic streams, as follows:

- On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control

on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams.

- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the combined broadcast, multicast, and unknown unicast streams.
- On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. Storm control can be disabled for each type of traffic individually.

You can disable storm control for all the applicable types of traffic on all interfaces or on a specified interface, as follows:

- On all switches—You can selectively disable storm control for broadcast streams, multicast streams, or for unknown unicast streams.
- On EX8200 switches—You can additionally selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.
- On EX6200 switches—You can selectively disable storm control for each type of traffic individually.

You can enable storm control for multicast traffic (both registered and unregistered) on all interfaces or on a specific interface. This applies to all switches.

This topic describes:

- Disabling Storm Control on Broadcast Traffic on page 22
- Disabling Storm Control on All Multicast Traffic on page 22
- Disabling Storm Control on Registered Multicast Traffic (EX8200 Switches Only) on page 22
- Disabling Storm Control on Unregistered Multicast Traffic (EX8200 Switches Only) on page 22
- Disabling Storm Control on Unknown Unicast Traffic on page 22
- Enabling Storm Control on Multicast Traffic on page 23

Disabling Storm Control on Broadcast Traffic

To disable storm control on broadcast traffic:

- For all interfaces:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface all no-broadcast
```

- For an individual interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface interface-name no-broadcast
```

Disabling Storm Control on All Multicast Traffic

To disable storm control on all multicast traffic:

- For all interfaces:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface all no-multicast
```

- For an individual interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface interface-name no-multicast
```

Disabling Storm Control on Registered Multicast Traffic (EX8200 Switches Only)

To disable storm control only on registered multicast traffic (on EX8200 switches only):

- For all interfaces:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface all no-registered-multicast
```

- For an individual interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface interface-name no-registered-multicast
```

Disabling Storm Control on Unregistered Multicast Traffic (EX8200 Switches Only)

To disable storm control only on unregistered multicast traffic (on EX8200 switches only):

- For all interfaces:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface all no-unregistered-multicast
```

- For an individual interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface interface-name no-unregistered-multicast
```

Disabling Storm Control on Unknown Unicast Traffic

To disable storm control on unknown unicast traffic:

- For all interfaces:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface all no-unknown-unicast
```

- For an individual interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface interface-name no-unknown-unicast
```

Enabling Storm Control on Multicast Traffic

To enable storm control on multicast traffic:

- For all interfaces:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface all multicast
```

- For an individual interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface interface-name multicast
```

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- Understanding Storm Control on EX Series Switches on page 7

CHAPTER 6

Configuration Statements

[edit ethernet-switching-options] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the **[edit ethernet-switching-options]** hierarchy level on EX Series switches.

- *Supported* statements are those that you can use to configure some aspect of a software feature on the switch.
- *Unsupported* statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see Feature Explorer.

This topic lists:

Supported Statements in the [edit ethernet-switching-options] Hierarchy Level

The following hierarchy shows the **[edit ethernet-switching-options]** configuration statements supported on EX Series switches:

```
ethernet-switching-options {
  analyzer {
    name {
      input {
        egress {
          interface (all | interface-name);
        }
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      }
      loss-priority priority;
      output {
        interface interface-name;
        vlan (vlan-id | vlan-name);
      }
      ratio number;
    }
  }
  authentication-whitelist {
    interface;
    vlan-assignment;
  }
  bpdu-block {
    disable-timeout timeout;
    interface (all | [interface-name]) {
      (disable | drop | shutdown);
      }
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100);
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-lookup-length number-of-entries;
  }
  mac-notification {
    notification-interval seconds;
  }
  mac-table-aging-time seconds;
  port-error-disable {
```

```
    disable-timeout timeout;
}
redundant-trunk-group {
    group name {
        description;
        interface interface-name {
            primary;
        }
        preempt-cutover-timer seconds;
    }
}
secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted );
        fcoe-trusted;
        mac-limit limit action action;
        no-allowed-mac-log;
        static-ip  ip-address {
            mac mac-address;
            vlan  vlan-name;
        }
    }
    uac-policy;
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection );
        dhcp-option82 {
            disable;
                circuit-id {
                prefix hostname;
                use-interface-description;
                use-vlan-id;
            }
            remote-id {
                prefix (hostname | mac | none);
                use-interface-description;
                use-string string;
            }
            vendor-id [string];
        }
        (examine-dhcp | no-examine-dhcp);
        examine-fip {
            fc-map fc-map-value;
        }
        (ip-source-guard | no-ip-source-guard);
        mac-move-limit limit action action;
    }
}
```

```
    static {
      vlan vlan-id {
        mac mac-address next-hop interface-name;
      }
    }
    storm-control {
      action-shutdown;
      interface (all | interface-name) {
        bandwidth bandwidth;
        multicast;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
      }
    }
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
    unknown-unicast-forwarding {
      vlan (all | vlan-name) {
        interface interface-name;
      }
    }
    voip {
      interface (all | [interface-name | access-ports]) {
        forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
          network-control);
        vlan vlan-name;
      }
    }
  }
```

Unsupported Statements in the [edit ethernet-switching-options] Hierarchy Level

All statements in the **[edit ethernet-switching-options]** hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

- *Example: Setting Up Q-in-Q Tunneling on EX Series Switches*
- *Example: Configuring Redundant Trunk Links for Faster Recovery*
- *Configuring MAC Table Aging (CLI Procedure)*
- *Configuring MAC Notification (CLI Procedure)*
- *Configuring Q-in-Q Tunneling (CLI Procedure)*
- *Configuring Redundant Trunk Links for Faster Recovery (CLI Procedure)*
- *Configuring Nonstop Bridging on EX Series Switches (CLI Procedure)*

action-shutdown

Syntax action-shutdown;

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers):

  [edit forwarding-options storm-control-profiles *profile-name*]

- For platforms without ELS:

  [edit ethernet-switching-options storm-control]

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10.
(See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description Shut down or temporarily disable interfaces when the storm control level is exceeded, as follows:

- If you set both the **action-shutdown** and the port-error-disable statements, the interfaces are disabled temporarily and recover automatically when the disable timeout expires. (The **port-error-disable** statement is not available for MX Series routers.)
- If you set both the **action-shutdown** and the **recovery-timeout** statements, the interfaces are disabled temporarily and recover automatically when the recovery timeout expires.
- If you set the **action-shutdown** statement and do not the specify the **port-error-disable** statement (the **port-error-disable** statement is not available for MX Series routers), the interfaces that are enabled for storm control are shut down when the storm control level is exceeded and they do not recover automatically from that port-error condition. You must issue the clear ethernet-switching port-error command to clear the port error and restore the interfaces to service. (The **clear ethernet-switching port-error** command is not available for MX Series routers.)
- If you set the **action-shutdown** statement and do not the specify the **recovery-timeout** statement, the interfaces that are enabled for storm control are shut down when the storm control level is exceeded and they do not recover automatically from that port-error condition. For EX Series switches you must issue the **clear ethernet-switching recovery-timeout** command and for MX Series routers you must issue the **clear bridge recovery-timeout** command to clear the port error and restore the interfaces to service.

Default The **action-shutdown** option is not enabled by default. The switching device drops packets for the controlled traffic types if the ingress rate of the combined traffic streams exceeds the specified storm control level. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- port-error-disable on page 47
- disable-timeout on page 32
- *recovery-timeout*
- clear ethernet-switching port-error on page 56
- *clear bridge recovery-timeout*
- *clear ethernet-switching recovery-timeout*
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- *Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers*
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 20
- *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*

bandwidth

Syntax bandwidth *bandwidth*;

Hierarchy Level [edit ethernet-switching-options storm-control interface (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 9.5 for EX Series switches.

Description Configure the storm control level as the bandwidth in kilobits per second of the applicable traffic streams, as follows:

- On EX2200, EX3200, EX3300, EX4200, and EX6200 switches—Applies to the combined broadcast and unknown unicast streams by default. Storm control does not apply to multicast traffic by default on these switches. If you enable storm control for multicast traffic on a specific interface, the configured bandwidth allocation applies to the combined broadcast, unknown unicast, and multicast traffic on that interface.
- On EX4500 and EX8200 switches—Applies to the combined broadcast, multicast, and unknown unicast streams.

NOTE: When you configure storm control bandwidth on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control bandwidth of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.

Default If you omit the **bandwidth** statement when you configure storm control on an interface, the storm control level defaults to 80 percent of the available bandwidth used by the combined applicable traffic streams. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.

Options **bandwidth**—Traffic rate in kilobits per second of the combined applicable traffic streams.

Range: 100 through 10,000,000

Default: None

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- level on page 39
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- Disabling or Enabling Storm Control (CLI Procedure) on page 20

disable-timeout

Syntax disable-timeout *timeout*;

Hierarchy Level [edit ethernet-switching-options port-error-disable],

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.

Description Specify how long the Ethernet switching interfaces remain in a disabled state because of MAC limiting, MAC move limiting, or storm control errors.

NOTE: If you modify the timeout value of an existing disable timeout setting, the new timeout value does not impact the timing of restoration to service of currently disabled interfaces that have been configured for automatic recovery. The new timeout value is applied only during the next occurrence of a port error.

You can bring up the currently disabled interfaces by running the operational command clear ethernet-switching port-error.

Default The disable timeout is not enabled.

Options ***timeout***—Time, in seconds, that the disabled state remains in effect. The disabled interface is automatically restored to service when the specified timeout value is reached.

Range: 10 through 3600 seconds

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 20

ethernet-switching-options

Syntax

```
ethernet-switching-options {
  analyzer {
    name {
      loss-priority priority;
      ratio number;
      input {
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
        egress {
          interface (all | interface-name);
        }
      }
      output {
        interface interface-name;
        vlan (vlan-id | vlan-name) {
        no-tag;
        }
      }
    }
  }
  bpdu-block {
    disable-timeout timeout;
    interface (all | [interface-name]) {
      (disable | drop | shutdown);
      }
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100);
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-lookup-length number-of-entries;
}
  mac-notification {
    notification-interval seconds;
  }
  mac-table-aging-time seconds;
  nonstop-bridging;
  port-error-disable {
    disable-timeout timeout;
  }
  redundant-trunk-group {
    group name {
      interface interface-name <primary>;
      interface interface-name;
    }
  }
  secure-access-port {
    dhcp-snooping-file {
```

```
    location local_pathname | remote_URL;
    timeout seconds;
    write-interval seconds;
  }
  dhcpv6-snooping-file {
    location local_pathname | remote_URL;
    timeout seconds;
    write-interval seconds;
  }
  interface (all | interface-name) {
    allowed-mac {
      mac-address-list;
    }
    (dhcp-trusted | no-dhcp-trusted);
    fcoe-trusted;
    mac-limit limit action (drop | log | none | shutdown);
    no-allowed-mac-log;
    persistent-learning;
    static-ip ip-address {
      vlan  vlan-name;
      mac mac-address;
    }
    static-ipv6 ip-address {
      vlan  vlan-name;
      mac mac-address;
    }
  }
  vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection) [
      forwarding-class class-name;
    }
    dhcp-option82 {
      circuit-id {
        prefix hostname;
        use-interface-description;
        use-vlan-id;
      }
      remote-id {
        prefix hostname | mac | none;
        use-interface-description;
        use-string string;
      }
      vendor-id [string];
    }
    (examine-dhcp | no-examine-dhcp) {
      forwarding-class class-name;
    }
    (examine-dhcpv6 | no-examine-dhcpv6) {
      forwarding-class class-name;
    }
    examine-fip {
      fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    (ipv6-source-guard | no-ipv6-source-guard);
    mac-move-limit limit action (drop | log | none | shutdown);
```

```
    }
    (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
  no-option-37;
  static {
    vlan name {
      mac mac-address {
        next-hop interface-name;
      }
    }
  }
  storm-control {
    action-shutdown;
    interface (all | interface-name) {
      bandwidth bandwidth;
      level level;
      multicast;
      no-broadcast;
      no-multicast;
      no-registered-multicast;
      no-unknown-unicast;
      no-unregistered-multicast;
    }
  }
  traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable |
      no-world-readable>;
    flag flag <disable>;
  }
  unknown-unicast-forwarding {
    vlan (all | vlan-name) {
      interface interface-name;
    }
  }
  voip {
    interface (all | [interface-name | access-ports]) {
      vlan vlan-name;
      forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
        network-control);
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure Ethernet switching options.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Understanding Port Mirroring on EX Series Switches*
- *Understanding Port Security*
- *Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches*
- *Understanding Redundant Trunk Links*
- Understanding Storm Control on EX Series Switches on page 7
- *Understanding 802.1X and VoIP on EX Series Switches*
- *Understanding Q-in-Q Tunneling on EX Series Switches*
- Understanding Unknown Unicast Forwarding on page 11
- *Understanding MAC Notification on EX Series Switches*
- *Understanding FIP Snooping*
- *Understanding Nonstop Bridging on EX Series Switches*

interface (Storm Control)

Syntax

```
interface (all | interface-name) {
  bandwidth bandwidth;
  level level;
  multicast;
  no-broadcast;
  no-multicast;
  no-registered-multicast;
  no-unknown-unicast;
  no-unregistered-multicast;
}
```

Hierarchy Level [edit ethernet-switching-options storm-control]

Release Information Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure storm control on all interfaces or on the specified interface.

Default

- On EX2200, EX3200, EX3300, EX4200, and EX6200 switches—Storm control does not apply by default to multicast traffic. The factory default configuration enables storm control for broadcast and unknown unicast traffic on all switch interfaces, with the storm control level set to 80 percent of the combined broadcast and unknown unicast streams.
- On EX4500 and EX8200 switches—Storm control applies to broadcast, multicast, and unknown unicast traffic. The factory default configuration enables storm control on all switch interfaces, with the storm control level set to 80 percent of the combined broadcast, multicast, and unknown unicast streams.

Options

all—All interfaces. The storm control settings configured with the **all** option affect only those interfaces that have not been individually configured for storm control.

interface-name—Name of an interface. The storm control settings configured with the ***interface-name*** option override any settings configured with the **all** option.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- Disabling or Enabling Storm Control (CLI Procedure) on page 20

interface (Unknown Unicast Forwarding)

Syntax interface *interface-name*;

Hierarchy Level
- For platforms with ELS:

  [edit switch-options unknown-unicast-forwarding vlan *vlan-name*]
- For platforms without ELS:

  [edit ethernet-switching-options unknown-unicast-forwarding vlan *vlan-name*]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Hierarchy level **[edit switch-options]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Description Specify the interface to which unknown unicast packets will be forwarded.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *show vlans*
- **show ethernet-switching table on page 59**
- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 19
- Understanding Unknown Unicast Forwarding on page 11

level

Syntax level *level*;

Hierarchy Level [edit ethernet-switching-options storm-control interface (all | *interface-name*)]

Release Information Statement introduced in JUNOS Release 9.1 for EX Series switches.
Statement deprecated in JUNOS Release 9.5 for EX Series switches.
Statement reinstated in JUNOS Release 11.4 for EX Series switches.

Description For interfaces that are enabled for storm control, configure the storm control level as a percentage of the combined traffic streams that are subject to storm control on that interface.

Default When storm control is enabled on an interface, the default storm control level is 80 percent of the combined traffic streams that are subject to storm control on that interface.

Options *level*—Percentage of the combined traffic streams that are subject to storm control on that interface.

Range: 0 through 100 percent

Default: 80 percent

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- bandwidth on page 31
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- Understanding Storm Control on EX Series Switches on page 7

no-broadcast

Syntax no-broadcast;

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers):

  [edit forwarding-options storm-control-profiles *profile-name* all]

- For platforms without ELS:

  [edit ethernet-switching-options storm-control interface (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 9.1 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10.
(See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description Disable storm control for broadcast traffic for the specified interface or for all interfaces.

Default

- On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control on broadcast, multicast, or unknown-unicast traffic.
- On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic.
- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.
- On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually.
- On EX9200 switches—Storm control is not enabled by default.
- On MX Series routers—Storm control is not enabled by default.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- *Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers*
- Disabling or Enabling Storm Control (CLI Procedure) on page 20
- *Configuring or Disabling Storm Control (CLI Procedure)*

no-multicast

Syntax no-multicast;

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers):

  [edit forwarding-options storm-control-profiles *profile-name* all]

- For platforms without ELS:

  [edit ethernet-switching-options storm-control interface (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 10.3 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description Disable storm control for all multicast traffic (both registered multicast and unregistered multicast) for the specified interface or for all interfaces.

Default

- On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams.
- On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic.
- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.
- On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually.
- On EX9200 switches—Storm control is not enabled by default.
- On MX Series routers—Storm control is not enabled by default.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- no-registered-multicast on page 43
- no-unregistered-multicast on page 46
- Disabling or Enabling Storm Control (CLI Procedure) on page 20
- *Configuring or Disabling Storm Control (CLI Procedure)*

no-registered-multicast

Syntax

```
no-registered-multicast;
```

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers):

  [edit forwarding-options storm-control-profiles *profile-name* all]

- For platforms without ELS:

  [edit ethernet-switching-options storm-control interface (all | *interface-name*)]

Release Information

Statement introduced in Junos OS Release 10.3 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 13.2 for the QFX series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description

(EX8200 switches only) Disable storm control for registered multicast traffic for the specified interface or for all interfaces.

(EX4300 and EX9200 switches only) Exclude storm control for registered multicast traffic from a storm control profile.

(MX Series routers only) Exclude storm control for registered multicast traffic from a storm control profile.

Default

EX4300 and EX8200 switches—Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic. The default storm control level is 80 percent of the available bandwidth used by the combined applicable traffic streams.

EX9200 switches—Storm control is not enabled by default.

MX Series routers—Storm control is not enabled by default.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- no-multicast on page 42
- no-unregistered-multicast on page 46
- Understanding Storm Control on EX Series Switches on page 7
- *Understanding Storm Control on Switching Devices*

no-unknown-unicast

Syntax no-unknown-unicast;

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers):

  [edit forwarding-options storm-control-profiles *profile-name* all]

- For platforms without ELS:

  [edit ethernet-switching-options storm-control interface (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 9.1 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10.
(See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description Disable storm control for unknown unicast traffic for the specified interface or for all interfaces.

Default

- On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control on broadcast, multicast, or unknown-unicast traffic.
- On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic.
- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.
- On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually.
- On EX9200 switches—Storm control is not enabled by default.
- MX Series routers—Storm control is not enabled by default.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- *Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers*
- Disabling or Enabling Storm Control (CLI Procedure) on page 20
- *Configuring or Disabling Storm Control (CLI Procedure)*

no-unregistered-multicast

Syntax no-unregistered-multicast;

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers):

  [edit forwarding-options storm-control-profiles *profile-name* all]

- For platforms without ELS:

  [edit ethernet-switching-options storm-control interface (all | *interface-name*)],

Release Information Statement introduced in Junos OS Release 10.3 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10.
(See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 13.2 for the QFX series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.

Description (EX8200 switches only) Disable storm control for unregistered multicast traffic for the specified interface or for all interfaces.

(EX4300 and EX9200 switches only) Exclude storm control for unregistered multicast traffic from a storm control profile.

(MX Series routers) Exclude storm control for unregistered multicast traffic from a storm control profile.

Default EX4300 and EX8200 switches—Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic. The default storm control level is 80 percent of the available bandwidth used by the combined applicable traffic streams.

EX9200 switches—Storm control is not enabled by default.

MX Series routers—Storm control is not enabled by default.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- no-multicast on page 42
- no-registered-multicast on page 43
- Understanding Storm Control on EX Series Switches on page 7
- *Understanding Storm Control on Switching Devices*

port-error-disable

Syntax

```
port-error-disable {
  disable-timeout timeout ;
}
```

Hierarchy Level [edit ethernet-switching-options],

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.

Description Disable rather than block an interface when enforcing MAC limiting, MAC move limiting, and rate-limiting configuration options for shutting down the interface, and allow the interface to recover automatically from the error condition after a specified period of time:

- If you have enabled MAC limiting with the **shutdown** option and you enable **port-error-disable**, the switch disables (rather than shuts down) the interface when the MAC address limit is reached.
- If you have enabled MAC move limiting with the **shutdown** option and you enable **port-error-disable**,, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached.
- If you have enabled storm control with the **action-shutdown** option and you enable **port-error-disable**, the switch disables (rather than shuts down) the interface when applicable traffic exceeds the specified levels. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.

NOTE: The port-error-disable configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after port-error-disable has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the operational command that appears in your CLI:

- clear ethernet-switching port-error

The remaining statement is explained separately.

Default Not enabled.

Required Privilege Level system—To view this statement in the configuration.
system–control—To add this statement to the configuration.

Related Documentation

- action-shutdown on page 29
- *Configuring MAC Move Limiting (CLI Procedure)*

storm-control

Syntax

```
storm-control {
  action-shutdown;
  interface (all | interface-name) {
    bandwidth bandwidth;
    level level;
    multicast;
    no-broadcast;
    no-multicast;
    no-registered-multicast;
    no-unknown-unicast;
    no-unregistered-multicast;
  }
}
```

Hierarchy Level [edit ethernet-switching-options]

Release Information Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure storm control on the switch.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- Understanding Storm Control on EX Series Switches on page 7

unknown-unicast-forwarding

Syntax

```
unknown-unicast-forwarding {
  vlan vlan-name {
    interface interface-name;
  }
}
```

Hierarchy Level

- For platforms with ELS:

  [edit switch-options]

- For platforms without ELS:

  [edit ethernet-switching-options]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Hierarchy level **[edit switch-options]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Description

Configure the switch to forward all unknown unicast packets in a VLAN or on all VLANs to a particular interface.

The remaining statements are explained separately.

Default

Unknown unicast packets are flooded to all interfaces that belong to the same VLAN.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *show vlans*
- **show ethernet-switching table on page 59**
- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 19
- *Configuring Unknown Unicast Forwarding (CLI Procedure)*
- Understanding Unknown Unicast Forwarding on page 11

vlan (Unknown Unicast Forwarding)

Syntax

```
vlan (all | vlan-name) {
  interface (Unknown Unicast Forwarding) interface-name;
}
```

Hierarchy Level [edit ethernet-switching-options unknown-unicast-forwarding]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement updated with enhanced **?** (CLI completion feature) functionality in Junos OS Release 9.5 for EX Series switches.

Description Specify a VLAN from which unknown unicast packets will be forwarded or specify that the packets will be forwarded from all VLANS. Unknown unicast packets are forwarded from a VLAN to a specific trunk interface.

The **interface** statement is explained separately.

TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type **?** after **vlan** or **vlans** in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

Options all—All VLANs.

vlan-name—Name of a VLAN.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *show vlans*
- **show ethernet-switching table on page 59**
- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 19
- Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 53
- Understanding Unknown Unicast Forwarding on page 11

PART 3

Administration

CHAPTER 7

Routine Monitoring

Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface

Purpose Verify that a VLAN is forwarding all unknown unicast packets (those with unknown destination MAC addresses) to a single trunk interface instead of flooding unknown unicast packets across all interfaces that are members of the same VLAN.

Action Display the forwarding interface for unknown unicast packets for a VLAN (here, the VLAN name is **v1**):

```
user@switch> show configuration ethernet-switching-options

unknown-unicast-forwarding {
    vlan v1 {
        interface ge-0/0/7.0;
    }
}
```

Display the Ethernet switching table:

```
user@switch> show ethernet-switching table vlan v1
Ethernet-switching table: 3 unicast entries
  VLAN              MAC address       Type         Age Interfaces
  v1                *                 Flood          - All-members
  v1                00:01:09:00:00:00 Learn         24 ge-0/0/7.0
  v1                00:11:09:00:01:00 Learn         37 ge-0/0/3.0
```

Meaning The sample output from the **show configuration ethernet-switching-options** command shows that the unknown unicast forwarding interface for VLAN **v1** is interface **ge-0/0/7**. The **show ethernet-switching table** command shows that an unknown unicast packet is received on interface **ge-0/0/3** with the destination MAC address (DMAC) **00:01:09:00:00:00** and the source MAC address (SMAC) of **00:11:09:00:01:00**. This shows that the SMAC of the packet is learned in the normal way (through the interface **ge-0/0/3.0**), while the DMAC is learned on interface **ge-0/0/7**.

Related Documentation

- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 19

Verifying That the Port Error Disable Setting Is Working Correctly

Purpose Verify that the port error disable setting is working as expected on MAC limited, MAC move limited, and rate-limited interfaces on an EX Series switch.

Action Display information about interfaces:

```
user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  up       T1122                  unblocked
ge-0/0/1.0  down     default                MAC limit exceeded
ge-0/0/2.0  down     default                MAC move limit exceeded
ge-0/0/3.0  down     default                Storm control in effect
ge-0/0/4.0  down     default                unblocked
ge-0/0/5.0  down     default                unblocked
ge-0/0/6.0  down     default                unblocked
ge-0/0/7.0  down     default                unblocked
ge-0/0/8.0  down     default                unblocked
ge-0/0/9.0  up       T111                   unblocked
ge-0/0/10.0 down     default                unblocked
ge-0/0/11.0 down     default                unblocked
ge-0/0/12.0 down     default                unblocked
ge-0/0/13.0 down     default                unblocked
ge-0/0/14.0 down     default                unblocked
ge-0/0/15.0 down     default                unblocked
ge-0/0/16.0 down     default                unblocked
ge-0/0/17.0 down     default                unblocked
ge-0/0/18.0 down     default                unblocked
ge-0/0/19.0 up       T111                   unblocked
ge-0/1/0.0  down     default                unblocked
ge-0/1/1.0  down     default                unblocked
ge-0/1/2.0  down     default                unblocked
ge-0/1/3.0  down     default                unblocked
```

Meaning The sample output from the **show ethernet-switching interfaces** command shows that three of the down interfaces specify the reason that the interface is disabled:

- **MAC limit exceeded**—The interface is temporarily disabled because of a MAC limit error. The disabled interface is automatically restored to service when the **disable-timeout** expires.
- **MAC move limit exceeded**—The interface is temporarily disabled because of a MAC move limit error. The disabled interface is automatically restored to service when the **disable-timeout** expires.
- **Storm control in efffect** —The interface is temporarily disabled because of a storm control error. The disabled interface is automatically restored to service when the **disable-timeout** expires.

Related Documentation

- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 20

CHAPTER 8

Operational Commands

- clear ethernet-switching port-error
- clear ethernet-switching table
- show ethernet-switching table

clear ethernet-switching port-error

Syntax clear ethernet-switching port-error
<interface *interface-name*>

Release Information Command introduced in JUNOS Release 9.6 for EX Series switches.

Description Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch or from the specified interface, and restore all interfaces or the specified interface to service.

Options **none**—Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch and restore these interfaces to service.

interface *interface-name*—(Optional) Clear all MAC limiting, MAC move limiting, and storm control errors from the specified interface and restore the interface to service.

Required Privilege Level clear

Related Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 15
- *Configuring Port Security (CLI Procedure)*
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 20

List of Sample Output clear ethernet-switching port-error on page 56

Output Fields This command produces no output.

Sample Output

clear ethernet-switching port-error

```
user@switch> clear ethernet-switching port-error
```

clear ethernet-switching table

Syntax

clear ethernet-switching table
<interface *interface-name*>
<mac *mac-address*>
<management-vlan>
<persistent-mac <*interface* | *mac-address*>>
<vlan *vlan-name*>

Syntax (QFX Series)

clear ethernet-switching table
<interface *interface-name*>
<mac *mac-address*>
<persistent-mac <*interface* | *mac-address*>>
<vlan *vlan-name*>

Release Information

Command introduced in Junos OS Release 9.3 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

NOTE: On a QFabric system, using this command on an FCoE-enabled VLAN when FCoE sessions are active can cause traffic flooding and FCoE traffic drop. The FCoE sessions are not terminated and the traffic reconverges after a short period of time.

Clear learned entries, which are media access control (MAC) addresses, in the Ethernet switching table (also called the forwarding database table).

Options

none—Clear learned entries in the Ethernet switching table, except for persistent MAC addresses.

interface ***interface-name***—(Optional) Clear all learned MAC addresses for the specified interface from the Ethernet switching table.

mac ***mac-address***—(Optional) Clear the specified learned MAC address from the Ethernet switching table.

management-vlan—(Optional) Clear all MAC addresses learned for the management VLAN from the Ethernet switching table. Note that you do not specify a VLAN name because only one management VLAN exists.

persistent-mac <*interface* | *mac-address*>—(Optional) Clear all MAC addresses, including persistent MAC addresses. Use the **interface** option to clear all MAC addresses on an interface, or use the **mac-address** option to clear all entries for a specific MAC address.

Use this command whenever you move a device in your network that has a persistent MAC address on the switch. If you move the device to another port on the switch and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address and the device will not be able to connect. If the original port is down when you move the device, then the new port

will learn the MAC address and the device can connect—however, unless you cleared the MAC address on the original port, when the port comes back up, the system reinstalls the persistent MAC address in the forwarding table for that port. If this occurs, the address is removed from the new port and the device loses connectivity.

vlan ***vlan-name***—(Optional) Clear all MAC addresses learned for the specified VLAN from the Ethernet switching table.

Required Privilege Level view

Related Documentation
- show ethernet-switching table on page 59
- *show ethernet-switching table*
- *Verifying That Persistent MAC Learning Is Working Correctly*

List of Sample Output clear ethernet-switching table on page 58

Output Fields This command produces no output.

Sample Output

clear ethernet-switching table

```
user@switch> clear ethernet-switching table
```

show ethernet-switching table

Syntax

show ethernet-switching table
<brief | detail | extensive | summary>
<interface *interface-name*>
<management-vlan>
<persistent-mac <interface *interface-name*>>
<sort-by (*name* | *tag*)>
<vlan *vlan-name*>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Options **summary**, **management-vlan**, and **vlan *vlan-name*** introduced in Junos OS Release 9.6 for EX Series switches.
Option **sort-by** and field name **tag** introduced in Junos OS Release 10.1 for EX Series switches.
Option **persistent-mac** introduced in Junos OS Release 11.4 for EX Series switches.

Description

NOTE: If your EX Series switch CLI displays different options for the **show ethernet-switching table** command than the options shown in this document, see *show ethernet-switching table*.

Display the Ethernet switching table.

Options

none—(Optional) Display brief information about the Ethernet switching table.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display the Ethernet switching table for a specific interface.

management-vlan—(Optional) Display the Ethernet switching table for a management VLAN.

persistent-mac <interface *interface-name*>—(Optional) Display the persistent MAC addresses learned for all interfaces or a specified interface. You can use this command to view entries that you want to clear for an interface that you intentionally disabled.

sort-by (*name* | *tag*)—(Optional) Display VLANs in ascending order of VLAN IDs or VLAN names.

vlan *vlan-name*—(Optional) Display the Ethernet switching table for a specific VLAN.

Required Privilege Level

view

Related Documentation

- clear ethernet-switching table on page 57
- *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*

- *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
- *Example: Setting Up Q-in-Q Tunneling on EX Series Switches*

List of Sample Output

Output Fields

Table 3 on page 60 lists the output fields for the **show ethernet-switching table** command. Output fields are listed in the approximate order in which they appear.

Table 3: show ethernet-switching table Output Fields

Field Name	Field Description	Level of Output
VLAN	The name of a VLAN.	All levels
Tag	The VLAN ID tag name or number.	**extensive**
MAC or **MAC address**	The MAC address associated with the VLAN.	All levels
Type	The type of MAC address. Values are: • **static**—The MAC address is manually created. • **learn**—The MAC address is learned dynamically from a packet's source MAC address. • **flood**—The MAC address is unknown and flooded to all members. • **persistent**—The learned MAC addresses that will persist across restarts of the switch or interface-down events.	All levels except **persistent-mac**
Type	The type of MAC address. Values are: • **installed**—addresses that are in the Ethernet switching table. • **uninstalled**—addresses that could not be installed in the table or were uninstalled in an interface-down event and will be reinstalled in the table when the interface comes back up.	**persistent-mac**
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.	All levels
Interfaces	Interface associated with learned MAC addresses or **All-members** (flood entry).	All levels
Learned	For learned entries, the time which the entry was added to the Ethernet switching table.	**detail**, **extensive**
Nexthop index	The next-hop index number.	**detail**, **extensive**

Table 3: show ethernet-switching table Output Fields *(continued)*

Field Name	Field Description	Level of Output
persistent-mac	**installed** indicates MAC addresses that are in the Ethernet switching table and **uninstalled** indicates MAC addresses that could not be installed in the table or were uninstalled in an interface-down event (and will be reinstalled in the table when the interface comes back up).	

Sample Output

show ethernet-switching table

```
user@switch> show ethernet-switching table
Ethernet-switching table: 57 entries, 15 learned, 2 persistent
  VLAN              MAC address       Type         Age Interfaces
  F2                *                 Flood          - All-members
  F2                00:00:05:00:00:03 Learn          0 ge-0/0/44.0
  F2                00:19:e2:50:7d:e0 Static         - Router
  Linux             *                 Flood          - All-members
  Linux             00:19:e2:50:7d:e0 Static         - Router
  Linux             00:30:48:90:54:89 Learn          0 ge-0/0/47.0
  T1                *                 Flood          - All-members
  T1                00:00:05:00:00:01 Persistent     0 ge-0/0/46.0
  T1                00:00:5e:00:01:00 Static         - Router
  T1                00:19:e2:50:63:e0 Persistent     0 ge-0/0/46.0
  T1                00:19:e2:50:7d:e0 Static         - Router
  T10               *                 Flood          - All-members
  T10               00:00:5e:00:01:09 Static         - Router
  T10               00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T10               00:19:e2:50:7d:e0 Static         - Router
  T111              *                 Flood          - All-members
  T111              00:19:e2:50:63:e0 Learn          0 ge-0/0/15.0
  T111              00:19:e2:50:7d:e0 Static         - Router
  T111              00:19:e2:50:ac:00 Learn          0 ge-0/0/15.0
  T2                *                 Flood          - All-members
  T2                00:00:5e:00:01:01 Static         - Router
  T2                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T2                00:19:e2:50:7d:e0 Static         - Router
  T3                *                 Flood          - All-members
  T3                00:00:5e:00:01:02 Static         - Router
  T3                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T3                00:19:e2:50:7d:e0 Static         - Router
  T4                *                 Flood          - All-members
  T4                00:00:5e:00:01:03 Static         - Router
  T4                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
[output truncated]
```

show ethernet-switching table brief

```
user@switch> show ethernet-switching table brief
Ethernet-switching table: 57 entries, 15 learned, 2 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  F2                *                 Flood          - All-members
  F2                00:00:05:00:00:03 Learn          0 ge-0/0/44.0
  F2                00:19:e2:50:7d:e0 Static         - Router
  Linux             *                 Flood          - All-members
  Linux             00:19:e2:50:7d:e0 Static         - Router
  Linux             00:30:48:90:54:89 Learn          0 ge-0/0/47.0
  T1                *                 Flood          - All-members
```

```
  T1                00:00:05:00:00:01 Persistent     0 ge-0/0/46.0
  T1                00:00:5e:00:01:00 Static         - Router
  T1                00:19:e2:50:63:e0 Persistent     0 ge-0/0/46.0
  T1                00:19:e2:50:7d:e0 Static         - Router
  T10               *                 Flood          - All-members
  T10               00:00:5e:00:01:09 Static         - Router
  T10               00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T10               00:19:e2:50:7d:e0 Static         - Router
  T111              *                 Flood          - All-members
  T111              00:19:e2:50:63:e0 Learn          0 ge-0/0/15.0
  T111              00:19:e2:50:7d:e0 Static         - Router
  T111              00:19:e2:50:ac:00 Learn          0 ge-0/0/15.0
  T2                *                 Flood          - All-members
  T2                00:00:5e:00:01:01 Static         - Router
  T2                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T2                00:19:e2:50:7d:e0 Static         - Router
  T3                *                 Flood          - All-members
  T3                00:00:5e:00:01:02 Static         - Router
  T3                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
  T3                00:19:e2:50:7d:e0 Static         - Router
  T4                *                 Flood          - All-members
  T4                00:00:5e:00:01:03 Static         - Router
  T4                00:19:e2:50:63:e0 Learn          0 ge-0/0/46.0
[output truncated]
```

show ethernet-switching table detail

```
user@switch> show ethernet-switching table detail
Ethernet-switching table: 5 entries, 2 learned entries
 VLAN: default, Tag: 0, MAC: *, Interface: All-members
  Interfaces:
   ge-0/0/11.0, ge-0/0/20.0, ge-0/0/30.0, ge-0/0/36.0, ge-0/0/3.0
  Type: Flood
  Nexthop index: 1307

 VLAN: default, Tag: 0, MAC: 00:1f:12:30:b8:83, Interface: ge-0/0/3.0
   Type: Learn, Age: 0, Learned: 20:09:26
   Nexthop index: 1315

 VLAN: v1, Tag: 101, MAC: *, Interface: All-members
  Interfaces:
   ge-0/0/31.0
  Type: Flood
  Nexthop index: 1313

 VLAN: v1, Tag: 101, MAC: 00:1f:12:30:b8:89, Interface: ge-0/0/31.0
  Type: Learn, Age: 0, Learned: 20:09:25
  Nexthop index: 1312

 VLAN: v2, Tag: 102, MAC: *, Interface: All-members
  Interfaces:
   ae0.0
  Type: Flood
  Nexthop index: 1317
```

show ethernet-switching table extensive

```
user@switch> show ethernet-switching table extensive
Ethernet-switching table: 3 entries, 1 learned, 5 persistent entries

    VLAN: v1, Tag: 10, MAC: *, Interface: All-members
```

```
Interfaces:
            ge-0/0/14.0, ge-0/0/1.0, ge-0/0/2.0, ge-0/0/3.0, ge-0/0/4.0,
            ge-0/0/5.0, ge-0/0/6.0, ge-0/0/7.0, ge-0/0/8.0, ge-0/0/10.0,
            ge-0/0/0.0
Type: Flood
Nexthop index: 567

VLAN: v1, Tag: 10, MAC: 00:21:59:c6:93:22, Interface: Router
Type: Static
Nexthop index: 0

VLAN: v1, Tag: 10, MAC: 00:21:59:c9:9a:4e, Interface: ge-0/0/14.0
Type: Learn, Age: 0, Learned: 18:40:50
Nexthop index: 564
```

show ethernet-switching table persistent-mac

```
user@switch> show ethernet-switching table persistent-mac
VLAN              MAC address       Type       Interface
default           00:10:94:00:00:02 installed    ge-0/0/42.0
default           00:10:94:00:00:03 installed    ge-0/0/42.0
default           00:10:94:00:00:04 installed    ge-0/0/42.0
default           00:10:94:00:00:05 installed    ge-0/0/42.0
default           00:10:94:00:00:06 installed    ge-0/0/42.0
default           00:10:94:00:05:02 uninstalled ge-0/0/16.0
default           00:10:94:00:06:03 uninstalled ge-0/0/16.0
default           00:10:94:00:07:04 uninstalled ge-0/0/16.0
```

show ethernet-switching table persistent-mac interface ge-0/0/16.0

```
VLAN              MAC address       Type       Interface
default           00:10:94:00:05:02 uninstalled ge-0/0/16.0
default           00:10:94:00:06:03 uninstalled ge-0/0/16.0
default           00:10:94:00:07:04 uninstalled ge-0/0/16.0
```