

# Device Security Feature Guide for EX9200 Switches

Release

15.1



---

Modified: 2015-06-28

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Device Security Feature Guide for EX9200 Switches*

15.1

Copyright © 2015, Juniper Networks, Inc.  
All rights reserved.

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

	About the Documentation . . . . .	vii
	Documentation and Release Notes . . . . .	vii
	Supported Platforms . . . . .	vii
	Using the Examples in This Manual . . . . .	vii
	Merging a Full Example . . . . .	viii
	Merging a Snippet . . . . .	viii
	Documentation Conventions . . . . .	ix
	Documentation Feedback . . . . .	xi
	Requesting Technical Support . . . . .	xi
	Self-Help Online Tools and Resources . . . . .	xi
	Opening a Case with JTAC . . . . .	xii
<b>Part 1</b>	<b>Configuring Storm Control to Monitor Traffic Levels and Prevent Packet-Flooding on LANs</b>	
<b>Chapter 1</b>	<b>Storm Control Overview . . . . .</b>	<b>3</b>
	Understanding Storm Control on Switching Devices . . . . .	3
<b>Chapter 2</b>	<b>Configuring Storm Control . . . . .</b>	<b>7</b>
	Configuring or Disabling Storm Control (CLI Procedure) . . . . .	7
	Configuring Storm Control . . . . .	8
	Disabling Storm Control on Broadcast Traffic . . . . .	8
	Disabling Storm Control on All Multicast Traffic . . . . .	9
	Disabling Storm Control on Registered Multicast Traffic . . . . .	9
	Disabling Storm Control on Unregistered Multicast Traffic . . . . .	10
	Disabling Storm Control on Unknown Unicast Traffic . . . . .	10
	Disabling Storm Control on Multiple Types of Traffic . . . . .	10
	Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) . . . . .	12
	Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches . . . . .	13
<b>Part 2</b>	<b>Configuring Unknown Unicast Forwarding to Prevent Traffic Storms</b>	
<b>Chapter 3</b>	<b>Unknown Unicast Forwarding Overview . . . . .</b>	<b>19</b>
	Understanding Unknown Unicast Forwarding . . . . .	19

<b>Chapter 4</b>	<b>Configuring Unknown Unicast Forwarding . . . . .</b>	<b>21</b>
	Configuring Unknown Unicast Forwarding (CLI Procedure) . . . . .	21
	Configuring Unknown Unicast Forwarding on EX4300 Switches . . . . .	21
	Configuring Unknown Unicast Forwarding on EX9200 Switches . . . . .	22
	Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages . . . . .	23
	Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages . . . . .	23
	Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface . . . . .	24
<b>Part 3</b>	<b>Configuration Statements and Operational Commands</b>	
<b>Chapter 5</b>	<b>Configuration Statements . . . . .</b>	<b>27</b>
	[edit switch-options] Configuration Statement Hierarchy on EX Series Switches . . . . .	27
	Supported Statements in the [edit switch-options] Hierarchy Level . . . . .	28
	Unsupported Statements in the [edit switch-options] Hierarchy Level . . . . .	29
	[edit system] Hierarchy Level . . . . .	29
	action-shutdown . . . . .	44
	bandwidth-level . . . . .	46
	bandwidth-percentage . . . . .	47
	filter (VLANs) . . . . .	48
	filter (Firewall Filters) . . . . .	49
	flood (VLANs) . . . . .	50
	forwarding-options . . . . .	51
	group-type (Unknown Unicast Forwarding) . . . . .	52
	icmpv4-rate-limit . . . . .	53
	icmpv6-rate-limit . . . . .	54
	next-hop-group (Unknown Unicast Forwarding) . . . . .	55
	no-broadcast . . . . .	56
	no-multicast . . . . .	58
	no-registered-multicast . . . . .	60
	no-unknown-unicast . . . . .	61
	no-unregistered-multicast . . . . .	63
	recovery-timeout . . . . .	64
	storm-control . . . . .	66
	storm-control-profiles . . . . .	67
<b>Chapter 6</b>	<b>Operational Commands . . . . .</b>	<b>69</b>
	clear ethernet-switching recovery-timeout . . . . .	70

# List of Tables

	<b>About the Documentation</b> .....	<b>vii</b>
	Table 1: Notice Icons .....	ix
	Table 2: Text and Syntax Conventions .....	ix
<b>Part 3</b>	<b>Configuration Statements and Operational Commands</b>	
<b>Chapter 5</b>	<b>Configuration Statements</b> .....	<b>27</b>
	Table 3: Unsupported [edit switch-options] Configuration Statements on EX Series Switches .....	29



# About the Documentation

- Documentation and Release Notes on page vii
- Supported Platforms on page vii
- Using the Examples in This Manual on page vii
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xi

## 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.xml;
    }
  }
}
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.xml; }
```

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
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host&gt; show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"><li>Introduces or emphasizes important new terms.</li><li>Identifies guide names.</li><li>Identifies RFC and Internet draft titles.</li></ul>	<ul style="list-style-type: none"><li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li><li><i>Junos OS CLI User Guide</i></li><li>RFC 1997, <i>BGP Communities Attribute</i></li></ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"><li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li><li>The console port is labeled <b>CONSOLE</b>.</li></ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric <i>metric</i>&gt;;</b>
(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.	<b>broadcast   multicast</b>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; 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.	<ul style="list-style-type: none"><li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>To cancel the configuration, click <b>Cancel</b>.</li></ul>

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 <b>Protocols&gt;Ospf</b> .

## 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](mailto: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 Partner Support Service 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

# Configuring Storm Control to Monitor Traffic Levels and Prevent Packet-Flooding on LANs

- [Storm Control Overview on page 3](#)
- [Configuring Storm Control on page 7](#)



## CHAPTER 1

# Storm Control Overview

- [Understanding Storm Control on Switching Devices on page 3](#)

## Understanding Storm Control on Switching Devices

---



**NOTE:** This topic uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switching device is an EX Series switch and runs software that does not support ELS, see *Understanding Storm Control on EX Series Switches*. If your switching device is an EX Series switch and runs software that does support ELS, see *Getting Started with Enhanced Layer 2 Software*.

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 switching device to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the *storm control level* or *storm control bandwidth*—is exceeded, thus preventing packets from proliferating and degrading the LAN. As an alternative to having the switching device drop packets, you can configure storm control to shut down interfaces or temporarily disable interfaces (see the [action-shutdown](#) statement and the [recovery-timeout](#) statement) when the storm control level is exceeded.



**NOTE:** On Juniper Networks EX4300 Ethernet Switches, the factory default configuration enables storm control on all Layer 2 interfaces, with the storm control level set to 80 percent of the combined broadcast, multicast, and unknown unicast traffic streams.

Storm control is not enabled by default on Juniper Networks EX9200 Ethernet Switches.

Storm control is not enabled by default on Juniper Networks MX Series routers.

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

- **Bandwidth level**—Configures the storm control level as the bandwidth in kilobits per second of the applicable traffic streams on that interface.
- **Bandwidth percentage**—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.



**NOTE:** You cannot configure both bandwidth level and bandwidth percentage for the same interface.

---

You can disable storm control selectively for broadcast, multicast, or unknown unicast traffic, or any combination of traffic types. When disabling storm control for multicast traffic, you can specify the traffic to be either registered multicast or unregistered multicast. 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. Therefore, 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 the switching device to drop broadcast traffic, multicast traffic, unknown unicast traffic, or two or all three of those traffic types.



**NOTE:** When you configure 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 level 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 13](#)
- [Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers](#)



- [Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 12](#)
- [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)



## CHAPTER 2

# Configuring Storm Control

- [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)
- [Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 12](#)
- [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13](#)

## Configuring or Disabling Storm Control (CLI Procedure)

---



**NOTE:** This task uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switching device is an EX Series switch and runs software that does not support ELS, see *Understanding Storm Control on EX Series Switches*. If your switching device is an EX Series switch and runs software that does support ELS, see *Getting Started with Enhanced Layer 2 Software*.

On EX4300 switches, the factory default configuration enables storm control on all Layer 2 switch interfaces. The default storm control level is set to 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.

Storm control is not enabled by default on EX9200 switches or MX Series routers.

You can customize the storm control level for a specific interface. You specify the storm control level as the traffic rate in kilobits per second (Kbps) of the combined traffic streams or as the percentage of available bandwidth used by the combined traffic streams.

You can selectively disable storm control for broadcast, multicast, or unknown unicast traffic on all interfaces or on a specified interface. You can additionally disable storm control on registered or unregistered multicast traffic.

In the tasks described in this topic, you use the `[edit interfaces interface-name unit 0 family ethernet-switching]` hierarchy level to bind the storm control profile for EX Series switches

and the `[edit interfaces interface-name unit 0 family bridge]` hierarchy level to bind the storm control profile for MX Series routers.

- [Configuring Storm Control on page 8](#)
- [Disabling Storm Control on Broadcast Traffic on page 8](#)
- [Disabling Storm Control on All Multicast Traffic on page 9](#)
- [Disabling Storm Control on Registered Multicast Traffic on page 9](#)
- [Disabling Storm Control on Unregistered Multicast Traffic on page 10](#)
- [Disabling Storm Control on Unknown Unicast Traffic on page 10](#)
- [Disabling Storm Control on Multiple Types of Traffic on page 10](#)

## Configuring Storm Control

You can configure storm control for a specific interface. The storm control level can be customized by explicitly configuring either the bandwidth level or the bandwidth percentage.

- **bandwidth-level**—Configures the storm control level as the bandwidth in kilobits per second of the combined traffic streams.
- **bandwidth-percentage**—Configures the storm control level as a percentage of the available bandwidth used by the combined traffic streams.

To configure storm control:

1. Create a storm control profile and set the storm control level as the traffic rate in kilobits per second of the combined traffic streams:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps
```



**NOTE:** The name of the storm control profile can contain no more than 127 characters.

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

## Disabling Storm Control on Broadcast Traffic

To disable storm control on broadcast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams and exclude broadcast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps no-broadcast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

## Disabling Storm Control on All Multicast Traffic

To disable storm control on all multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, but exclude multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps no-multicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

## Disabling Storm Control on Registered Multicast Traffic

To disable storm control on only registered multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, but exclude registered multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps
no-registered-multicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

## Disabling Storm Control on Unregistered Multicast Traffic

To disable storm control on only unregistered multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, but exclude unregistered multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps
no-unregistered-multicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

## Disabling Storm Control on Unknown Unicast Traffic

To disable storm control on only unknown unicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, but exclude unregistered multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps
no-unknown-unicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

## Disabling Storm Control on Multiple Types of Traffic

To disable storm control on multiple types of traffic; for example, broadcast and multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams but exclude broadcast and multicast traffic:

```
[edit forwarding-options]
```

```
user@device# set storm-control-profiles profile-name all bandwidth-level kbps no-broadcast no-multicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

**Related  
Documentation**

- [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13](#)
- [Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers](#)
- [Understanding Storm Control on Switching Devices on page 3](#)

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



**NOTE:** This example uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switching device is an EX Series switch and runs software that does not support ELS, see *Understanding Storm Control on EX Series Switches*. If your switching device is an EX Series switch and runs software that does support ELS, see *Getting Started with Enhanced Layer 2 Software*.

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

- MAC limiting—(Not supported on MX Series routers) The **mac-limit** statement is configured with the **action-shutdown** statement.
- MAC move limiting—(Not supported on MX Series routers) The **mac-move-limit** statement is configured with the **action-shutdown** statement.
- Storm control—The **storm-control** statement is configured with the **action-shutdown** statement.

You can configure the switching device to automatically restore the disabled interfaces to service after a specified period of time. The specified time configured in the **recovery-timeout** statement applies to all the interfaces that have been disabled due to MAC limiting, MAC move limiting, or storm control errors.



**NOTE:** To enable autorecovery, specify the recovery timeout value for the interfaces to recover automatically. There is no default recovery timeout. If you do not specify a timeout value, you need to use the [clear ethernet-switching recovery-timeout](#) command for EX Series switches and the [clear bridge recovery-timeout](#) command for MX Series routers to clear the errors and restore the interfaces to service.

To specify the recovery timeout period for the interface:

- Set the **recovery-timeout** statement.

For EX Series switches:

```
[edit interfaces interface-name family unit 0 ethernet-switching]
user@switch# set recovery-timeout seconds
```

For MX Series routers:

```
[edit interfaces interface-name family unit 0 bridge]
user@switch# set recovery-timeout seconds
```

**Related  
Documentation**



- [Configuring MAC Limiting \(CLI Procedure\)](#)
- [Configuring MAC Move Limiting \(CLI Procedure\)](#)
- [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)

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



**NOTE:** This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

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, unknown unicast, and multicast (BUM) traffic, and at a specified level and to have packets dropped when the specified traffic level is exceeded, thereby preventing packets from proliferating and degrading the LAN.



**NOTE:** On EX4300 switches, the factory default configuration enables storm control on all Layer 2 interfaces, with the storm control level set to 80 percent of the available bandwidth used by the applicable traffic streams on that interface.

This example shows how to configure storm control on an EX Series switch running Junos OS with ELS.

- [Requirements on page 13](#)
- [Overview and Topology on page 13](#)
- [Configuration on page 14](#)
- [Verification on page 15](#)

### Requirements

This example uses the following hardware and software components:

- One EX Series switch running Junos OS with ELS
- Junos OS Release 13.2 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 BUM 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 or as the percentage of available bandwidth used by the combined applicable traffic streams.

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 storm control to have the switch shut down interfaces or temporarily disable interfaces (see the [action-shutdown](#) statement or the [recovery-timeout](#) statement) when the storm control level is exceeded.

The topology used in this example consists of one switch 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 of the combined traffic streams, copy the following command and paste it into the switch terminal window:

```
[edit]
set forwarding-options storm-control-profiles sc all bandwidth-level 15000
set interfaces ge-0/0/0 unit 0 family ethernet-switching storm-control sc
```

**Step-by-Step Procedure** To configure storm control:

1. Configure a storm control profile, **sc**, and specify the traffic rate in Kbps of the combined traffic streams:

```
[edit]
user@switch# set forwarding-options storm-control-profiles sc all bandwidth-level 15000
```



**NOTE:** The name of the storm control profile can contain no more than 127 characters.

2. Bind the storm control profile, **sc**, to a logical interface:

```
[edit]
user@switch> set interfaces ge-0/0/0 unit 0 family ethernet-switching storm-control sc
```

**Results** Display the results of the configuration:

```
[edit forwarding-options]
user@switch> show storm-control-profiles sc
all {
    bandwidth 15000;
}

[edit]
user@switch> show interfaces ge-0/0/0
```

```

unit 0 {
  family ethernet-switching {
    vlan {
      members default;
    }
    storm-control sc;
  }
}

```

## 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 (in bits per second) must not exceed the storm control limit.

```

user@switch> show interfaces ge-0/0/0 detail
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
  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
Interface transmit statistics: Disabled
```

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

- Related Documentation**
- [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)
  - [Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 12](#)
  - [Understanding Storm Control on Switching Devices on page 3](#)

## PART 2

# Configuring Unknown Unicast Forwarding to Prevent Traffic Storms

- [Unknown Unicast Forwarding Overview on page 19](#)
- [Configuring Unknown Unicast Forwarding on page 21](#)



## CHAPTER 3

# Unknown Unicast Forwarding Overview

- [Understanding Unknown Unicast Forwarding on page 19](#)

## 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 traverse a VLAN to all interfaces that are members of that 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 flooding of packets is known as a traffic storm.

To prevent a traffic storm, you can disable the flooding of unknown unicast packets to all VLAN interfaces by configuring specific VLANs or all VLANs to forward all unknown unicast traffic traversing them to a specific interface. You can configure multiple VLANs to forward unknown unicast packets to the same interface or configure different interfaces for different VLANs. This channels the unknown unicast traffic traversing VLANs to specific interfaces instead of flooding all interfaces.

### Related Documentation

- [Configuring Unknown Unicast Forwarding \(CLI Procedure\)](#)
- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 21](#)
- [Understanding Storm Control on EX Series Switches](#)
- [Understanding Storm Control on Switching Devices on page 3](#)
- [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches](#)
- [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13](#)





## CHAPTER 4

# Configuring Unknown Unicast Forwarding

- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 21](#)
- [Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 23](#)
- [Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 23](#)
- [Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface on page 24](#)

## Configuring Unknown Unicast Forwarding (CLI Procedure)

---



**NOTE:** This task uses Junos OS for EX Series switches or QFX Series with support for the Enhanced Layer 2 Software (ELS) configuration style. If your EX Series switch runs software that does not support ELS, see *Configuring Unknown Unicast Forwarding (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets that traverse a VLAN to all interfaces associated with that VLAN. This flooding of packets is known as a traffic storm and can negatively impact network performance.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN to a specific interface. You can configure each VLAN to divert unknown unicast traffic to a different interface or use the same interface for multiple VLANs.

- [Configuring Unknown Unicast Forwarding on EX4300 Switches on page 21](#)
- [Configuring Unknown Unicast Forwarding on EX9200 Switches on page 22](#)

## Configuring Unknown Unicast Forwarding on EX4300 Switches

To configure unknown unicast forwarding options on EX4300 switches:

- Configure unknown unicast forwarding for a specific VLAN and specify the interface to which all unknown unicast traffic will be forwarded:

```
[edit switch-options]
```

```
user@switch# set unknown-unicast-forwarding vlan vlan-name interface interface-name
```

- Configure unknown unicast forwarding for all VLANs and specify the interface to which all unknown unicast traffic will be forwarded:

```
[edit switch-options]
```

```
user@switch# set unknown-unicast-forwarding vlan all interface interface-name
```

## Configuring Unknown Unicast Forwarding on EX9200 Switches

To configure unknown unicast forwarding on EX9200 switches, you must configure a flood filter and apply it to VLANs for which you want to configure unknown unicast forwarding. Flood filters are firewall filters that are applied only to broadcast, unknown unicast, and multicast (BUM) traffic. If a flood filter is configured, only traffic packets that are of the packet type **unknown-unicast** are forwarded to the interface on which unicast forwarding is configured. A next-hop group redirects the packets according to the action specified in the flood filter.

To configure the next-hop group that receives Layer 2 packets and then configure the interface to which these packets are forwarded:

1. Configure the **next-hop-group** action for the Layer 2 interface expected to receive unknown unicast packets:

```
[edit forwarding-options]
```

```
user@switch# set next-hop-group next-hop-group-name group-type layer-2
```

```
[edit forwarding-options]
```

```
user@switch# set next-hop-group next-hop-group-name interface interface-name
```

For example:

```
[edit forwarding-options]
```

```
user@switch# set next-hop-group uuf-nhg group-type layer-2
```

```
[edit forwarding-options]
```

```
user@switch# set next-hop-group uuf-nhg interface ge-3/1/7.0
```

2. Configure a firewall filter with family address type **ethernet-switching**:

```
[edit firewall]
```

```
user@switch# set family ethernet-switching filter filter-name
```

For example:

```
[edit firewall]
```

```
user@switch# set family ethernet-switching filter uuf_filter
```

3. Configure a term in the firewall filter for the interface that receives unknown unicast packets (the interface specified in Step 1) to discard unknown unicast packets:

```
[edit firewall family ethernet-switching filter filter-name]
```

```
user@switch# set term term-name from interface interface-name
```

```
user@switch# set term term-name from traffic-type unknown-unicast
```

```
user@switch# set term term-name then discard
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
```

```
user@switch# set term source-drop from interface ge-3/1/7.0
```

```
user@switch# set term source-drop from traffic-type unknown-unicast
```

```
user@switch# set term source-drop then discard
```

4. Configure a term in the firewall filter for unknown unicast packets to be flooded to the interface enabled for unknown unicast forwarding by using **next-hop-group** (in step 1):

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name from traffic-type unknown-unicast
user@switch# set term term-name then next-hop-group group-name
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term uuf-flood from traffic-type unknown-unicast
user@switch# set term uuf-flood then next-hop-group uuf-nhg
```

5. Configure a default term for the firewall filter to forward packets other than unknown unicast packets:

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name then accept
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term fwd-default then accept
```

6. Apply the filter as a flood filter on the VLAN that includes the interface which will receive unknown unicast packets:

```
[edit vlans vlan-name]
user@switch# set forwarding-options flood input filter-name
```

For example:

```
[edit vlans v1]
user@switch# set forwarding-options flood input uuf_filter
```

- Related Documentation**
- [Understanding Unknown Unicast Forwarding on page 19](#)
  - [Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface on page 24](#)

## Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages

To limit the rate at which ICMPv4 messages can be generated by the Routing Engine and sent to the Routing Engine, include the **icmpv4-rate-limit** statement at the **[edit system internet-options]** hierarchy level:

```
icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
```

The bucket size is the number of seconds in the rate-limiting bucket. The packet rate is the rate-limiting packets earned per second. Specify a **bucket-size** from 0 through 4294967295 seconds. The default value is 5 seconds. Specify a **packet-rate** from 0 through 4,294,967,295. The default value is 1000.

- Related Documentation**
- [Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 23](#)

## Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages

To limit the rate at which ICMPv6 messages are sent, include the **icmpv6-rate-limit** statement at the **[edit system internet-options]** hierarchy level:

```
icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
```

The bucket size is the the number of seconds in the rate-limiting bucket. The packet rate is the rate-limiting packets earned per second. Specify a **bucket-size** from 0 through 4294967295 seconds. The default value is 5 seconds. Specify a **packet-rate** from 0 through 4294967295. The default value is 1000.

- Related Documentation**
- [Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 23](#)

---

## Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface

---

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



**NOTE:** This procedure uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, See: *Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface*. For ELS details see: *Getting Started with Enhanced Layer 2 Software*.

---

**Action** (EX4300 Switches) Display the forwarding interface for unknown unicast packets for a VLAN (here, the VLAN name is v1):

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

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

(EX9200 Switches) Display the forwarding interface for unknown unicast packets:

```
user@switch> show forwarding-options
```

```
next-hop-group uuf-nhg {  
  group-type layer-2;  
  interface ge-0/0/7.0;  
}
```

**Meaning** The sample output from the **show** commands show that the unknown unicast forwarding interface for VLAN v1 is interface **ge-0/0/7**.

- Related Documentation**
- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 21](#)

## PART 3

# Configuration Statements and Operational Commands

- Configuration Statements on page 27
- Operational Commands on page 69



## CHAPTER 5

# Configuration Statements

- [\[edit switch-options\] Configuration Statement Hierarchy on EX Series Switches on page 27](#)
- [\[edit system\] Hierarchy Level on page 29](#)
- [action-shutdown on page 44](#)
- [bandwidth-level on page 46](#)
- [bandwidth-percentage on page 47](#)
- [filter \(VLANs\) on page 48](#)
- [filter \(Firewall Filters\) on page 49](#)
- [flood \(VLANs\) on page 50](#)
- [forwarding-options on page 51](#)
- [group-type \(Unknown Unicast Forwarding\) on page 52](#)
- [icmpv4-rate-limit on page 53](#)
- [icmpv6-rate-limit on page 54](#)
- [next-hop-group \(Unknown Unicast Forwarding\) on page 55](#)
- [no-broadcast on page 56](#)
- [no-multicast on page 58](#)
- [no-registered-multicast on page 60](#)
- [no-unknown-unicast on page 61](#)
- [no-unregistered-multicast on page 63](#)
- [recovery-timeout on page 64](#)
- [storm-control on page 66](#)
- [storm-control-profiles on page 67](#)

### [\[edit switch-options\] Configuration Statement Hierarchy on EX Series Switches](#)

---

This topic lists supported and unsupported configuration statements in the **[edit switch-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 *EX Series Switch Software Features Overview*.

This topic lists:

- [Supported Statements in the \[edit switch-options\] Hierarchy Level on page 28](#)
- [Unsupported Statements in the \[edit switch-options\] Hierarchy Level on page 29](#)

## Supported Statements in the [edit switch-options] Hierarchy Level

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

```
switch-options {
  authentication-whitelist mac-address {
    interface interface-name;
    vlan-assignment (vlan-id | vlan-name);
  }
  interface interface-name {
    interface-mac-limit number {
      packet-action action;
    }
    no-mac-learning;
    persistent-learning
  }
  no-mac-learning;
  redundant-trunk-group {
    group name {
      description text;
      interface interface-name {
        primary;
      }
      preempt-cutover-timer seconds
    }
  }
  unknown-unicast-forwarding {
    vlan (all | vlan-name | vlan-tag) {
      interface interface-name;
    }
  }
  voip {
    interface (all | [interface-name | access-ports]) {
      forwarding-class (assured-forwarding | best-effort | expedited-forwarding | mcast-af
        | mcast-be | mcast-ef | mcast-nc | network-control);
      vlan vlan-name;
    }
  }
}
```



## Unsupported Statements in the [edit switch-options] Hierarchy Level

All statements in the [edit switch-options] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

**Table 3: Unsupported [edit switch-options] Configuration Statements on EX Series Switches**

Statement	Hierarchy Level
port-error-disable	[edit switch-options]
disable-timeout	[edit switch-options port-error-disable]

**NOTE:** Variables, such as *filename*, are not shown in the statements or hierarchies.

## [edit system] Hierarchy Level

```

system {
  accounting {
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number;
            max-outstanding-requests
            port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        source-address address;
        timeout seconds;
      }
    }
  }
}
events [ change-log interactive-commands login ];
allow-6pe-traceroute;
allow-v4mapped-packets;
archival {
  configuration {
    archive-sites {

```

```

        ftp://<username>:<password>@<host>:<port>/<url-path>;
        scp://<username>:<password>@<host>:<port>/<url-path>;
    }
    transfer-interval interval;
    transfer-on-commit;
}
}
arp {
    aging-timer minutes;
    gratuitous-arp-delay;
    gratuitous-arp-on-ifup;
    interfaces {
        logical-interface-name {
            aging-timer minutes;
        }
    }
    passive-learning;
    purging;
}
authentication-order [ authentication-methods ];
auto-configuration {
    traceoptions {
        file <filename> <files number> <match regular-expression> <size size>
            <world-readable | no-world-readable>;
        flag <all | auth | configuration | ;interfaces | io | rtsock | ui>
        level level;
        no-remote-trace;
    }
}
}
backup-router address <destination [ destination-addresses ]>;
commit {
    fast-synchronize;
    synchronize;
    server {
        commit-interval number;
        days-to-keep-error-logs number;
        maximum-aggregate-pool number;
        maximum-entries number;
        traceoptions {
            file <filename> <files number> <match regular-expression> <size size>
                <world-readable | no-world-readable>;
            flag <all | auth | configuration | ;interfaces | io | rtsock | ui>
            level level;
            no-remote-trace;
        }
    }
}
}
(compress-configuration-files | no-compress-configuration-files);
ddos-protection {
    global {
        disable-fpc;
        disable-logging;
        disable-routing-engine;
        flow-detection;
        flow-report-rate;
        violation-report-rate;
    }
}

```

```

}
protocols protocol-group (aggregate | packet-type) {
    bandwidth packets-per-second;
    burst size;
    disable-fpc;
    disable-logging;
    disable-routing-engine;
    fpc {
        bandwidth-scale percentage;
        burst-scale percentage;
        disable-fpc;
    }
    priority level;
    recover-time seconds;
    flow-detection {
        flow-detect-time detect-period;
        no-flow-logging;
        timeout-active-flows enable-period;
        flow-level-bandwidth;
        flow-level-control (all | keep-all | police);
        flow-detection-mode (always-on | automatic | disabled);
        physical-interface;
        flow-recover-time recover-period;
        flow-timeout-time timeout-period;
        subscriber;
    }
}
}
traceoptions{
    file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
}
default-address-selection;
diag-port-authentication (encrypted-password "password" | plain-text-password);
dynamic-profile-options {
    versioning;
}
domain-name domain-name;
domain-search [ domain-list ];
do-not-disable-ip6op-ondad;
extensions {
    providers {
        provider-id {
            license-type license deployment-scope [ deployments ];
        }
    }
}
resource-limits {
    package package-name {
        resources {
            cpu {
                priority number;
                time seconds;
            }
        }
    }
}

```

```

    file {
        core-size bytes;
        open number;
        size bytes;
    }
    memory {
        data-size bytes;
        locked-in bytes;
        resident-set-size bytes;
        socket-buffers bytes;
        stack-size bytes;
    }
}
}
process process-ui-name {
    resources {
        cpu {
            priority number;
            time seconds;
        }
        file {
            core-size bytes;
            open number;
            size bytes;
        }
        memory {
            data-size bytes;
            locked-in bytes;
            resident-set-size bytes;
            socket-buffers bytes;
            stack-size bytes;
        }
    }
}
}
}
fips {
    level level;
}
host-name hostname;
inet6-backup-router ipv6-address <destination address>;
internet-options {
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit bucket-size number packet-rate rate;
    icmpv6-rate-limit bucket-size number packet-rate rate;
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    (ipv6-path-mtu-discovery | noipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout;
    no-tcp-rfc1323-paws;
    no-tcp-rfc1323;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit port-number;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
}
kernel-replication;

```

```

license {
    autoupdate {
        url URL;
        password password;
    }
    renew before-expiration number;
    interval number
    traceoptions {
        file <filename> <files number> <size maximum-file-size> <world-readable |
            no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
login {
    announcement "text";
    class class-name {
        access-end "hh<:mm:<ss>>";
        access-start "hh<:mm:<ss>>";
        allow-commands "regular-expression";
        ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular
            expression 2";
        allowed-days [ sunday monday tuesday wednesday thursday friday saturday ];
        configuration-breadcrumbs;
        deny-commands "regular-expression";
        ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
            expression 2";
        idle-timeout minutes;
        logical-system logical-system-name;
        login-alarms;
        login-script filename;
        login-tip;
        permissions [ permissions ];
        security-role [ security-role ];
    }
    deny-sources (address address | apply-groups | apply-groups-except) ;
    message "text";
    password {
        change-type (character-sets | set-transitions);
        format (des | md5 | sha1);
        maximum-length length;
        minimum-changes number;
    }
}

```

```
    minimum-length length;  
    minimum-lower-cases number;  
    minimum-numeric number;  
    minimum-punctuations number;  
    minimum-upper-cases number;  
}  
retry-options {  
    backoff-factor number;  
    backoff-threshold number;  
    maximum-time number;  
    minimum-time number;  
    tries-before-disconnect number;  
}  
user username {  
    authentication {  
        (encrypted-password "password" | plain-text-password);  
        load-key-file filename;  
        ssh-dsa "public-key" <from hostname>;  
        ssh-ecdsa "public-key" <from hostname>;  
        ssh-rsa "public-key" <from hostname>;  
    }  
    class class-name;  
    full-name "complete-name";  
    uid uid-value;  
}  
}  
max-configurations-on-flash number;  
mirror-flash-on-disk;  
name-server {  
    address;  
}  
nd-maxmcast-solicit  
nd-retransmit-timer  
no-multicast-echo;  
no-neighbor-learn;;  
no-ping-record-route;  
no-ping-time-stamp;  
no-redirects;  
no-redirects-ipv6;  
ntp {  
    authentication-key key-number type md5 value password;  
    boot-server address;  
    broadcast <address> <key-number> <ttl value> <version value>;  
    broadcast-client;  
    multicast-client <address>;  
    peer address <key-number> <prefer> <version value>;  
    server address <key-number> <prefer> <version value>;  
    source-address source-address;  
    trusted-key [ key-numbers ];  
}  
pic-console-authentication {  
    (encrypted-password "encrypted-password" | plain-text-password);  
}  
ports {  
    auxiliary {  
        disable;
```

```

    insecure;
    type (ansi | small-xterm | vt100 | xterm);
    port-type (mini-usb | rj45);
  }
}
console {
  disable;
  insecure;
  log-out-on-disconnect;
  type (ansi | small-xterm | vt100 | xterm);
}
}
processes {
  process-name (enable | disable) failover (alternate-media | other-routing-engine);
  command path;
  timeout seconds;
}
proxy {
  password password;
  port port-number;
  server (hostname | ip-address);
  username username;
}
radius-options {
  attributes {
    nas-ip-address address;
  }
  password-protocol mschap-v2;
}
radius-server {
  server-address {
    accounting-port port-number;
    max-outstanding-requests number;
    port port-number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
  }
}
root-authentication {
  (encrypted-password "password" | plain-text-password);
  load-key-file filename;
  ssh-dsa "public-key" <from hostname>;
  ssh-ecdsa "public-key" <from hostname>;
  ssh-rsa "public-key" <from hostname>;
}
(saved-core-context | no-saved-core-context);
saved-core-files number;
scripts {
  load-scripts-from-flash;
  commit {
    allow-transients;
    direct-access;
    file filename.xml {
      checksum (md5 | sha-256 | sha1) hash;
    }
  }
}

```

```

        optional;
        refresh;
        refresh-from url;
        source url;
    }
    max-datasize
    refresh;
    refresh-from url;
    traceoptions {
        file <filename> <files number> <size maximum-file-size> <world-readable |
            no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
op {
    file filename.xml {
        arguments {
            argument-name {
                description descriptive-text;
            }
        }
        checksum (md5 | sha-256 | sha1) hash;
        command filename-alias;
        description descriptive-text;
        refresh;
        refresh-from url;
        source url;
    }
    max-datasize
    no-allow-url
    refresh;
    refresh-from url;
    traceoptions {
        file <filename> <files number> <size maximum-file-size> <world-readable |
            no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
}
static-host-mapping {
    hostname {
        alias [ aliases ];
        inet [ addresses ];
        inet6 [ addresses ];
        sysid system-identifier;
    }
}
syslog {
    allow-duplicates;
    archive <binary-data | no-binary-data> <files number> <size size> <world-readable |
        no-world-readable>;
    console {

```



```

any | authorization | change-log | conflict-log | daemon | dfc | external | firewall | ftp
| interactive-commands | kernel | ntp | pfe | security | user) (alert | any | critical |
emergency | error | info | none | notice | warning);
}
file filename {
    facility severity;
    allow-duplicates;
    any (alert | any | critical | emergency | error | info | none | notice | warning);
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
        <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
no-world-readable>;
    authorization (alert | any | critical | emergency | error | info | none | notice | warning);
    change-log (alert | any | critical | emergency | error | info | none | notice | warning);
    conflict-log (alert | any | critical | emergency | error | info | none | notice | warning);
    daemon (alert | any | critical | emergency | error | info | none | notice | warning);
    dfc (alert | any | critical | emergency | error | info | none | notice | warning);
    explicit-priority;
    external (alert | any | critical | emergency | error | info | none | notice | warning);
    firewall (alert | any | critical | emergency | error | info | none | notice | warning);
    ftp (alert | any | critical | emergency | error | info | none | notice | warning);
    interactive-commands (alert | any | critical | emergency | error | info | none | notice
| warning);
    kernel (alert | any | critical | emergency | error | info | none | notice | warning);
    match "regular-expression";
    ntp (alert | any | critical | emergency | error | info | none | notice | warning);
    pfe (alert | any | critical | emergency | error | info | none | notice | warning);
    security (alert | any | critical | emergency | error | info | none | notice | warning);
    structured-data {
        brief
    }
}
host (hostname | other-routing-engine | scc-master) {
    facility severity;
    authorization (alert | any | critical | emergency | error | info | none | notice | warning);
    change-log (alert | any | critical | emergency | error | info | none | notice | warning);
    conflict-log (alert | any | critical | emergency | error | info | none | notice | warning);
    daemon (alert | any | critical | emergency | error | info | none | notice | warning);
    dfc (alert | any | critical | emergency | error | info | none | notice | warning);
    explicit-priority;
    external (alert | any | critical | emergency | error | info | none | notice | warning);
    facility-override facility;
    firewall (alert | any | critical | emergency | error | info | none | notice | warning);
    ftp (alert | any | critical | emergency | error | info | none | notice | warning);
    interactive-commands (alert | any | critical | emergency | error | info | none | notice
| warning);
    kernel (alert | any | critical | emergency | error | info | none | notice | warning);
    log-prefix string;
    match "regular-expression";
    ntp (alert | any | critical | emergency | error | info | none | notice | warning);
    pfe (alert | any | critical | emergency | error | info | none | notice | warning);
    security (alert | any | critical | emergency | error | info | none | notice | warning);
    source-address source-address;
    structured-data {
        brief
    }
    user (username | *) {
    }
}
log-rotate-frequency minutes;

```

```

server;
source-address address;
time-format (year | millisecond | year millisecond);
user (username | *) {
    facility severity;
    match "regular-expression";
}
}
tacplus-options {
    (exclude-cmd-attribute | no-cmd-attribute-value);
    service-name service-name;
}
tacplus-server {
    server-address {
        port port-number;
        secret password;
        single-connection;
        source-address source-address;
        timeout seconds;
    }
}
time-zone (GMT | GMT+hour-offset | GMT-hour-offset | zone-name);
tracing destination-override syslog host address;
use-imported-time-zones;
}
}
system {
    services {
        database-replication {
            traceoptions {
                file <filename> <files number> <match regular-expression>
                <size maximum-file-size> <world-readable | no-world-readable>;
                flag flag;
                no-remote-trace;
            }
        }
        dhcp-local-server {
            authentication {
                password password;
                username-include {
                    circuit-type;
                    delimiter delimiter-character;
                    domain-name domain-name;
                    logical-system-name;
                    mac-address;
                    option-60;
                    option-82 <circuit-id> <remote-id>;
                    routing-instance-name;
                    user-prefix user-prefix;
                }
            }
        }
        dynamic-profile (profile-name | junos-default-profile) <aggregate-clients <merge |
        replace> | use-primary primary-profile-name>;
        forward-snooped-clients (all-interfaces | configured-interfaces |
        non-configured-interfaces);
        group group-name {

```

```

dynamic-profile (profile-name | junos-default-profile) <aggregate-clients <merge |
    replace> | use-primary primary-profile-name>;
interface interface-name {
    exclude;
    overrides {
        ...same statements as at the [edit system services dhcp-local-server overrides]
        hierarchy level ...
    }
    trace;
    upto upto-interface-name;
}
}
overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
}
dhcpv4-profiles profile-name {
    bind-interface interface-name;
    dead-server-retry-interval interval-in-seconds;
    dead-server-successive-retry-attempt number-of-attempts;
    dhcp-server-selection-algorithm (highest-priority-server | round-robin);
    lease-time time-in-seconds;
    pool-name pool-name;
    retransmission-attempt number-of-attempts;
    retransmission-interval interval-in-seconds;
    servers ip-address {
        priority value;
    }
}
}
dhcpv6-profiles profile-name {
    bind-interface interface-name;
    lease-time time-in-seconds;
    pool-name pool-name;
    retransmission-attempt number-of-attempts;
    retransmission-interval interval-in-seconds;
}
}
}

```

```
finger {
    connection-limit limit;
    rate-limit limit;
}
flow-tap-dtcp {
    ssh {
        connection-limit limit;
        rate-limit limit;
    }
}
ftp {
    connection-limit limit;
    rate-limit limit;
}
local-policy-decision-function {
    statistics {
        aacl-statistics-profile profile-name {
            aacl-fields {
                address;
                all-fields;
                application;
                application-group;
                input-bytes;
                input-interface;
                input-packets;
                ipv6-address
                ipv6-prefix-length
                mask;
                output-bytes;
                output-packets;
                subscriber-name;
                timestamp;
                vrf-name;
            }
            file filename;
            record-type (delta | interim);
        }
        file filename {
            archive-sites {
                url;
            }
            files number;
            size bytes;
            transfer-interval minutes;
        }
        record-type (data | interim);
    }
    traceoptions {
        file <filename> <files number> <match regular-expression>
          <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
netconf {
    ssh {
```

```

        connection-limit limit;
        port port;
        rate-limit limit;
    }
    traceoptions {
        file <filename> <files number> <match regular-expression> <size size>
            <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
        on-demand;
    }
}
outbound-ssh {
    client client-id {
        address {
            port port-number;
            retry number;
            timeout seconds;
        }
        device-id device-id;
        keep-alive {
            retry number;
            timeout seconds;
        }
        reconnect-strategy (in-order | sticky);
        secret secret;
        services netconf;
    }
    traceoptions {
        file <filename> <files number> <match regular-expression>
            <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
resource-monitor {
    resource-category jtree {
        resource-type free-dwords {
            low-watermark number;
            high-watermark number;
        }
        resource-type free-pages {
            low-watermark number;
            high-watermark number;
        }
    }
}
no-throttle;
no-logging;
high-threshold number;
traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
}

```

```
service-deployment {
  local-certificate certificate-name;
  servers {
    server-address {
      port port-number;
      security-options {
        (ssl3 | tls);
      }
      user username;
    }
  }
  source-address source-address;
  traceoptions {
    flag flag;
  }
}
ssh {
  ciphers [ cipher-1 cipher-2 cipher-3 ... ]
  client-alive-count-max seconds;
  client-alive-interval seconds;
  connection-limit limit;
  hostkey-algorithm limit;
  key-exchange limit;
  macs limit;
  max-sessions-per-connection number;
  no-tcp-forwarding;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
}
subscriber-management {
  enforce-strict-scale-limit-license;
  gres-route-flush-delay;
  maintain-subscriber {
    interface-delete;
  }
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
telnet {
  connection-limit limit;
  rate-limit limit;
}
tftp-server {
  connection-limit limit;
  rate-limit limit;
```

```
}
xnm-clear-text {
  connection-limit limit;
  rate-limit limit;
}
xnm-ssl {
  connection-limit limit;
  local-certificate certificate-name;
  rate-limit limit;
  ssl-renegotiation ;
}
}
```

**Related Documentation** • *Notational Conventions Used in Junos OS Configuration Hierarchies*


## action-shutdown

<b>Syntax</b>	<code>action-shutdown;</code>
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): [edit forwarding-options <b>storm-control-profiles</b> <i>profile-name</i>]</li> <li>For platforms without ELS: [edit ethernet-switching-options storm-control]</li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>
<b>Description</b>	<p>Shut down or temporarily disable interfaces when the storm control level is exceeded, as follows:</p> <ul style="list-style-type: none"> <li>If you set both the <b>action-shutdown</b> and the <b>port-error-disable</b> statements, the interfaces are disabled temporarily and recover automatically when the disable timeout expires. (The <b>port-error-disable</b> statement is not available for MX Series routers.)</li> <li>If you set both the <b>action-shutdown</b> and the <b>recovery-timeout</b> statements, the interfaces are disabled temporarily and recover automatically when the recovery timeout expires.</li> <li>If you set the <b>action-shutdown</b> statement and do not specify the <b>port-error-disable</b> statement (the <b>port-error-disable</b> 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 <b>clear ethernet-switching port-error</b> command to clear the port error and restore the interfaces to service. (The <b>clear ethernet-switching port-error</b> command is not available for MX Series routers.)</li> <li>If you set the <b>action-shutdown</b> statement and do not specify the <b>recovery-timeout</b> 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 <b>clear ethernet-switching recovery-timeout</b> command and for MX Series routers you must issue the <b>clear bridge recovery-timeout</b> command to clear the port error and restore the interfaces to service.</li> </ul>
<b>Default</b>	The <b>action-shutdown</b> 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.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>




- Related Documentation**
- *port-error-disable*
  - *disable-timeout*
  - [recovery-timeout on page 64](#)
  - *clear ethernet-switching port-error*
  - *clear bridge recovery-timeout*
  - [clear ethernet-switching recovery-timeout on page 70](#)
  - *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
  - *Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers*
  - [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13](#)
  - *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*
  - [Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces \(CLI Procedure\) on page 12](#)

## bandwidth-level

<b>Syntax</b>	<code>bandwidth-level <i>kbps</i>;</code>
<b>Hierarchy Level</b>	[edit forwarding-options <a href="#">storm-control-profiles</a> <i>profile-name</i> all]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX Series. Statement introduced in Junos OS Release 14.1 for MX Series routers.
<b>Description</b>	Configure the storm control level as the bandwidth in kilobits per second of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.
<div>  <p><b>NOTE:</b> When you configure 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. For example, if you configure a storm control level 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.</p> </div>	
<b>Default</b>	<p>On EX4300 switches—If you do not specify the storm control level using either the <b>bandwidth-level</b> or the <b>bandwidth-percentage</b> statements, the storm control level defaults to 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.</p> <p>On EX9200 switches—Storm control is not enabled by default.</p> <p>On MX Series routers—Storm control is not enabled by default.</p>
<b>Options</b>	<p><b>bandwidth-level <i>kbps</i></b>—Traffic rate in kilobits per second of the combined broadcast, multicast, and unknown unicast traffic streams.</p> <p><b>Range:</b> 100 through 10,000,000</p> <p><b>Range:</b> 100 through 100,000,000 on QFX10000 Series switches</p> <p><b>Default:</b> None</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">bandwidth-percentage on page 47</a></li> <li>• <a href="#">Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13</a></li> <li>• <a href="#">Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers</a></li> </ul>

- [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)

## bandwidth-percentage

<b>Syntax</b>	<code>bandwidth-percentage <i>percentage</i>;</code>
<b>Hierarchy Level</b>	[edit forwarding-options <a href="#">storm-control-profiles</a> <i>profile-name</i> all]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series. Statement introduced in Junos OS Release 14.1 for MX Series routers.
<b>Description</b>	Configure the storm control level as the percentage of available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams on an interface. The storm control level is configured as part of the storm control profile.
<div>  <p><b>NOTE:</b> When you configure 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. For example, if you configure a storm control level 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.</p> </div>	
<b>Default</b>	<p>On EX4300 switches—The storm control level is 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.</p> <p>On EX9200 switches—Storm control is not enabled by default.</p> <p>On MX Series routers—Storm control is not enabled by default.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">bandwidth-level on page 46</a></li> <li>• <a href="#">Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13</a></li> <li>• <a href="#">Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers</a></li> <li>• <a href="#">Configuring or Disabling Storm Control (CLI Procedure) on page 7</a></li> </ul>

## filter (VLANs)

---

<b>Syntax</b>	<code>filter (input   output) <i>filter-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit vlans <i>vlan-name</i>],</code> <code>[edit vlans <i>vlan-name</i> forwarding-options]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
<b>Description</b>	Apply a firewall filter to traffic entering or exiting a VLAN.
<b>Default</b>	All incoming traffic is accepted unmodified to a VLAN, and all outgoing traffic is sent unmodified from a VLAN.
<b>Options</b>	<b><i>filter-name</i></b> —Name of a firewall filter defined at the <code>[edit firewall family <i>family-name</i> filter]</code> hierarchy level.  <b>input</b> —Apply a firewall filter to VLAN ingress traffic.  <b>output</b> —Apply a firewall filter to VLAN egress traffic.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Firewall Filters</i></li><li>• <i>Overview of Firewall Filters</i></li></ul>

## filter (Firewall Filters)

<b>Syntax</b>	<pre> filter <i>filter-name</i> {     interface-specific;     term <i>term-name</i> {         from {             <i>match-conditions</i>;         }         then {             <i>action</i>;             <i>action-modifiers</i>;         }     } } </pre>
<b>Hierarchy Level</b>	[edit firewall family <i>family-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches. Option <i>interface-specific</i> introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Configure firewall filters.
<b>Options</b>	<p><i>filter-name</i>—Name that identifies the filter. The name can contain letters, numbers, and hyphens (-), and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches</i></li> <li>• <i>Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches</i></li> <li>• <i>Configuring Firewall Filters (CLI Procedure)</i></li> <li>• <i>Configuring Firewall Filters (J-Web Procedure)</i></li> <li>• <i>Firewall Filters for EX Series Switches Overview</i></li> </ul>

## flood (VLANs)

---

<b>Syntax</b>	<pre>flood {     input <i>filter-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit vlans <i>vlan-name</i> ], [edit vlans <i>vlan-name</i> forwarding-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
<b>Description</b>	<p>Apply a flood filter to traffic ingressing a VLAN. Flood filters are triggered only for broadcast, unknown unicast, and multicast (BUM) traffic.</p> <p>Flood filters and firewall filters can coexist on the same VLAN. If the actions in the filters are conflicting, then the firewall filter takes priority over the flood filter.</p>
<b>Default</b>	All incoming traffic is accepted unmodified to a VLAN, and all outgoing traffic is sent unmodified from a VLAN.
<b>Options</b>	<p><i>filter-name</i>—Name of a filter defined at the [edit firewall family <i>family-name</i> filter] hierarchy level.</p> <p><i>input</i>—Apply a flood filter to VLAN ingress traffic.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Unknown Unicast Forwarding (CLI Procedure) on page 21</a></li><li>• <a href="#">Configuring Firewall Filters</a></li><li>• <a href="#">Overview of Firewall Filters</a></li></ul>

## forwarding-options

```
Syntax forwarding-options {
    dhcp-security {
        arp-inspection;
        group group-name {
            interface interface-name {
                static-ip ip-address {
                    mac mac-address;
                }
            }
        }
        overrides {
            no-option82;
            (trusted | untrusted);
        }
    }
    ip-source-guard;
    no-dhcp-snooping;
    option-82 {
        circuit-id {
            prefix {
                host-name;
                logical-system-name;
                routing-instance-name;
            }
            use-interface-description (device | logical);
            use-vlan-id;
        }
        remote-id {
            host-name hostname;
            use-interface-description (device | logical);
            use-string string;
        }
        vendor-id {
            use-string string;
        }
    }
}
filter {
    input filter-name;
    output filter-name;
}
flood {
    input filter-name;
}
```

**Hierarchy Level** [edit],  
[edit bridge-domains *bridge-domain-name*],  
[edit vlans *vlan-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

	Hierarchy level <b>[edit vlans <i>vlan-name</i>]</b> introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Hierarchy level <b>[edit bridge-domains <i>bridge-domain-name</i>]</b> introduced in Junos OS Release 14.1 for MX Series routers.
<b>Description</b>	Configure traffic forwarding.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Traffic Forwarding and Monitoring</i></li><li>• <i>[edit forwarding-options] Hierarchy Level</i></li></ul>

---

## group-type (Unknown Unicast Forwarding)

---

<b>Syntax</b>	group-type ( <i>none</i>   layer-2)
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options next-hop-group</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.2 for EX Series switches.
<b>Description</b>	Configure the type of addresses to be used in the next-hop group.
<b>Options</b>	<i>none</i> —Next-hop group uses Layer 2 addresses.  <i>layer-2</i> —Specify a next-hop group that uses Layer 2 addresses.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Unknown Unicast Forwarding (CLI Procedure) on page 21</a></li><li>• <i>Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure)</i></li></ul>



## icmpv4-rate-limit

---

<b>Syntax</b>	icmpv4-rate-limit { bucket-size <i>seconds</i> ; packet-rate <i>pps</i> ; }
<b>Hierarchy Level</b>	[edit system internet-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure rate-limiting parameters for ICMPv4 messages sent.
<b>Options</b>	<p><b>bucket-size <i>seconds</i></b>—Number of seconds in the rate-limiting bucket.  <b>Range:</b> 0 through 4294967295 seconds  <b>Default:</b> 5</p> <p><b>packet-rate <i>pps</i></b>—Rate-limiting packets earned per second.  <b>Range:</b> 0 through 4294967295 pps  <b>Default:</b> 1000</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 23</a></li> </ul>

## icmpv6-rate-limit

---

<b>Syntax</b>	<code>icmpv6-rate-limit {     bucket-size <i>seconds</i>;     packet-rate <i>packet-rate</i>; }</code>
<b>Hierarchy Level</b>	[edit system internet-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure rate-limiting parameters for ICMPv6 messages sent.
<b>Options</b>	<b>bucket-size <i>seconds</i></b> —Number of seconds in the rate-limiting bucket. <b>Range:</b> 0 through 4294967295 seconds <b>Default:</b> 5  <b>packet-rate <i>pps</i></b> —Rate-limiting packets earned per second. <b>Range:</b> 0 through 4294967295 pps <b>Default:</b> 1000
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 23</a></li></ul>

## next-hop-group (Unknown Unicast Forwarding)

**Syntax** `next-hop-group group-name {  
     group-type {  
         layer-2;  
     }  
     interface interface-name {  
         next-hop address;  
     }  
     next-hop-subgroup subgroup-name {  
         interface interface-name;  
     }  
 }`

**Hierarchy Level** [edit [forwarding-options](#)]

**Release Information** Statement introduced in Junos OS Release 14.2 for EX Series switches.

**Description** Configure a next-hop group to forward unknown unicast packets to a specific interface or interfaces.

**Options** *group-name*—Name of the next-hop group.

The remaining statements are explained separately.

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

**Related Documentation**

- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 21](#)
- [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\)](#)

## no-broadcast

<b>Syntax</b>	no-broadcast;
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): [edit forwarding-options <b>storm-control-profiles</b> <i>profile-name</i> all]</li> <li>For platforms without ELS: [edit ethernet-switching-options storm-control interface (all   <i>interface-name</i>)]</li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>
<b>Description</b>	Disable storm control for broadcast traffic for the specified interface or for all interfaces.
<b>Default</b>	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> <li>On EX9200 switches—Storm control is not enabled by default.</li> <li>On MX Series routers—Storm control is not enabled by default.</li> </ul>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

**Related  
Documentation**

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13](#)
- *Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers*
- *Disabling or Enabling Storm Control (CLI Procedure)*
- [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)

## no-multicast

<b>Syntax</b>	no-multicast;
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): [edit forwarding-options <b>storm-control-profiles</b> <i>profile-name</i> all]</li> <li>For platforms without ELS: [edit ethernet-switching-options storm-control interface (all   <i>interface-name</i>)]</li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.3 for EX Series switches.</p> <p>Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>
<b>Description</b>	Disable storm control for all multicast traffic (both registered multicast and unregistered multicast) for the specified interface or for all interfaces.
<b>Default</b>	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> <li>On EX9200 switches—Storm control is not enabled by default.</li> <li>On MX Series routers—Storm control is not enabled by default.</li> </ul>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [no-registered-multicast on page 60](#)
  - [no-unregistered-multicast on page 63](#)
  - *Disabling or Enabling Storm Control (CLI Procedure)*
  - [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)

## no-registered-multicast

---

<b>Syntax</b>	no-registered-multicast;
<b>Hierarchy Level</b>	<ul style="list-style-type: none"><li>For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): [edit forwarding-options <b>storm-control-profiles</b> <i>profile-name</i> all]</li><li>For platforms without ELS: [edit ethernet-switching-options storm-control interface (all   <i>interface-name</i>)]</li></ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.3 for EX Series switches.</p> <p>Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
<b>Description</b>	<p>(EX8200 switches only) Disable storm control for registered multicast traffic for the specified interface or for all interfaces.</p> <p>(EX4300 and EX9200 switches only) Exclude storm control for registered multicast traffic from a storm control profile.</p> <p>(MX Series routers only) Exclude storm control for registered multicast traffic from a storm control profile.</p>
<b>Default</b>	<p>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.</p> <p>EX9200 switches—Storm control is not enabled by default.</p> <p>MX Series routers—Storm control is not enabled by default.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li><a href="#">no-multicast on page 58</a></li><li><a href="#">no-unregistered-multicast on page 63</a></li><li><i>Understanding Storm Control on EX Series Switches</i></li><li><a href="#">Understanding Storm Control on Switching Devices on page 3</a></li></ul>



## no-unknown-unicast

<b>Syntax</b>	no-unknown-unicast;
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): [edit forwarding-options <b>storm-control-profiles</b> <i>profile-name</i> all]</li> <li>For platforms without ELS: [edit ethernet-switching-options storm-control interface (all   <i>interface-name</i>)]</li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>
<b>Description</b>	Disable storm control for unknown unicast traffic for the specified interface or for all interfaces.
<b>Default</b>	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> <li>On EX9200 switches—Storm control is not enabled by default.</li> <li>MX Series routers—Storm control is not enabled by default.</li> </ul>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>


**Related  
Documentation**

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13](#)
- *Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers*
- *Disabling or Enabling Storm Control (CLI Procedure)*
- [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)

## no-unregistered-multicast

<b>Syntax</b>	no-unregistered-multicast;
<b>Hierarchy Level</b>	<ul style="list-style-type: none"> <li>For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): [edit forwarding-options <a href="#">storm-control-profiles</a> <i>profile-name</i> all]</li> <li>For platforms without ELS: [edit ethernet-switching-options storm-control interface (all   <i>interface-name</i>)]</li> </ul>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.3 for EX Series switches.</p> <p>Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
<b>Description</b>	<p>(EX8200 switches only) Disable storm control for unregistered multicast traffic for the specified interface or for all interfaces.</p> <p>(EX4300 and EX9200 switches only) Exclude storm control for unregistered multicast traffic from a storm control profile.</p> <p>(MX Series routers) Exclude storm control for unregistered multicast traffic from a storm control profile.</p>
<b>Default</b>	<p>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.</p> <p>EX9200 switches—Storm control is not enabled by default.</p> <p>MX Series routers—Storm control is not enabled by default.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">no-multicast on page 58</a></li> <li><a href="#">no-registered-multicast on page 60</a></li> <li><i>Understanding Storm Control on EX Series Switches</i></li> <li><a href="#">Understanding Storm Control on Switching Devices on page 3</a></li> </ul>

## recovery-timeout

<b>Syntax</b>	<code>recovery-timeout seconds;</code>
<b>Hierarchy Level (EX Series and QFX Series)</b>	[edit interfaces <i>interface-name</i> unit 0 family ethernet-switching]
<b>Hierarchy Level (MX Series)</b>	[edit interfaces <i>interface-name</i> unit 0 family bridge]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX Series. Statement introduced in Junos OS Release 14.1 for the MX Series routers.
<b>Description</b>	<p>Configure an interface to be temporarily disabled when MAC limiting, MAC move limiting, or rate-limiting is in effect with the action <b>shutdown</b>. This enables the affected interface to recover automatically from the error condition after the specified period of time:</p> <ul style="list-style-type: none"> <li>• If you configure MAC limiting with the <b>shutdown</b> option and you enable <b>recovery-timeout</b>, the interface is temporarily disabled when the MAC address limit is reached. The interface will recover automatically after the number of seconds specified.</li> <li>• If you enable MAC move limiting with the <b>shutdown</b> option and you enable <b>recovery-timeout</b>, the interface is temporarily disabled when the maximum number of MAC address moves is reached. The interface will recover automatically after the number of seconds specified.</li> <li>• If you enable MAC move limiting with the <b>vlan-member-shutdown</b> option and you enable <b>recovery-timeout</b>, the interface is temporarily disabled when the maximum number of MAC address moves is reached. The interface will recover automatically after the number of seconds specified. If the recovery timeout is not configured, the interface will recover automatically after 180 seconds.</li> <li>• If you enable storm control with the <b>action-shutdown</b> option and you enable <b>recovery-timeout</b>, the interface is temporarily disabled when applicable traffic exceeds the specified levels. Depending upon the configuration, applicable traffic can include broadcast, unknown unicast, and multicast traffic.</li> </ul>
	<p> <b>NOTE:</b> The <b>recovery-timeout</b> configuration does not apply to preexisting error conditions. It impacts only error conditions that are detected after the <b>recovery-timeout</b> statement is configured and committed. To clear a preexisting error condition and restore the interface to service, use the operational mode commands <b>clear ethernet-switching recovery-timeout</b> for EX Series and QFX Series and <b>clear bridge recovery-timeout</b> for MX Series routers.</p>
<b>Default</b>	The interface does not automatically recover from an error condition.



**NOTE:** On EX9200 switches, if a MAC move limit is configured with the action `vlan-member-shutdown`, the interface automatically recovers from the disabled condition after 180 seconds by default.

**Options** **seconds**— Number of seconds that the interface remains in a disabled state due to a port error prior to automatic recovery.


**Range:** 10 through 3600

**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 44](#)
  - [Configuring MAC Limiting \(CLI Procedure\)](#)
  - [Configuring MAC Move Limiting \(CLI Procedure\)](#)
  - [Configuring or Disabling Storm Control \(CLI Procedure\) on page 7](#)

## storm-control

---

<b>Syntax</b>	<code>storm-control storm-control-profile;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>number</i> family ethernet-switching], [edit interfaces <i>interface-name</i> unit <i>number</i> family bridge] [edit interfaces <i>interface-name</i> ether-options ethernet-switch-profile]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series. Statement introduced in Junos OS Release 14.1 for the MX Series routers.
<b>Description</b>	<p>Bind a storm control profile to a logical interface.</p> <p>On switches running ELS software, storm control is enabled by default on all switch interfaces at a level of 80 percent of the combined broadcast and unknown unicast streams. (For the equivalent statement for platforms running non-ELS software, see <i>storm-control</i>.)</p> <div><b>NOTE:</b> If you configure storm control on an aggregated Ethernet interface, the storm-control level is applied to each member interface individually. For example, if the aggregated interface has two members and you configure a storm-control level of 20 kbps, Junos will not detect a storm if one or both of the member interfaces receives traffic at 15 kbps because in neither of these cases does an individual member receive traffic at a rate greater than the configured storm-control level. In this example, Junos detects a storm only if at least one member interface receives traffic at greater than 20 Kbps.</div>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 13</a></li><li>• <a href="#">Understanding Storm Control on Switching Devices on page 3</a></li></ul>

## storm-control-profiles

**Syntax** `storm-control-profiles profile-name {  
     action-shutdown;  
     all {  
         bandwidth-level;  
         bandwidth-percentage;  
         no-broadcast;  
         no-multicast;  
         no-registered-multicast;  
         no-unknown-unicast;  
         no-unregistered-multicast;  
     }  
 }`

**Hierarchy Level** [edit forwarding-options]

**Release Information** Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  
 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** Configure a storm control profile on a switch or router. Storm control is used to prevent network outages that are caused by broadcast traffic storms. Storm control enables the switching device to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the storm control level or storm control bandwidth—is exceeded, thus preventing packets from proliferating and degrading the LAN.



**NOTE:** The name of the storm control profile can contain no more than 127 characters.

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 13](#)
- [Understanding Storm Control on Switching Devices on page 3](#)





## CHAPTER 6

# Operational Commands

- `clear ethernet-switching recovery-timeout`

## clear ethernet-switching recovery-timeout

---

<b>Syntax</b>	clear ethernet-switching recovery-timeout
<b>Release Information</b>	Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
<b>Description</b>	Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch, and restore the interfaces to service.
<b>Options</b>	<b>interface <i>interface-name</i> vlan <i>vlan-name</i></b> —(EX9200 switches) Unblock an interface on the basis of its membership in the specified VLAN. This option can be used to restore an interface that is blocked because of a <b>vlan-member-shutdown</b> action.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Autorecovery from the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)</a> on page 12</li></ul>
<b>Output Fields</b>	This command produces no output.